OMRON

Safety Network Controller

NX-series

Safety Control Unit/ Communication Control Unit

User's Manual

NX-SL5□□□
NX-SI□□□□
NX-SO□□□□
NX-CSG□□□

Safety Control Unit
Communication Control Unit



SYSMAC always in control

Z395-E1-21

NOTE

- All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, mechanical, electronic, photocopying, recording, or otherwise, without the prior written permission of OMRON.
- No patent liability is assumed with respect to the use of the information contained herein. Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this manual is subject to change without notice.
- Every precaution has been taken in the preparation of this manual. Nevertheless, OMRON assumes no responsibility for errors or omissions.
  Neither is any liability assumed for damages resulting from the use of the information contained in this publication.

Trademarks

- Sysmac and SYSMAC are trademarks or registered trademarks of OMRON Corporation in Japan and other countries for OMRON factory automation products.
- Microsoft, Windows, Excel, Visual Basic, and Microsoft Edge are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.
- Safety over EtherCAT® is a registered trademark and a patented technology licensed by Beckhoff Automation GmbH, Germany.
- ODVA, CIP, CompoNet, DeviceNet, EtherNet/IP, and CIP Safety are trademarks of ODVA.
- The SD and SDHC logos are trademarks of SD-3C, LLC.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

- Microsoft product screen shots used with permission from Microsoft.
- This product incorporates certain third party software. The license and copyright information associated with this software is available at http://www.fa.omron.co.jp/nj_info_e/.

Introduction

Thank you for purchasing an NX-series Safety Control Unit / Communication Control Unit.
This manual contains information that is necessary to use the NX-series Safety Control Unit / Communication Control Unit.
Please read this manual and make sure you understand the functionality and performance of the Unit before you attempt to use it in a control system.
Keep this manual in a safe place where it will be available for reference during operation.

Intended Audience

This manual is intended for the following personnel, who must also have knowledge of electrical systems (an electrical engineer or the equivalent).

- Personnel in charge of introducing FA systems.
- Personnel in charge of designing FA systems.
- Personnel in charge of installing and maintaining FA systems.
- Personnel in charge of managing FA systems and facilities.
- Personnel with the qualifications, authority, and responsibility for providing safety at each phase of the lifecycle of the machine: design, installation, operation, maintenance, and disposal.
- Personnel with a knowledge of functional safety.

For programming, this manual is intended for personnel who understand the programming language specifications in international standard IEC 61131-3 or Japanese standard JIS B 3503.

Applicable Products

This manual covers the following products.

- NX-series Safety Control Units
  NX-SL5□□□
  NX-SI□□□□
  NX-SO□□□□
- NX-series Communication Control Unit
  NX-CSG□□□

Note that this manual provides information for using an NX-series Safety Control Unit described above together with an NX-series Communication Control Unit. When you use it with an NJ/NX-series CPU Unit, an EtherCAT Coupler Unit, or an EtherNet/IP Coupler Unit, refer to the *NX-series Safety Control Unit User's Manual (Cat. No. Z930)*.

Sections in this Manual

1 Overview

2 System Configuration and Configuration Devices

3 Specifications of Configuration Units

4 Designing the Power Supply System

5 Installation and Wiring

6 Safety Network Controller Operation

7 Settings

8 Programming

9 Checking Operation and Actual Operation

10 Calculating Safety Reaction Times

11 Communications Load

12 Safety Unit Restore

13 Backup Functions of the Communication Control Unit

14 Safety Data Logging

15 Troubleshooting

16 Inspection and Maintenance

A Appendices

I Index

CONTENTS

Introduction **1**
Intended Audience 1
Applicable Products 1

Sections in this Manual **3**

Relevant Manuals **13**

Manual Structure **15**
Page Structure 15
Special Information 16
Precaution on Terminology 16

Terms and Conditions Agreement **17**
Warranty, Limitations of Liability 17
Application Considerations 18
Disclaimers 18
Statement of security responsibilities for assumed use cases and against threats 19

Safety Precautions **20**
Definition of Precautionary Information 20
Symbols 20
Warnings 21
Cautions 28

Precautions for Safe Use **29**

Precautions for Correct Use **36**

Regulations and Standards **40**
Conformance to EU Directives 40
Conformance to EN ISO 13849-1 42
Conformance to UL and CSA Standards 42
Conformance to Shipbuilding Standards 42
Conformance to KC Certification 42

Unit Versions **44**
Unit Versions 44
Unit Versions of Units and Sysmac Studio Versions 46

Related Manuals **48**

Terminology **50**

Revision History **54**

Section 1 Overview

1-1 Overview of the Safety Network Controller **1-2**
1-1-1 Features 1-2
1-1-2 Introduction to the System Configurations 1-4

1-2 Procedure **1-7**
1-2-1 Overall Procedure 1-7

1-2-2 Detailed Procedures....1-8

Section 2 System Configuration and Configuration Devices

2-1 Basic Configuration....2-2
2-1-1 CPU Rack Configuration....2-2
2-1-2 EtherNet/IP Field Network Configuration....2-3
2-1-3 Configuration Units....2-3
2-2 Connecting the Support Software....2-5
2-3 Network Configuration between Controllers....2-6

Section 3 Specifications of Configuration Units

3-1 Communication Control Unit....3-2
3-1-1 Models and Specifications....3-2
3-1-2 Built-in EtherNet/IP Port Specifications....3-7
3-1-3 Part Names and Functions....3-10
3-1-4 Terminal Blocks....3-12
3-1-5 Indicators....3-14
3-1-6 ID Information Indication....3-21
3-2 Safety CPU Unit....3-22
3-2-1 Models and Specifications....3-22
3-2-2 Part Names and Functions....3-26
3-2-3 Indicators....3-27
3-3 Safety Input Unit....3-32
3-3-1 Models and Specifications....3-32
3-3-2 Part Names and Functions....3-38
3-3-3 Indicators....3-40
3-4 Safety Output Unit....3-45
3-4-1 Models and Specifications....3-45
3-4-2 Part Names and Functions....3-52
3-4-3 Indicators....3-55
3-5 End Cover....3-59
3-5-1 Models and Specifications....3-59
3-6 SD Memory Cards....3-60
3-6-1 Models and Specifications....3-60
3-6-2 Purpose....3-60
3-7 Support Software....3-61
3-7-1 Product Model....3-61
3-7-2 Connection....3-62
3-8 PFH....3-63

Section 4 Designing the Power Supply System

4-1 Power Supply System....4-2
4-1-1 NX Unit Power Supply and I/O Power Supply....4-2
4-1-2 NX-series Power Supply-related Units....4-3
4-2 Designing the NX Unit Power Supply System....4-9
4-2-1 Procedure for Designing the NX Unit Power Supply System....4-9
4-2-2 Calculation Example for the NX Unit Power Supply....4-10
4-3 Designing the I/O Power Supply System....4-12
4-3-1 I/O Power Supply Method....4-12
4-3-2 Designing the I/O Power Supply from the NX Bus....4-13

4-3-3 Designing the I/O Power Supply from External Sources....4-18
4-3-4 Restrictions on Inrush Current for ON/OFF Operation....4-19

4-4 Selecting External Power Supplies and Protective Devices....4-20
4-4-1 Selecting the Unit Power Supply....4-20
4-4-2 Selecting the I/O Power Supplies....4-22
4-4-3 Selecting Protective Devices....4-23

Section 5 Installation and Wiring

5-1 Processing at Power ON....5-2
5-1-1 Power ON Operation....5-2
5-1-2 Operation When Resetting the Controller from the Sysmac Studio....5-2

5-2 Mounting Units....5-4
5-2-1 Installation in a Control Panel....5-5
5-2-2 Preparations for Installation....5-9
5-2-3 Installing the Communication Control Unit....5-11
5-2-4 Installing and Connecting NX Units....5-13
5-2-5 Mounting the End Cover....5-17
5-2-6 Mounting the End Plates....5-18
5-2-7 Attaching Markers....5-20
5-2-8 Installing and Removing the SD Memory Card....5-21
5-2-9 Removal of the Communication Control Unit....5-26
5-2-10 Removing NX Units....5-27
5-2-11 Assembled Appearance and Dimensions....5-28

5-3 Wiring....5-32
5-3-1 Wiring the Power Supply....5-33
5-3-2 Wiring the Additional NX Unit Power Supply Unit....5-34
5-3-3 Wiring the Additional I/O Power Supply Unit....5-34
5-3-4 Wiring the Protective Devices....5-34
5-3-5 Grounding....5-35
5-3-6 Connecting the Built-in EtherNet/IP Port....5-39
5-3-7 Wiring to the Screwless Clamping Terminal Blocks....5-46

5-4 Control Panel Installation....5-60
5-4-1 Temperature....5-60
5-4-2 Humidity....5-62
5-4-3 Vibration and Shock....5-62
5-4-4 Atmosphere....5-62
5-4-5 Electrical Environment....5-63
5-4-6 Grounding....5-67

Section 6 Safety Network Controller Operation

6-1 Overview of the Safety Network Controller Operation....6-2
6-1-1 Introduction to FSoE Communications....6-2
6-1-2 Introduction to Communications between NX Units....6-3
6-1-3 Introduction to CIP Safety Communications....6-3
6-1-4 Introduction to Tag Data Links....6-4
6-1-5 Calculating the Number of Connections....6-9

6-2 I/O System....6-14
6-2-1 Relationship between the Types of Signals and the Types of Communications....6-14
6-2-2 Safety Data Types and Standard Data Types....6-14
6-2-3 Specifying Safety Data Types and Standard Data Types....6-15

6-3 Safety I/O Function....6-16
6-3-1 Safety Input Function....6-16
6-3-2 Safety Output Function....6-38

Section 7 Settings

7-1 Configuration and Setup Procedures 7-2

7-2 Part Names and Functions of the Sysmac Studio Window 7-3

7-3 CPU Rack Configuration and Setup 7-5
7-3-1 Procedures for Creating the CPU Rack Configuration 7-5
7-3-2 Setting and Viewing the NX Unit Settings 7-6
7-3-3 Setting Up the FSoE Communications 7-7

7-4 EtherNet/IP Network Configuration and Setup 7-9
7-4-1 Setting IP Addresses 7-9
7-4-2 Setting Tag Data Links 7-17

7-5 CIP Safety Communication Settings 7-21
7-5-1 Safety Network Number Settings for the NX Bus 7-21
7-5-2 Originator Connection Settings 7-22
7-5-3 Target I/O Assembly Settings 7-33
7-5-4 Connecting Target Devices of Other Manufacturers 7-35

7-6 Setting the Input and Output Functions 7-42
7-6-1 Safety I/O Functions 7-42
7-6-2 Setting the Standard Input and Output Functions 7-45

7-7 Assigning Variables to I/O Ports 7-46
7-7-1 Registering Device Variables 7-46
7-7-2 Settings of Communications between NX Units 7-51

7-8 Exposing Variables to Standard Controllers 7-53
7-8-1 Exposing Global Variables 7-53
7-8-2 Setting Exposed Variables 7-54
7-8-3 Safety CPU Unit Status 7-58
7-8-4 I/O Ports of Safety I/O Units 7-59
7-8-5 I/O Ports for Standard I/O Units 7-59

7-9 Exporting/Importing Settings Data 7-60
7-9-1 Exporting/Importing the All NX Unit Settings 7-60
7-9-2 Exporting/Importing Data for Individual Safety CPU Unit 7-62
7-9-3 Importing the Safety Unit Restore File 7-64

7-10 Offline Comparison 7-65
7-10-1 Procedure for Offline Comparison 7-65
7-10-2 Checking the Comparison Results 7-66
7-10-3 Detailed Comparison 7-67
7-10-4 Target Data of Offline Comparison 7-69

Section 8 Programming

8-1 POUs (Program Organization Units) 8-3
8-1-1 POU 8-3
8-1-2 Overview of the Three Types of POUs 8-3
8-1-3 Differences between Programs, Functions, and Function Blocks 8-4
8-1-4 Details on Programs 8-5
8-1-5 Details on Function Blocks 8-6
8-1-6 Details on Functions 8-10
8-1-7 Instructions 8-11

8-2 Variables 8-12
8-2-1 Variables 8-12
8-2-2 Types of Variables 8-12
8-2-3 Type of User-defined Variable 8-12
8-2-4 Attributes of Variables 8-13
8-2-5 Data Type 8-14
8-2-6 Variable Attributes Other Than Data Type 8-16
8-2-7 Function Block Instances 8-17

8-2-8 Restrictions on Variable Names and Other Safety Program-related Names....8-17

8-3 Constants (Literals)....8-20
8-3-1 Constants....8-20
8-3-2 Types of Constants....8-20

8-4 Programming Languages....8-22
8-4-1 Programming Languages....8-22
8-4-2 FBD Language....8-22

8-5 Programming Operations....8-27
8-5-1 Programming Layer on the Sysmac Studio....8-27
8-5-2 Registering POUs....8-28
8-5-3 Registering Variables....8-38
8-5-4 FBD Programming....8-46
8-5-5 Program Pattern Copy....8-67
8-5-6 Function Block Conversion for Programs....8-70
8-5-7 Building....8-71
8-5-8 Searching and Replacing....8-73
8-5-9 Safety Task Settings....8-76
8-5-10 Variable Comment Switching Function....8-78

8-6 Automatic Programming....8-87
8-6-1 Generation Algorithms for Automatic Programming....8-87
8-6-2 Automatic Programming Settings....8-90
8-6-3 Automatic Programming Execution Procedure....8-93

8-7 Monitoring Memory Usage for Communication Control Unit....8-97

8-8 Monitoring Memory Usage for Safety Control Unit....8-98

8-9 Offline Debugging....8-100
8-9-1 Offline Safety Program Debugging....8-100
8-9-2 Monitoring....8-103
8-9-3 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing....8-103
8-9-4 Cross References....8-103
8-9-5 Setting the Initial Values of Variables....8-103
8-9-6 Feedback Settings....8-104
8-9-7 Simple Automatic Test....8-105

Section 9 Checking Operation and Actual Operation

9-1 Procedures before Operation and Transferring the Required Data....9-3
9-1-1 Commissioning Procedure....9-3
9-1-2 Data That You Must Transfer before Operation and Data Transfer Procedures....9-4

9-2 Transferring the Configuration Information....9-6
9-2-1 Overview....9-6
9-2-2 Transfer Procedure....9-6

9-3 Operating Modes of the Safety CPU Unit....9-8
9-3-1 Startup Operating Mode and Changing the Operating Mode....9-8
9-3-2 Operation When Changing Operating Mode....9-10
9-3-3 Executable Functions in Each Mode of the Safety CPU Unit....9-11

9-4 Changing to DEBUG Mode....9-13

9-5 Checking External Device Wiring....9-16
9-5-1 Overview of Functions for Checking Wiring....9-16
9-5-2 Monitoring Safety I/O Units....9-16
9-5-3 Troubleshooting Safety I/O Terminals....9-19
9-5-4 Clear All Memory Operation for Safety I/O Units....9-20

9-6 Functions for Checking Operation....9-22
9-6-1 Overview of Functions for Checking Operation....9-22
9-6-2 Starting and Stopping the Safety Programs in DEBUG Mode....9-22
9-6-3 Monitoring Variables in the FBD Editor....9-23
9-6-4 Monitoring Variables in a Watch Tab Page....9-24

9-6-5 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing 9-26
9-6-6 Cross References 9-34

9-7 Online Functional Test 9-38
9-7-1 Online Functional Test Settings 9-38
9-7-2 Online Functional Test Execution Procedure 9-42

9-8 Search FB Where Safety Output Is OFF 9-48
9-8-1 Procedure for Operating Search FB Where Safety Output Is OFF 9-48
9-8-2 Editing Function Blocks to be Searched for 9-49
9-8-3 Registering a Data Type in the Function Block Search Settings Window 9-50

9-9 Node Name 9-52

9-10 Security Settings 9-53
9-10-1 Setting the Safety Password 9-53
9-10-2 Data Protection 9-54

9-11 Performing Safety Validation and Operation 9-59
9-11-1 Performing Safety Validation 9-59
9-11-2 Changing to RUN Mode 9-61
9-11-3 Changing to PROGRAM Mode 9-62

9-12 Starting and Stopping the Safety Application Monitoring 9-64
9-12-1 Procedure to Start and Stop the Safety Application Monitoring 9-64
9-12-2 Changing the Monitoring Options for the Safety Application 9-65

9-13 Uploading Configuration Information and Safety Application Data 9-66
9-13-1 Outline 9-66
9-13-2 Upload Procedures 9-66

9-14 Transferring Safety Application Data 9-68
9-14-1 Outline 9-68
9-14-2 Transfer Procedure 9-68

9-15 Monitoring Controller Status 9-70

9-16 Restarting and Clearing All Memory 9-72
9-16-1 Restarting 9-72
9-16-2 Clear All Memory Operation 9-72

Section 10 Calculating Safety Reaction Times

10-1 Safety Reaction Time 10-2
10-1-1 Calculating the Safety Reaction Time 10-2
10-1-2 Verifying Safety Reaction Times 10-4

10-2 Safety Task 10-5
10-2-1 Safety Task 10-5
10-2-2 Operation of Safety Task 10-5
10-2-3 Minimum Safety Task Period 10-5
10-2-4 Setting the Safety Task Period 10-6

10-3 FSoE Watchdog Timer 10-7
10-3-1 FSoE Watchdog Timers 10-7
10-3-2 Checking FSoE Watchdog Timers 10-7
10-3-3 Changing FSoE Watchdog Timers 10-7

10-4 EPI (Data Packet Interval) 10-9
10-4-1 Changing the EPI 10-9
10-4-2 EPI Restrictions 10-9

Section 11 Communications Load

11-1 Adjusting the Communications Load 11-2
11-1-1 Checking Bandwidth Usage for Tag Data Links 11-3
11-1-2 Checking the Device Bandwidth Usage of the CIP Safety Routing 11-4

11-1-3 Relationship between the Number of Packets Used per Second and Packet Intervals 11-5
11-1-4 Adjusting the Device Bandwidth Usage 11-5

Section 12 Safety Unit Restore

12-1 Safety Unit Restore 12-2
12-1-1 Generate Safety Unit Restore File Function 12-2
12-1-2 Safety Unit Restore Function 12-3
12-1-3 Specifications of a Safety Unit Restore File 12-5

Section 13 Backup Functions of the Communication Control Unit

13-1 The Backup Functions 13-2
13-1-1 Applications of Backup Functions 13-2
13-1-2 Examples of Operating Procedures for the Backup Functions 13-2
13-1-3 Data that Is Backed Up 13-4
13-1-4 Types of Backup Functions 13-5
13-1-5 Relation between the Different Types of Backup Functions and Data Groups 13-7
13-1-6 Applicable Range of the Backup Functions 13-8
13-2 SD Memory Card Backups 13-10
13-2-1 Backup (Controller to SD Memory Card) 13-10
13-2-2 Restore (SD Memory Card to Controller) 13-12
13-2-3 Verify (between Controller and SD Memory Card) 13-13
13-3 Disabling Backups to SD Memory Cards 13-15
13-4 Sysmac Studio Controller Backups 13-16
13-4-1 Backup (Controller to Computer) 13-16
13-4-2 Restore (Computer to Controller) 13-17
13-4-3 Verify (between Controller and Computer) 13-18
13-5 Importing and Exporting Sysmac Studio Backup File Data 13-20
13-6 Backup Functions when NX Units are Connected 13-21
13-6-1 Backing Up Data in NX Units on the Communication Control Unit 13-21
13-6-2 Backup Support Depending on the Controller Status 13-21
13-6-3 Conditions for Restoring NX Unit Data on the Communication Control Unit 13-22
13-7 Backup-related Files 13-23
13-7-1 Types of Backup-related Files 13-23
13-7-2 Specifications of a Backup File 13-23
13-7-3 Specifications of a Restore Command File 13-24
13-7-4 Specifications of a Controller Verification Results File 13-25
13-7-5 Specifications of an NX Unit Verification Results File 13-26
13-8 Compatibility between Backup-related Files 13-28
13-8-1 Compatibility between Backup Functions 13-28
13-9 Functions That Cannot Be Executed during Backup Functions 13-29

Section 14 Safety Data Logging

14-1 Outline of the Safety Data Logging Function 14-2
14-2 Creating a Safety Data Logging Settings File with the Sysmac Studio 14-4
14-3 Safety Data Logging Operation Procedure 14-6
14-4 Checking the Logging Status 14-7
14-4-1 Checking the Seven-segment Indicator 14-7
14-4-2 Checking with System-defined Variables 14-7
14-5 Log File Specifications 14-9

Section 15 Troubleshooting

15-1 Operation after an Error 15-2
15-1-1 Overview of Communication Control Unit Status 15-2
15-1-2 Fatal Errors 15-4
15-1-3 Non-fatal Errors in the Communication Control Unit 15-6
15-1-4 Checking for Non-fatal Errors 15-15
15-1-5 Resetting Non-fatal Errors 15-17
15-1-6 Errors Related to the EtherNet/IP Function Module 15-19
15-1-7 Errors Related to Safety Control Units 15-20
15-1-8 Errors on CIP Safety Target Devices 15-21

15-2 Error Troubleshooting Methods 15-23
15-2-1 Troubleshooting Flowcharts 15-23
15-2-2 Troubleshooting Fatal Errors 15-24
15-2-3 Troubleshooting Non-fatal Errors 15-25
15-2-4 Troubleshooting When You Cannot Go Online from the Sysmac Studio 15-31
15-2-5 Troubleshooting Errors in the Safety Control Unit 15-35
15-2-6 Troubleshooting the CIP Safety Target Device Errors 15-43

15-3 Error Descriptions and Corrections 15-48
15-3-1 Interpreting Tables 15-48
15-3-2 Communication Control Unit Error 15-51
15-3-3 Safety CPU Unit Error 15-167
15-3-4 Safety I/O Unit Error 15-213
15-3-5 Other Troubles and Corrections 15-240

15-4 Checking Status with the Network Configurator 15-241
15-4-1 The Network Configurator's Device Monitor Function 15-241
15-4-2 Connection Status Codes and Troubleshooting 15-249
15-4-3 CIP Safety Connection Status Codes and Troubleshooting 15-257

Section 16 Inspection and Maintenance

16-1 Cleaning and Inspection 16-2
16-1-1 Cleaning 16-2
16-1-2 Periodic Inspections 16-2

16-2 Maintenance Procedures 16-5
16-2-1 Replacing the Communication Control Unit and the Safety CPU Unit 16-5
16-2-2 Replacing Safety I/O Units 16-6

Appendices

A-1 General Specifications A-3

A-2 Dimensions A-4
A-2-1 Communication Control Unit A-4
A-2-2 Safety CPU Unit A-5
A-2-3 Safety I/O Units A-5
A-2-4 End Cover A-6
A-2-5 SD Memory Card A-6

A-3 NX Objects A-7
A-3-1 Format of NX Object Descriptions A-7
A-3-2 Safety CPU Unit A-7
A-3-3 NX-SID800 Safety Input Unit A-11
A-3-4 NX-SIH400 Safety Input Unit A-16
A-3-5 NX-SOD400 Safety Output Unit A-21
A-3-6 NX-SOH200 Safety Output Unit A-25

A-4 Application Examples A-30
A-4-1 Emergency Stop Pushbutton Switches A-30
A-4-2 Safety Doors A-32

A-4-3 Safety Laser Scanners ... A-36
A-4-4 Safety Door Switches with Magnetic Locks and Key Selector Switches ... A-39
A-4-5 Enable Switches ... A-43
A-4-6 Two-hand Switches ... A-47
A-4-7 D40A Non-contact Door Switches ... A-50
A-4-8 D40A-2/D40Z Non-contact Door Switches ... A-53
A-4-9 Safety Mats and Safety Light Curtains ... A-56
A-4-10 Safety Edges ... A-61
A-4-11 Single Beam Safety Sensor ... A-63

A-5 Change Tracking ... A-67

A-6 Safety CPU Unit Status ... A-69

A-7 I/O Ports of Safety I/O Units ... A-71
A-7-1 NX-SIH400 Safety Input Unit ... A-71
A-7-2 NX-SID800 Safety Input Unit ... A-73
A-7-3 NX-SOH200 Safety Output Unit ... A-74
A-7-4 NX-SOD400 Safety Output Unit ... A-75

A-8 CIP Response Codes ... A-78
A-8-1 General Status Codes ... A-78
A-8-2 Extended Status Codes ... A-80

A-9 Icon list for Safety Slave Unit Parameters ... A-83
A-9-1 External Device Icons for Input Devices ... A-83
A-9-2 Contact Icons for Input Devices ... A-87
A-9-3 External Device Icons for Output Devices ... A-89
A-9-4 Contact Icons for Output Devices ... A-90

A-10 Printing ... A-91
A-10-1 Selecting the Items to Print ... A-91
A-10-2 Items that are Printed ... A-91

A-11 List of Screwless Clamping Terminal Block Models ... A-93
A-11-1 Model Notation ... A-93
A-11-2 List of Terminal Block Models ... A-93

A-12 I/O Refreshing between NX Units ... A-95
A-12-1 I/O Refreshing from the Communication Control Unit to NX Units ... A-95
A-12-2 Methods of I/O Refreshing between the Communication Control Unit and NX Units ... A-95
A-12-3 I/O Response Time for Communications between NX Units ... A-101

A-13 Units That Support Communications between NX Units ... A-103

A-14 Checking the Signature Code on the Seven-segment Indicator ... A-104

A-15 Execution Scenarios for the Simple Automatic Test ... A-105

A-16 Differences in Checking Operation between the Simulator and Safety CPU Unit ... A-108

A-17 I/O Data Enable Flag for CIP Safety Connections ... A-109

A-18 Safety: Update Configurations and Setup Transfer Data ... A-111

A-19 CIP Safety Target Device Operation ... A-112

A-20 Version Information ... A-115
A-20-1 Relationship between the Unit Versions and Sysmac Studio Versions ... A-115

Index

Relevant Manuals

The following table provides the relevant manuals for this product. Read all of the manuals that are relevant to your system configuration and application before you use the product.
Most operations on this product are performed from the Sysmac Studio Automation Software. For details on the Sysmac Studio, refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)*.

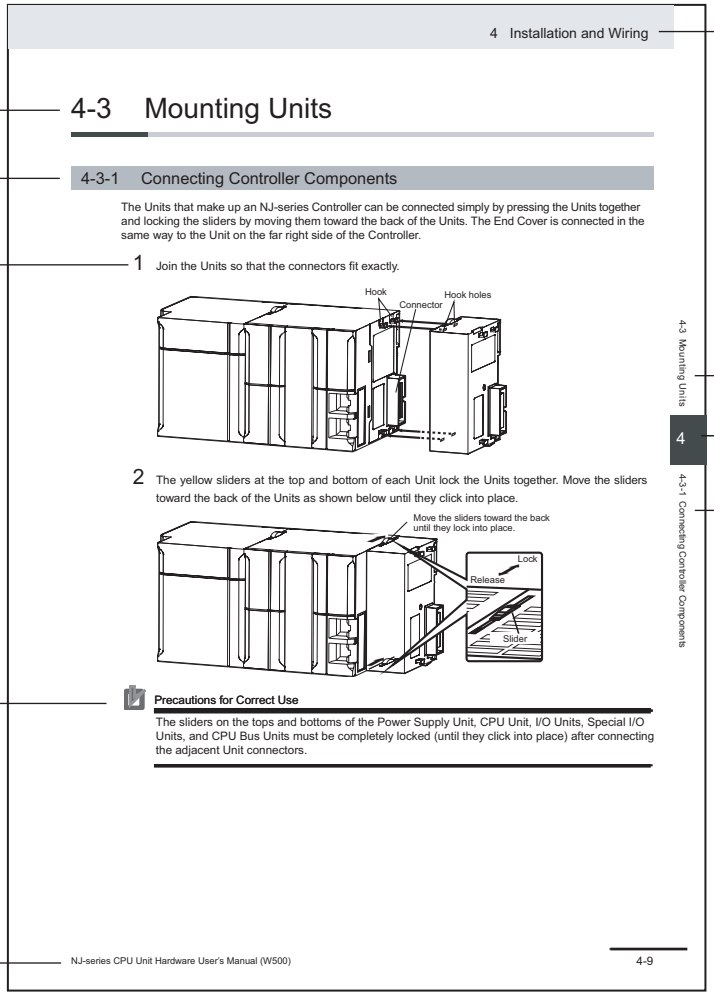
Purpose of use	NX-series Safety Control Unit User's Manual	NX-series Safety Control Unit / Communication Control Unit User's Manual	NX-series Communication Control Unit Built-in Function User's Manual	NX-series Safety Control Unit Instructions Reference Manual
Building a safety control system integrated with NJ/NX-series CPU Units	●			
Building a standalone safety control system with EtherNet/IP Coupler Units	●			
Building a safety network control system with Communication Control Units		●		
Introduction to Communication Control Unit	●	●		
Setting devices and hardware				
NX-SL5□□□ Safety CPU Unit	●	●		
NX-SL3□□□ Safety CPU Unit	●			
NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
NX-CSG□□□ Communication Control Unit		●		
Software settings				
NX-SL5□□□ Safety CPU Unit	●	●		
NX-SL3□□□ Safety CPU Unit	●			
NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
NX-CSG□□□ Communication Control Unit		●	●	
Creating safety programs	●	●		●
Testing operation and debugging				
Safety programs	●	●		●
Safety process data communications	●	●		
Safety I/O functions	●	●		
Tag data links		●		
Built-in functions for Communication Control Unit		●	●	
Learning about error corrections				
NX-SL5□□□ Safety CPU Unit	●	●		●
NX-SL3□□□ Safety CPU Unit	●			●
NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
NX-CSG□□□ Communication Control Unit		●		
Maintenance				

Purpose of use		NX-series Safety Control Unit User's Manual	NX-series Safety Control Unit / Communication Control Unit User's Manual	NX-series Communication Control Unit Built-in Function User's Manual	NX-series Safety Control Unit Instructions Reference Manual
	NX-SL5□□□ Safety CPU Unit	●	●		
	NX-SL3□□□ Safety CPU Unit	●			
	NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
	NX-CSG□□□ Communication Control Unit		●		

Manual Structure

Page Structure

The following page structure is used in this manual.



This illustration is provided only as a sample. It may not literally appear in this manual.

Special Information

Special information in this manual is classified as follows:

Precautions for Safe Use

Precautions on what to do and what not to do to ensure safe usage of the product.

Precautions for Correct Use

Precautions on what to do and what not to do to ensure proper operation and performance.

Additional Information

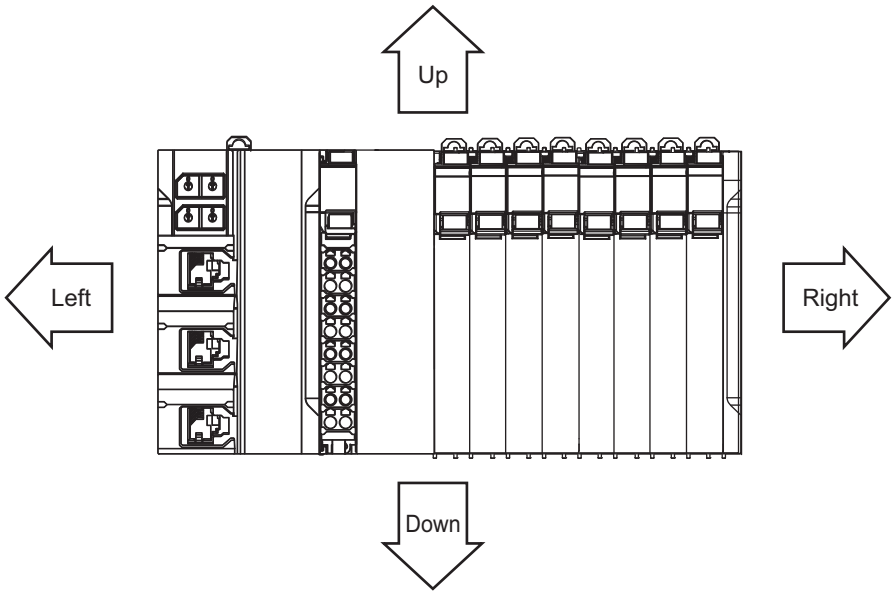
Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality for Controller with different unit versions and for different versions of the Sysmac Studio is given.

Precaution on Terminology

In this manual, the directions in relation to the Units are given in the following figure, which shows upright installation.



Terms and Conditions Agreement

Warranty, Limitations of Liability

Warranties

- **Exclusive Warranty**

  Omron's exclusive warranty is that the Products will be free from defects in materials and workmanship for a period of twelve months from the date of sale by Omron (or such other period expressed in writing by Omron). Omron disclaims all other warranties, express or implied.

- **Limitations**

  OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, ABOUT NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE PRODUCTS. BUYER ACKNOWLEDGES THAT IT ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE.

  Omron further disclaims all warranties and responsibility of any type for claims or expenses based on infringement by the Products or otherwise of any intellectual property right.

- **Buyer Remedy**

  Omron's sole obligation hereunder shall be, at Omron's election, to (i) replace (in the form originally shipped with Buyer responsible for labor charges for removal or replacement thereof) the non-complying Product, (ii) repair the non-complying Product, or (iii) repay or credit Buyer an amount equal to the purchase price of the non-complying Product; provided that in no event shall Omron be responsible for warranty, repair, indemnity or any other claims or expenses regarding the Products unless Omron's analysis confirms that the Products were properly handled, stored, installed and maintained and not subject to contamination, abuse, misuse or inappropriate modification. Return of any Products by Buyer must be approved in writing by Omron before shipment. Omron Companies shall not be liable for the suitability or unsuitability or the results from the use of Products in combination with any electrical or electronic components, circuits, system assemblies or any other materials or substances or environments. Any advice, recommendations or information given orally or in writing, are not to be construed as an amendment or addition to the above warranty.

  See https://www.omron.com/global/ or contact your Omron representative for published information.

Limitation on Liability; Etc

OMRON COMPANIES SHALL NOT BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR PRODUCTION OR COMMERCIAL LOSS IN ANY

WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY.

OMRON SHALL NOT BE RESPONSIBLE AND/OR LIABLE FOR ANY LOSS, DAMAGE, OR EXPENSES DIRECTLY OR INDIRECTLY RESULTING FROM THE INFECTION OF OMRON PRODUCTS, ANY SOFTWARE INSTALLED THEREON OR ANY COMPUTER EQUIPMENT, COMPUTER PROGRAMS, NETWORKS, DATABASES OR OTHER PROPRIETARY MATERIAL CONNECTED THERETO BY DISTRIBUTED DENIAL OF SERVICE ATTACK, COMPUTER VIRUSES, OTHER TECHNOLOGICALLY HARMFUL MATERIAL AND/OR UNAUTHORIZED ACCESS.

It shall be the users sole responsibility to determine and use adequate measures and checkpoints to satisfy the users particular requirements for (i) antivirus protection, (ii) data input and output, (iii) maintaining a means for reconstruction of lost data, (iv) preventing Omron Products and/or software installed thereon from being infected with computer viruses and (v) protecting Omron Products from unauthorized access.

Further, in no event shall liability of Omron Companies exceed the individual price of the Product on which liability is asserted.

Application Considerations

Suitability of Use

Omron Companies shall not be responsible for conformity with any standards, codes or regulations which apply to the combination of the Product in the Buyer’s application or use of the Product. At Buyer’s request, Omron will provide applicable third party certification documents identifying ratings and limitations of use which apply to the Product. This information by itself is not sufficient for a complete determination of the suitability of the Product in combination with the end product, machine, system, or other application or use. Buyer shall be solely responsible for determining appropriateness of the particular Product with respect to Buyer’s application, product or system. Buyer shall take application responsibility in all cases.

NEVER USE THE PRODUCT FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY OR IN LARGE QUANTITIES WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT(S) IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

Programmable Products

Omron Companies shall not be responsible for the user’s programming of a programmable Product, or any consequence thereof.

Disclaimers

Performance Data

Data presented in Omron Company websites, catalogs and other materials is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of Omron's test conditions, and the user must correlate it to actual application requirements. Actual performance is subject to the Omron's Warranty and Limitations of Liability.

Change in Specifications

Product specifications and accessories may be changed at any time based on improvements and other reasons. It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without any notice. When in doubt, special part numbers may be assigned to fix or establish key specifications for your application. Please consult with your Omron's representative at any time to confirm actual specifications of purchased Product.

Errors and Omissions

Information presented by Omron Companies has been checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical or proofreading errors or omissions.

Statement of security responsibilities for assumed use cases and against threats

OMRON SHALL NOT BE RESPONSIBLE AND/OR LIABLE FOR ANY LOSS, DAMAGE, OR EXPENSES DIRECTLY OR INDIRECTLY RESULTING FROM THE INFECTION OF OMRON PRODUCTS, ANY SOFTWARE INSTALLED THEREON OR ANY COMPUTER EQUIPMENT, COMPUTER PROGRAMS, NETWORKS, DATABASES OR OTHER PROPRIETARY MATERIAL CONNECTED THERETO BY DISTRIBUTED DENIAL OF SERVICE ATTACK, COMPUTER VIRUSES, OTHER TECHNOLOGICALLY HARMFUL MATERIAL AND/OR UNAUTHORIZED ACCESS.

It shall be the users sole responsibility to determine and use adequate measures and checkpoints to satisfy the users particular requirements for (i) antivirus protection, (ii) data input and output, (iii) maintaining a means for reconstruction of lost data, (iv) preventing Omron Products and/or software installed thereon from being infected with computer viruses and (v) protecting Omron Products from unauthorized access.

Safety Precautions

Definition of Precautionary Information

The following notation is used in this manual to provide precautions required to ensure safe usage of the NX-series Safety Control Unit / Communication Control Unit. The safety precautions that are provided are extremely important to safety. Always read and heed the information provided in all safety precautions.
The following notation is used.

⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. Additionally, there may be severe property damage.
⚠ Caution	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, or property damage.

Symbols

	The circle and slash symbol indicates operations that you must not do. The specific operation is shown in the circle and explained in text. This example indicates prohibiting disassembly.
	The triangle symbol indicates precautions (including warnings). The specific operation is shown in the triangle and explained in text. This example indicates a precaution for electric shock.
	The triangle symbol indicates precautions (including warnings). The specific operation is shown in the triangle and explained in text. This example indicates a general precaution.
	The filled circle symbol indicates operations that you must do. The specific operation is shown in the circle and explained in text. This example shows a general precaution for something that you must do.

Warnings

Serious injury may possibly occur due to loss of required safety functions.
When building the system, observe the following warnings to ensure the integrity of the safety-related components.

⚠ WARNING

Setting Up a Risk Assessment System

The process of selecting these products should include the development and execution of a risk assessment system early in the design development stage to help identify potential dangers in your equipment and optimize safety product selection.
Related International Standards:
- ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction

Protective Measure

When developing a safety system for the equipment and devices that use safety products, make every effort to understand and conform to the entire series of international and industry standards available, such as the examples given below.
Related International Standards:
- ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction
- IEC 60204-1 Electrical Equipment of Machines - Part 1: General Requirements
- ISO 13849-1, -2 Safety-related Parts of Control Systems
- ISO 14119 Interlocking Devices Associated with Guards - Principles for Design and Selection
- IEC 62046 Application of Protective Equipment to Detect the Presence of Persons
- IEC 62061 Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems
- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

Role of Safety Products

Safety products incorporate standardized safety functions and mechanisms, but the benefits of these functions and mechanisms are designed to attain their full potential only within properly designed safety-related systems. Make sure you fully understand all functions and mechanisms, and use that understanding to develop systems that will ensure optimal usage.
Related International Standards:
- ISO 14119 Interlocking Devices Associated with Guards - Principles for Design and Selection
- ISO 13857 Safety Distances to Prevent Hazard Zones being Reached by Upper and Lower Limbs

Installing Safety Products

Qualified engineers must develop your safety-related system and install safety products in devices and equipment. Prior to machine commissioning verify through testing that the safety products works as expected.
Related International Standards:

- ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction
- IEC 60204-1 Electrical Equipment of Machines - Part 1: General Requirements
- ISO 13849-1, -2 Safety-related Parts of Control Systems
- ISO 14119 Interlocking Devices Associated with Guards - Principles for Design and Selection
- IEC 62061 Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems
- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems



Observing Laws and Regulations

Safety products must conform to pertinent laws, regulations, and standards. Make sure that they are installed and used in accordance with the laws, regulations, and standards of the country where the devices and equipment incorporating these products are distributed.



Observing Usage Precautions

Carefully read the specifications and precautions as well as all items in the Instruction Manual for your safety product to learn appropriate usage procedures. Any deviation from instructions will lead to unexpected device or equipment failure not anticipated by the safety-related system.



Transferring Devices and Equipment

When transferring devices and equipment, be sure to retain one copy of the Instruction Manual and supply another copy with the device or equipment so the person receiving it will have no problems with operation and maintenance.
Related International Standards:

- ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction
- IEC 60204-1 Electrical Equipment of Machines - Part 1: General Requirements
- ISO 13849-1, -2 Safety-related Parts of Control Systems
- IEC 62061 Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems
- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems



Design

Confirm that the calculated reaction times meet the required specifications for all safety chains.
Serious injury may possibly occur due to loss of required safety functions.



All safety devices and components that are connected to an NX-series Safety Control Unit must be selected and used to meet the required level of safety and the relevant safety category.
Serious injury may possibly occur due to loss of required safety functions.



Do not use indicators on the NX-series Safety Control Units for safety operations.
Serious injury may possibly occur due to loss of required safety functions.



Check during the import of the program that the CRC of the program is correct.
Serious injury may possibly occur due to loss of required safety functions.



Check during the import of the user defined function that the CRC of the imported function block is correct.
Serious injury may possibly occur due to loss of required safety functions.



Do not use non-safety signals, including tag data links, explicit messages, and exposed variables, as safety signals.
Serious injury may possibly occur due to loss of required safety functions.



If you select “Open Only” for the Open Type setting, make sure to verify that the originator/target have correct configurations.
Serious injury may possibly occur due to loss of required safety functions.



Before connecting an NX Series Safety Control Unit to the network, clear the previous settings.
Serious injury may possibly occur due to loss of required safety functions.



Before you connect the Communication Control Unit to the network, set the appropriate IP address and communication speed settings.
Serious injury may possibly occur due to loss of required safety functions.



Debugging

Before you perform safety validation of the safety programs, complete debugging of the safety programs.
Otherwise, the Safety CPU Unit will start with safety programs that are not fully debugged and may cause serious personal injury.



Make sure that the area around the system is safe before you change the operating mode, change present values, or execute forced refreshing. The outputs may operate and may cause serious injury.



Make sure that the area around the system is safe before you start the system operation while the online functional test is in progress. The outputs may operate and may cause serious injury.



Testing Operation

Before you start the system, perform user testing to make sure that all safety devices operate correctly. The safety signature is validated upon completion of the user testing.
Serious injury may possibly occur due to loss of required safety functions.



After you perform safety validation, check items for safety validation printed out to confirm Safety Control Units are correctly configured.



Although the Simulator and Simple Automatic Test simulate the operation of the Safety CPU Unit, there are differences from the Safety CPU Unit in operation and timing. Always confirm operation on the actual equipment before you operate the equipment.
Accidents may occur if the controlled system performs unexpected operation.



Wiring

Wire the safety input and output lines so that they do not touch other lines.
Serious injury may possibly occur due to loss of required safety functions.



Wire the Safety Control Unit properly so that 24-VDC lines do not touch output lines accidentally or unintentionally.
Serious injury may possibly occur due to loss of required safety functions.



Wire the safety output lines and 24-VDC lines so that ground faults will not cause the loads to turn ON.
Serious injury may possibly occur due to loss of required safety functions.



The wiring information that is displayed on the Sysmac Studio is for reference only and may differ from the actual wiring diagrams. Always confirm the actual wiring and performing suitable wiring.
Serious injury may possibly occur due to loss of required safety functions.



During Power Supply

Do not touch any of the terminals or terminal blocks while the power is being supplied.
Doing so may result in electric shock.



Do not attempt to take any Unit apart.
In particular, high-voltage parts are present in Units that supply power while power is supplied or immediately after power is turned OFF. Touching any of these parts may result in electric shock.
There are sharp parts inside the Unit that may cause injury.



Replacing Units

When replacing a Safety Control Unit, confirm that the model of the Unit is correct, confirm that the Unit and terminal block mounting positions are correct, configure the replacement Unit suitably, and confirm that the Unit operates correctly.



Voltage and Current Inputs

Make sure that the voltages and currents that are input to the Units and slaves are within the specified ranges.
Inputting voltages or currents that are outside of the specified ranges may cause accidents or fire.



Transferring

Always confirm safety at the destination before you transfer the unit configuration information, parameters, set values, or other data from tools such as the Sysmac Studio.
The devices or machines may perform unexpected operation regardless of the operating mode of the Controller.



Restoring Data

When you restore the Safety CPU Unit, confirm that the safety signature for the restored programs is correct. Serious injury may possibly occur due to loss of required safety functions.



Fail-safe Measures

Provide safety measures in external circuits to ensure safety in the system if an abnormality occurs due to malfunction of the Communication Control Unit, slaves, or Units or due to other external factors affecting operation. Not doing so may result in serious accidents due to incorrect operation.



Emergency stop circuits, interlock circuits, limit circuits, and similar safety measures must be provided in external control circuits.



The outputs may remain ON or OFF due to deposition or burning of the output relays or destruction of the output transistors. As a countermeasure for such problems, external safety measures must be provided to ensure safe operation of the system.



The Communication Control Unit will turn OFF digital outputs on the CPU Rack in the following cases:

- While the Communication Control Unit is on standby until RUN mode is entered after the power is turned ON.
- If an error occurs in the power supply.
- If a system initialization error occurs.

Digital outputs on the CPU Rack will produce outputs according to the settings in the following cases.

- If a CPU error or CPU reset occurs.
- If a major fault level Controller error occurs.

External safety measures must be provided to ensure safe operation of the system in such cases.



If there is interference in remote I/O communications or if a major fault level error occurs, output status will depend on the products that are used.
Confirm the operation that will occur when there is interference in communications or a major fault level error, and implement safety measures.
Correctly set all of the settings in the slaves and Units.



If external power supplies for Units, slaves or other devices are overloaded or short-circuited, the voltage will drop, outputs will turn OFF, and the system may be unable to read inputs. Provide external safety measures in controls with monitoring of external power supply voltage as required so that the system operates safely in such a case.



Unintended outputs may occur when an error occurs in variable memory. As a countermeasure for such problems, external safety measures must be provided to ensure safe operation of the system.



Provide measures in the communications system and user program to ensure safety in the overall system even if errors or malfunctions occur in data link communications or remote I/O communications.



The NX-series Controller continues normal operation for a certain period of time when a momentary power interruption occurs. This means that the NX-series Controller may receive incorrect signals from external devices that are also affected by the power interruption.
Accordingly, take suitable actions, such as external fail-safe measures and interlock conditions, to monitor the power supply voltage of the external device as required.



You must take fail-safe measures to ensure safety in the event of incorrect, missing, or abnormal signals caused by broken signal lines, momentary power interruptions, or other causes.
Not doing so may result in serious accidents due to incorrect operation.



Security Measures

Anti-virus protection
Install the latest commercial-quality antivirus software on the computer connected to the control system and maintain to keep the software up-to-date.



Security measures to prevent unauthorized access
Take the following measures to prevent unauthorized access to our products.

- Install physical controls so that only authorized personnel can access control systems and equipment.
- Reduce connections to control systems and equipment via networks to prevent access from untrusted devices.
- Install firewalls to shut down unused communications ports and limit communications hosts and isolate control systems and equipment from the IT network.
- Use a virtual private network (VPN) for remote access to control systems and equipment.
- Adopt multifactor authentication to devices with remote access to control systems and equipment.
- Set strong passwords and change them frequently.
- Scan virus to ensure safety of USB drives or other external storages before connecting them to control systems and equipment.



Data input and output protection Validate backups and ranges to cope with unintentional modification of input/output data to control systems and equipment. • Checking the scope of data • Checking validity of backups and preparing data for restore in case of falsification and abnormalities • Safety design, such as emergency shutdown and fail-soft operation in case of data tampering and abnormalities	
Data recovery Backup data and keep the data up-to-date periodically to prepare for data loss.	
When using an intranet environment through a global address, connecting to an unauthorized terminal such as a SCADA, HMI or to an unauthorized server may result in network security issues such as spoofing and tampering. You must take sufficient measures such as restricting access to the terminal, using a terminal equipped with a secure function, and locking the installation area by yourself.	
When constructing an intranet, communication failure may occur due to cable disconnection or the influence of unauthorized network equipment. Take adequate measures, such as restricting physical access to network devices, by means such as locking the installation area.	
When using a device equipped with the SD Memory Card function, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing the removable media or unmounting the removable media. Please take sufficient measures, such as restricting physical access to the Controller or taking appropriate management measures for removable media, by means of locking the installation area, entrance management, etc., by yourself.	

Cautions

⚠ Caution

Application

Do not touch any Unit when power is being supplied or immediately after the power supply is turned OFF. Doing so may result in burn injury.



Wiring

Be sure that all terminal screws and cable connector screws are tightened to the torque specified in the relevant manuals. Loose screws may result in fire or malfunction.



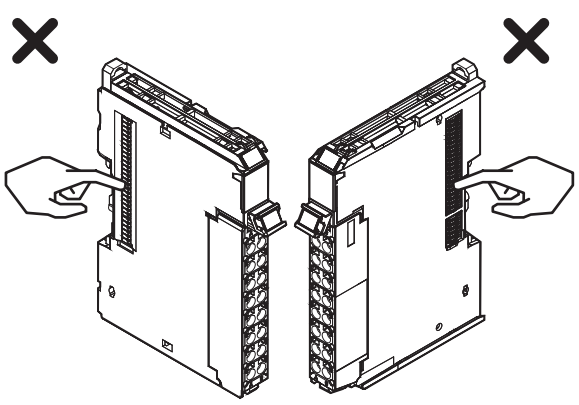
Precautions for Safe Use

Transporting

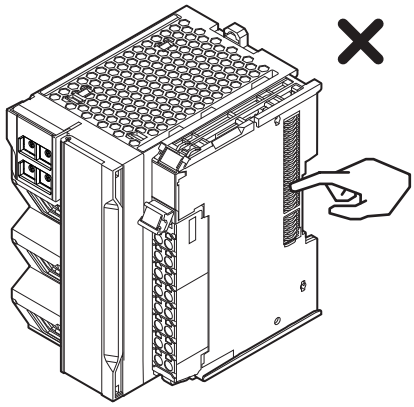
- Do not attempt to disassemble, repair, or modify any Units. Doing so may result in malfunction or fire.
- Do not drop any Unit or subject it to abnormal vibration or shock. Doing so may result in Unit malfunction or burning.
- When transporting any Unit, use the special packing box for it. Also, do not subject the Unit to excessive vibration or shock during transportation.

Mounting

- Always turn OFF the power supply before mounting a Unit. If the power supply is not OFF, the Unit may malfunction or may be damaged.
- Mount terminal blocks and connectors only after checking the mounting location carefully. Be sure that the terminal blocks, expansion cables, and other items with locking devices are properly locked into place.
- Do not apply labels or tape to the Unit. When the Units are installed or removed, adhesive or scraps may adhere to the pins in the NX bus connector, which may result in malfunctions.
- Do not touch the pins in the NX bus connector on the Unit. Dirt may adhere to the pins in the NX bus connector, which may result in malfunctions.

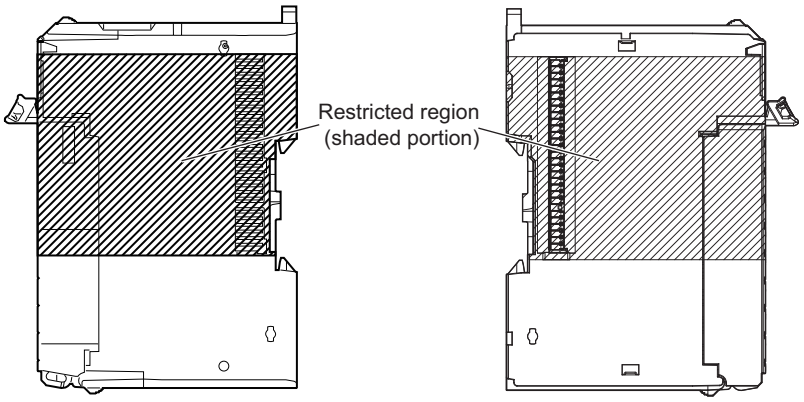


Example: NX Units (12 mm wide)



Communication Control Unit

- Do not write on the Communication Control Unit or an NX Unit with ink within the restricted region that is shown in the following figure. Also do not get this area dirty. When the Unit is installed or removed, ink or dirt may adhere to the pins in the NX bus connector, which may result in malfunctions in the Controller.



- The End Cover has a metal portion and is heavier than it looks. Be careful not to drop it when handling.

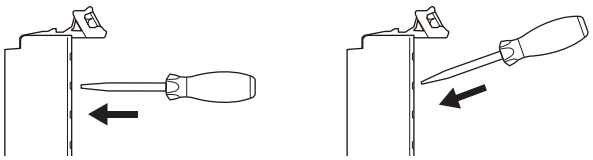
Installation

- Always connect to a ground of 100 Ω or less when installing the Units.

Wiring

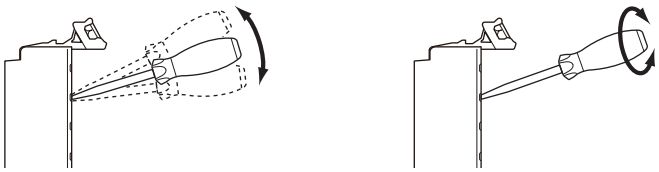
- Follow the instructions in this manual to correctly perform wiring.
- Double-check all switch settings to make sure that they are correct before turning ON the power supply.
- Use the methods that are specified in this manual for wiring the terminal blocks.
- Use crimp terminals for wiring the M3 screw terminal blocks. Do not connect bare stranded wires directly to the M3 screw terminal blocks.
- Use the correct wiring parts and tools when you wire the system. Otherwise, cables may be disconnected to cause short-circuit or wire breakage.
- Do not pull on the cables or bend the cables beyond their natural limit. Do not place any heavy objects on the cables or other wiring lines. Doing so may severe the cables.
- When wiring or installing the Units, do not allow metal fragments to enter the Units.
- Mount terminal blocks and connectors only after checking the mounting location carefully.
- Be sure that the terminal blocks, communications cables, and other items with locking devices are properly locked into place.
- If the external power supply to a Output Unit or slave has polarity, connect it with the correct polarity. If the polarity is reversed, current may flow in the reverse direction and damage the connected devices regardless of the operation of the Controller.
- Do not press the flat-blade screwdriver straight into the release hole on the screwless clamping terminal block. Doing so may damage the terminal block.

NG OK



- When you insert a flat-blade screwdriver into a release hole on the screwless clamping terminal block, press the screwdriver down with a force of 30 N or less. Applying excessive force may damage the terminal block.
- Do not tilt or twist the flat-blade screwdriver while it is pressed into the release hole on the screwless clamping terminal block. Doing so may damage the terminal block.

NG NG



Power Supply Design

- Select an external power supply with sufficient capacity by considering the power supply capacity or inrush current when the power is turned ON that is specified in this manual.
  Otherwise, the external power supply may not be turned ON or malfunction due to unstable power supply voltage.
- Use the I/O power supply current at 4 A or less. Using the currents that are outside of the specifications may cause failure or damage.
- Do not apply voltages or connect loads to the Output Units or slaves in excess of the rated value.
- Surge current occurs when the power supply is turned ON. When selecting fuses or breakers for external circuits, consider the above precaution and allow sufficient margin in shut-off performance. Refer to this manual for surge current specifications.
- If the full dielectric strength voltage is applied or turned OFF using the switch on the tester, the generated impulse voltage may damage the Power Supply Unit. Use the adjustment on the tester to gradually increase and decrease the voltage.
- Install external breakers and take other safety measures against short-circuiting and overcurrents in external wiring.
- Use the I/O power supply capacity within the range that is given in the Unit specifications.
- Provide suitable power supply capacity according to the reference manuals.
- Use the power supply voltage that is specified in the related manuals.
- Do not apply voltages that exceed the rated value to any Input Unit.

Debugging

- With forced refreshing, the values of variables are overwritten with specified values and then the safety programs are executed. If forced refreshing is used for variables that give the results of program processing, the variables will first take the specified values, but they will then be overwritten by the safety program.
- Depending on the difference in the forced status, the control system may operate unexpectedly.
- After you clear the memory, the Controller operates in the same way as immediately after you create the system configuration with the Controller in the factory default condition.
- Verify that the safety communications with a remote node will be established in the debug mode of the Safety CPU Unit.

Turning ON the Power Supply or Restarting after Safety Validation

- Remember that if safety validation is successful, the next time the Safety CPU Unit is started, it will automatically start in RUN mode.
- When you download the parameters for the Communication Control Unit and NX Units, the Safety CPU Unit automatically restarts.

Turning ON the Power Supply

- Double-check all wiring connections and switch settings to make sure that they are correct before turning ON the power supply. Use the correct wiring parts and tools when you wire the system.
- Make sure that the voltages and currents that are input to the Units and slaves are within the specified ranges. Inputting voltages or currents that are outside of the specified ranges may damage the Units or slaves or cause fire.
- It takes approximately 20 seconds for the Communication Control Unit to start up after the power supply is turned ON. During that time, digital outputs on the CPU Rack will be OFF. Note that the slave outputs will behave according to the setting values.
  Use the system-defined variables and the NX Unit device variables in the user program to confirm that I/O data communications are established before attempting control operations. During the start-up process, communications with external devices will not be established.
- Configure the external circuits so that the power supply to the control system turns ON only after the power supply to the Controller has turned ON. If the power supply to the Controller is turned ON after the control power supply, temporary errors may result in incorrect control system signals because the output terminals on Output Units may momentarily turn ON when power supply is turned ON to the Controller.
- You cannot obtain normal input data from NX Units while the Units are restarting. Use device variables for the NX bus master of the Communication Control Unit in the user program to check the validity of the I/O data before you attempt control operations.

Actual Operation

- The relevant Units will maintain the safe states for I/O data with safety connections after an error is detected in safety process data communications. However, when the cause of the error is removed, safety process data communications will recover automatically.

If you need to prevent equipment from restarting when safety process data communications recover automatically, implement suitable restart conditions in the user program.

- If you change the fail-soft operation setting, the output status when the error occurs may also change. Confirm safety before you change the setting.
- If you use fail-soft operation, write programming to determine whether Unit I/O data is valid. Without such programming, the user program cannot distinguish between Units for which I/O refreshing is continued and Units for which I/O refreshing is stopped.

Turning OFF the Power Supply

- Never turn OFF the power supply to the Controller when the BUSY indicator is flashing. While the BUSY indicator is lit, the settings in the Communication Control Unit are being backed up in the built-in non-volatile memory. This data will not be backed up correctly if the power supply is turned OFF. Also, a major fault level Controller error will occur the next time you start operation, and operation will stop.
- Do not turn OFF the power supply or remove the SD Memory Card while SD Memory Card access is in progress (i.e., while the SD BUSY indicator flashes). Data may become corrupted, and the Controller will not operate correctly if it uses corrupted data. To remove the SD Memory Card from the Communication Control Unit while the power supply is ON, press the SD Memory Card power supply switch first. Make sure that the SD BUSY Indicator and the SD PWR Indicator are turned OFF before you remove the SD Memory Card.
- If the Unit power supply is turned OFF before the I/O power supply for the control system is turned OFF, the output terminals of Output Units may malfunction and the control system may perform incorrect output temporarily. To avoid this problem, configure the external circuit to make sure that the Unit power supply is turned OFF only after the power supply for the control system is turned OFF.
- Do not disconnect the cable or turn OFF the power supply to the Controller when downloading data or the user program from Support Software.
- Always turn OFF the power supply to the Controller before you attempt any of the following.
  a) Mounting or removing an NX Unit, Communication Control Unit
  b) Assembling Units
  c) Setting DIP switches or rotary switches
  d) Connecting or wiring cables
  e) Attaching or removing terminal blocks or connectors

  The Power Supply Unit may continue to supply power to the Controller for a few seconds after the power supply turns OFF. The UNIT PWR and I/O PWR indicators are lit during this time. Confirm that the UNIT PWR and the I/O PWR indicators are not lit before you perform any of the above actions.

Operation

- Confirm that no adverse effect will occur in the system before you attempt any of the following.
  a) Changing the operating mode of the Safety CPU Unit
  b) Changing the user program or settings
  c) Changing set values or present values
  d) Forced refreshing
  e) Restarting a slave or Unit after you change any settings

f) Transferring a backup file on the SD Memory Card

- After you change any slave or Unit settings, carefully check the safety of the controlled system before you restart the Unit.
- If two different function modules are used together, such as when you use an EtherNet/IP Function Module and an NX Bus Function Module, take suitable measures in the user program and external controls to ensure that safety is maintained in the controlled system if one of the function modules stops. The relevant outputs will behave according to the slave or Unit specifications if a partial fault level error occurs in one of the function modules.

General Communications

- When you use data link communications, check the error information that is given in *_ErrSta* (Controller Error Status) to make sure that no error has occurred in the source device. Create a user program that uses reception data only when there is no error in the source device.
  If there is an error in the source device, the data for the data link may contain incorrect values.
- If an error occurs in tag data link communications or communications between NX Units, this product continues refreshing variables with the last values that it receives.
- Unexpected operation may result if inappropriate data link tables are set. Even if appropriate data link tables have been set, confirm that the controlled system will not be adversely affected before you transfer the data link tables. The data links start automatically after the data link tables are transferred.

EtherNet/IP Communications

- Before using I/O data, confirm that this product serves your purpose, in consideration of the following specifications of tag data link communications for this product.
  a) If an error occurs in tag data link communications, this product continues refreshing variables with the last values that it receives.
  b) If an error occurs in tag data link communications, the Omron EtherNet/IP Originator automatically restores the communications after resolving the cause of the error.
  c) This product cannot monitor the target connection status. If you use this product as a target device, make sure to use the originator to check the connection status.
- Make sure to use the communications distance, number of nodes connected, and method of connection for EtherNet/IP within specifications. Do not connect EtherNet/IP communications to EtherCAT or other networks. An overload may cause the network to fail or malfunction.
- All related EtherNet/IP nodes are reset when you transfer settings for the built-in EtherNet/IP port (including IP addresses and tag data links settings). The settings can only be enabled after the reset. Confirm that the system will not be adversely affected by resetting nodes before you transfer the settings.
- If EtherNet/IP tag data links (cyclic communications) are used with a repeating hub, the communications load on the network will increase. This will increase collisions and may prevent stable communications. Do not use repeating hubs on networks where tag data links are used. Use an Ethernet switch instead.

Restoring Data

- You cannot back up, restore, or compare some or all of the settings for certain slaves and Units. Also, you cannot back up, restore, or compare data for disabled slaves or Units. After you restore data, sufficiently confirm that operation is correct before you start actual operation.

Transferring Programs

- Always confirm safety at the connected equipment before you perform the download when the device output hold configuration is set to enable. The equipment may operate unexpectedly because the last status for outputs is retained.

Standards

- The customer is responsible for attaining conformance of the entire system to standards.

Maintenance

- Test the functionality every six months to detect welded contactor contacts.
  To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

Unit Replacement

- Make sure that the required data, including the configurations, settings and variables, is transferred to a Communication Control Unit that was replaced and to externally connected devices before restarting operation. Be sure to transfer the tag data link settings and routing tables, which are stored in the Communication Control Unit.
- After you replace the Safety Control Unit, set the program and all configuration settings that are necessary to resume operation. Make sure that the safety functions operate normally before you start actual operation.
- When you replace a Unit, start operation only after you transfer the settings and variables that are required for operation to the new Unit.

Disposal

- Dispose of the product according to local ordinances as they apply.

Precautions for Correct Use

Storage and Installation

- Follow the instructions in this manual to correctly perform installation and wiring.
- Do not operate or store the Units in the following locations. Doing so may result in burning, in operation stopping, or in malfunction.
  a) Locations subject to direct sunlight
  b) Locations subject to temperatures or humidity outside the range specified in the specifications
  c) Locations subject to condensation as the result of severe changes in temperature
  d) Locations subject to corrosive or flammable gases
  e) Locations subject to dust (especially iron dust) or salts
  f) Locations subject to exposure to water, oil, or chemicals
  g) Locations subject to shock or vibration
  h) Locations subject to static electricity or other forms of noise
- Take appropriate and sufficient countermeasures when installing the Controller in the following locations.
  a) Locations subject to strong, high-frequency noise
  b) Locations subject to static electricity or other forms of noise
  c) Locations subject to strong electromagnetic fields
  d) Locations subject to possible exposure to radioactivity
  e) Locations close to power lines
- Before touching a Unit, be sure to first touch a grounded metallic object in order to discharge any static build-up.
- Use the rated power supply voltage for the Units that supply power. Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.
- Install the Units in a well-ventilated area. Avoid installing the Units near heating elements. Doing so may result in malfunction, in operation stopping, or in burning.

Mounting

- When you install the Unit, be careful not to touch or bump the pins in the NX bus connector.
- When you handle the Unit, be careful not to apply stress to the pins in the NX bus connector. If the Unit is installed and the power supply is turned ON when the pins in the connector are deformed, contact failure may cause malfunctions.
- Always mount an End Cover to the end of the CPU Rack to protect the last Unit on the CPU Rack. Not mounting the End Cover may result in malfunction or failure of the Units.
- After you mount the Unit, always secure it with End Plates at both sides. If you do not secure it, the Unit may be damaged or malfunction.
- If you use DIN Track Insulation Spacers to install a CPU Rack, the height will be increased by approximately 10 mm. Make sure that the CPU Rack and connecting cables do not come into contact with other devices.
- To remove an NX Unit, remove multiple NX Units together including the one you need to remove. If you attempt to remove only one NX Unit, it may be tight and difficult to pull out. Do not unlock the

DIN Track mounting hooks on all of the NX Units at the same time. If you unlock the DIN Track mounting hooks on all of the NX Units at the same time, all of the Units may come off.

Wiring

- Do not allow foreign matter to enter the openings in the Unit. Doing so may result in Unit burning, electric shock, or failure.
- Do not allow wire clippings, shavings, or other foreign material to enter any Unit. Otherwise, Unit burning, failure, or malfunction may occur. Cover the Units or take other suitable countermeasures, especially during wiring work.
- For EtherNet/IP, use the connection methods and cables that are specified in this manual. Otherwise, communications may be faulty.
- Use the rated power supply voltage for the Units that supply power. Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.
- Make sure that the current capacity of the wire is sufficient. Otherwise, excessive heat may be generated. When cross-wiring terminals, the total current for all the terminals will flow in the wire. When wiring cross-overs, make sure that the current capacity of each of the wires is not exceeded.
- If you use reed switches for the input contacts for AC Input Units, use switches with a current capacity of 1 A or greater.
  If reed switches with smaller allowable currents are used, the contacts may fuse due to surge currents.

Operation

- Confirm the Device Output Hold Configuration before you download data from the Communication Control Unit.
- Take safety measures for the controlled system as well.

EtherNet/IP Communications

- To set up an intranet through a global address involves network security considerations. Be sure to consult with a network specialist in advance and consider installation of a firewall.
  After a firewall is set up by a communications technician, there may be some applications that cannot be used. Be sure to check first with the communications technician.

Error Processing

- If you change the event level of a Controller error, the output status when the error occurs may also change. Confirm safety before use.

Restoring Data

- When you edit the restore command file or the automatic transfer command file, do not change anything in the file except for the “yes” and “no” specifications for the selectable data groups. If you

change anything else in the file, the Controller may perform unexpected operation when you restore or automatically transfer the data.
- To prevent an unexpected restoration, set to enter the password for each execution before the restore operation.

Actual Operation

- Make sure that you are connected to the correct Safety CPU Unit before you perform any online operations with the Safety CPU Unit.
- Before you transfer safety application data to the Safety CPU Unit, check the safety signature and make sure the data is the intended data.
- Always confirm the destination before you transfer configuration information and safety application data from the Sysmac Studio.
- You cannot monitor or perform certain online operations with the same Safety CPU Unit from more than one copy of the Sysmac Studio at the same time.

Turning OFF the Power Supply

- Do not turn OFF the power supply while data is being transferred.

Debugging

- The task period affects the safety response performance. If the task period changes due to changes in the configuration or programs, recalculate the safety reaction times.
- If you change the I/O for a variable to publish to a Communication Control Unit, the device variable assignments to the Communication Control Unit will be canceled. In this case, you need to assign the device variables, and then transfer the settings and programs to the Communication Control Unit. After you transfer the settings and programs, check that the operation of the Communication Control Unit is correct.
- For security purposes, we recommend that you set a password for the Safety CPU Unit and the project file. To avoid the leakage, keep the passwords under strict control. Especially, when you transmit password data through the Internet, implement a measure to secure the transmission such as by using the public key encryption.
- If you lose the password that is set to the Safety CPU Unit, you will no longer be able to make changes to the Safety CPU Unit. Take caution not to lose the password. If you want to reset the configured password, contact your OMRON representative.
- For safety data logging, make sure to use the settings file generated from the same project file as the logging target.
- After editing the CIP Safety connection settings, you need to transfer the Communication Control Unit settings and programs. Once the settings and programs are transferred, check to see if the Communication Control Unit runs normally.

SD Memory Cards

- Insert the SD Memory Card all the way.

- Do not turn OFF the power supply to the Controller during SD Memory Card access. The files may be corrupted.
  If there is a corrupted file in the SD Memory Card, the file is automatically deleted by the restoration function when the power supply is turned ON.
- If you use an OMRON SD Memory Card, the end of the life of the SD Memory Card can be detected in the following ways.
  a) *_Card1Deteriorated* (SD Memory Card Life Warning Flag) system-defined variable
  b) *SD Memory Card Life Exceeded (Observation)* event in the event log
  When the end of the life is detected in any of the above ways, replace the SD Memory Card.
- You can use the SD memory card life expiration detection function on some specific SD Memory Cards. Refer to *Specifications of Supported SD Memory Cards, Folders, and Files* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for details.

Replacing Slaves and Units

- If you replace a slave or Unit, refer to the operation manual for the slave or Unit for information on the data required for individual slaves or Units and redo the necessary settings.

Periodic Inspections and Maintenance

- Do not disassemble, repair, or modify the Safety Control Unit. Doing so may lead to loss of safety functions.

Disposal

- Be careful not to injure yourself when dismantling the Safety Control Unit.

Regulations and Standards

The NX-series Safety Control Units are certified for the following standards.

- Safety CPU Unit NX-SL5500 / NX-SL5700

Certification body	Standards
TÜV Rheinland*1	• EN ISO 13849-1: 2015 • EN ISO 13849-2: 2012 • IEC 61508 parts 1-7: 2010 • IEC/EN 61131-2: 2007 • IEC 61326-3-1: 2017 • IEC 61131-6: 2012
UL	NRAG (UL61010-1, UL61010-2-201, and UL121201) NRAG7 (CSA C22.2 No.61010-1, CSA C22.2 No.61010-2-201, and CSA C22.2 No.213) FSPC (IEC 61508 and ISO 13849)

*1. The FSoE protocol was certified for applications in which OMRON FSoE devices are connected to each other.
For compatibility with FSoE devices other than OMRON FSoE devices, the customer must validate FSoE communications.

- Safety I/O Unit NX-SID800 / NX-SIH400 / NX-SOD400 / NX-SOH200

Certification body	Standards
TÜV Rheinland*1	• EN ISO 13849-1: 2015 • EN ISO 13849-2: 2012 • IEC 61508 parts 1-7: 2010 • IEC/EN 61131-2: 2007 • IEC 61326-3-1: 2017
UL	NRAG (UL508 and ANSI/ISA 12.12.01) NRAG7 (CSA C22.2 No.142 and CSA C22.2 No.213)

*1. The FSoE protocol was certified for applications in which OMRON FSoE devices are connected to each other.
For compatibility with FSoE devices other than OMRON FSoE devices, the customer must validate FSoE communications.

The NX-series Safety Control Units allow you to build a safety control system that meets the following standards.

- Requirements for SIL 3 (Safety Integrity Level 3) in IEC 61508, IEC/EN 62061, (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)
- Requirements for PLe (Performance Level e) and for safety category 4 in EN ISO13849-1

The NX-series Safety Control Units are also registered for RCM, EAC, and KC compliance.

The NX-series Communication Control Units are certified for the following standards.

Certification body	Standards
UL	NRAG (UL61010-1, UL61010-2-201, and UL121201) NRAG7 (CSA C22.2 No.61010-1, CSA C22.2 No.61010-2-201, and CSA C22.2 No.213)

The NX-series Communication Control Units are also registered for RCM, EAC, and KC compliance.

Conformance to EU Directives

Applicable Directives

- EMC Directives
- Machinery Directive

Concepts

EMC Directives

OMRON devices that comply with EU Directives also conform to the related EMC standards so that they can be more easily built into other devices or the overall machine. The actual products have been checked for conformity to EMC standards.*1

Whether the products conform to the standards in the system used by the customer, however, must be checked by the customer. EMC-related performance of the OMRON devices that comply with EU Directives will vary depending on the configuration, wiring, and other conditions of the equipment or control panel on which the OMRON devices are installed. The customer must, therefore, perform the final check to confirm that devices and the overall machine conform to EMC standards.

*1. Applicable EMC (Electromagnetic Compatibility) standards are as follows: EMS (Electromagnetic Susceptibility): EN 61131-2 EMI (Electromagnetic Interference): EN 61131-2 (Radiated emission: 10-m regulations).

Machinery Directive

The Machinery Directive requires ensuring the required safety for safety components used for machinery safety.

Applicable standards: EN ISO 13849-1.

Conformance to EU Directives

The NX-series Units comply with EU Directives. To ensure that the machine or device in which the NX-series Units are used complies with EU Directives, the following precautions must be observed.

- The NX-series Units must be installed within a control panel.
- You must use SELV power supply for the DC power supplies that are connected as the Unit power supplies and I/O power supplies for the NX-series Units.
  EMC standard compliance was confirmed for the recommended Power Supplies. Refer to the user's manual for the connected CPU Unit for information on the recommended Power Supplies for the CPU Rack of the NX-series CPU Unit. If your High-speed Analog Input Unit is connected to a Slave Terminal, we recommend that you use the OMRON S8VK-S-series Power Supplies.
- NX-series Units that comply with EU Directives also conform to the Common Emission Standard. Radiated emission characteristics (10-m regulations) may vary depending on the configuration of the control panel used, other devices connected to the control panel, wiring, and other conditions.
  You must therefore confirm that the overall machine or equipment in which the NX-series Units are used complies with EU Directives.
- This is a Class A product (for industrial environments). In a residential environment, it may cause radio interference. If radio interference occurs, the user may be required to take appropriate measures.

Conformance to EN ISO 13849-1

EN ISO 13849-1 requires functional safety management to avoid systematic failure during the software development. This is required in all phases of the life cycle of software programming and software design (e.g., basic software design, safety circuit system design, and software upgrades) in safety control systems to be developed using safety controllers.
Therefore, functional safety management is required for design and development of software for facilities and equipment that use the function blocks provided in the Safety Controller.
The customer must implement measures to ensure compliance with these standards.

You can download the reliability data for safety of machinery that is required to verify the safety performance of your equipment from the following URL: http://www.ia.omron.com/support/sistemalibrary/index.html.

Conformance to UL and CSA Standards

The NX-series Safety Control Units comply with the following UL and CSA standards. The application conditions for standard compliance are defined. Refer to the *Instruction Sheet* that is provided with each Unit before application.

Conformance to Shipbuilding Standards

Some NX-series products comply with shipbuilding standards. If you use an NX-series product that complies with shipbuilding standards and the machinery or system in which you use the NX-series product must also comply with the standards, consult with your OMRON representative. Application conditions are defined according to the installation location. Application may not be possible for some installation locations.

Usage Conditions for NK and LR Shipbuilding Standards

- A Safety Control Unit must be installed within a control panel.
- Gaps in the door to the control panel must be completely filled or covered with gaskets or other material.
- The following noise filter must be connected to the power supply line.

Noise Filter

Name	Manufacturer	Model
Noise filter	Cosel Co., Ltd.	TAH-06-683

Conformance to KC Certification

When you use this product in South Korea, observe the following precautions.

사 용 자 안 내 문
이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

This product meets the electromagnetic compatibility requirements for business use. There is a risk of radio interference when this product is used in home.

Usage Conditions for KC Certification

Take the same measures as those described in *Conformance to EU Directives* on page 40. In addition, attach a clamp core to the port side of the EtherNet/IP cable.
The recommended clamp core is given below.

Recommended Clamp Core

Manufacturer	Product	Model	Turns of cable
TOKIN	Clamp core	ESD-SR-250	1 turn

Unit Versions

This section describes the notation that is used for unit versions, the confirmation method for unit versions, and the relationship between unit versions and Sysmac Studio versions.

Unit Versions

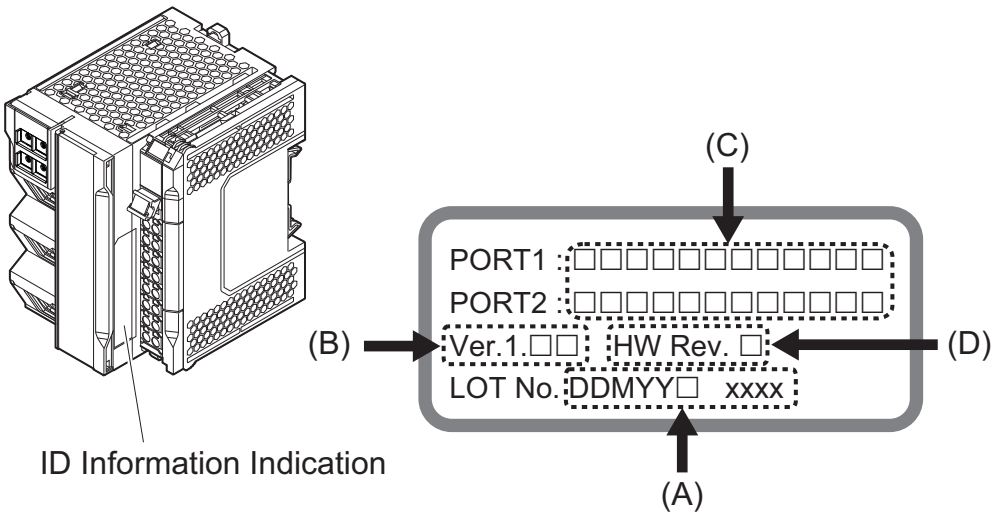
A “unit version” has been introduced to manage the Communication Control Unit and the Safety Control Unit according to differences in functionality accompanying Unit upgrades.

Notation of Unit Versions on Products

The unit version is given with the Unit specifications on the side of the Unit or in the notched area.

● Communication Control Unit

ID Information is given with the ID information indication on the side of the Unit.

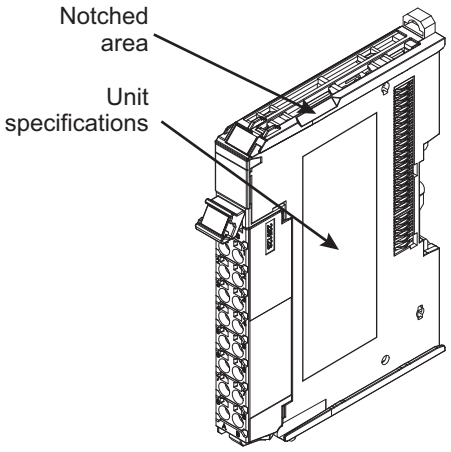


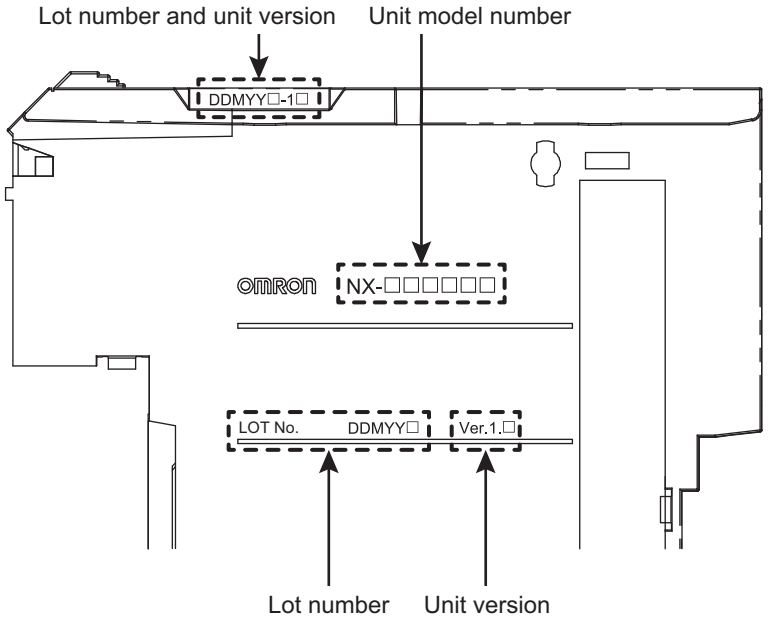
Letter	Name	Function
A	Lot number and serial number	Gives the lot number and the serial number of the Unit. DDMYY: Lot number, □: Used by OMRON, SSSS: Serial number “M” gives the month (1 to 9: January to September, X: October, Y: November, Z: December)
B	Unit version	Gives the unit version of the Unit.
C	MAC addresses	Gives the MAC addresses of the built-in EtherNet/IP port (port 1) and the built-in EtherNet/IP port (port 2) on the Unit.
D	Hardware revision	Gives the hardware revision of the Unit. *1

*1. The hardware revision is not displayed for the Unit that the hardware revision is in blank.

● NX Units

The unit version is given with the Unit specifications on the side of the Unit or in the notched area.





The following information is provided in the Unit specifications on the Unit.

Name	Function
Unit model number	Gives the model of the Unit.
Unit version	Shows the unit version of the Unit.
Lot number	Gives the lot number of the Unit. DDMYY□: Lot number, □: Used by OMRON. “M” gives the month (1 to 9: January to September, X: October, Y: November, Z: December)

The following information is provided in the notched area on the Unit.

Name	Function
Lot number and unit version	Gives the lot number and unit version of the Unit. • DDMYY☐: Lot number, ☐: Used by OMRON. “M” gives the month (1 to 9: January to September, X: October, Y: November, Z: December) • 1☐: Unit version The decimal portion of the unit version is omitted. (It is provided in the Unit specifications.)

Checking Unit Versions with the Sysmac Studio

You can check unit versions with the Sysmac Studio.

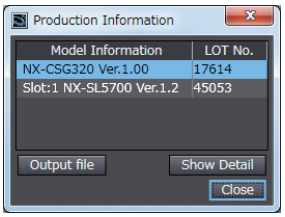
● Checking the Unit Version of a Communication Control Unit

You can use the Production Information while the Sysmac Studio is online to check the unit version of a Unit. You can do this for the Communication Control Unit, NX Units on the CPU Rack.

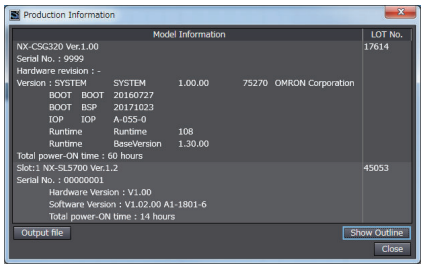
1 Right-click **CPU Rack** under **Configurations and Setup** - **CPU/Expansion Racks** in the Multiview Explorer and select **Display Production Information**.
The Production Information Dialog Box is displayed.

● Changing Information Displayed in Production Information Dialog Box

1 Click the **Show Detail** or **Show Outline** Button at the lower right of the Production Information Dialog Box.
The view will change between the production information details and outline.



Outline View



Detail View

The information that is displayed is different for the Outline View and Detail View. The Detail View displays the unit version, hardware revision, and various versions. The Outline View displays only the unit version.

Note The hardware revision is separated by "/" and displayed on the right of the hardware version. The hardware revision is not displayed for the Unit that the hardware revision is in blank.

Unit Versions of Units and Sysmac Studio Versions

The functions that are supported depend on the unit version of the Unit. The version of Sysmac Studio that supports the functions that were added for an upgrade is also required to use those functions.

To use the NX-CSG□□□ Communication Control Unit and the NX-SL5□□□ Safety CPU Unit, Sysmac Studio version 1.24 or higher is required.
Refer to *A-20 Version Information* on page A-115 for the relationship between the unit versions of the Units and the Sysmac Studio versions, and for the functions that are supported by each unit version.

Related Manuals

The followings are the manuals related. Use these manuals for reference.

Manual name	Cat. No.	Model numbers	Application	Description
NX-series Safety Control Unit / Communication Control Unit User's Manual	Z395	NX-SL5□□□ NX-SI□□□□ NX-SO□□□□ NX-CSG□□□	Learning how to use the NX-series Safety Control Units and Communication Control Units.	Describes the hardware, setup methods, and functions of the NX-series Safety Control Units and Communication Control Units.
NX-series Communication Control Unit Built-in Function User's Manual	Z396	NX-CSG□□□	Learning about the built-in functions of an NX-series Communication Control Unit.	Describes the software setup methods and communicantions functions of an NX-series Communication Control Unit.
GI-S Series Safety I/O Terminal User's Manual	Z400	GI-S□□□□□□	Learning how to use the GI-S Series Safety I/O Terminals.	Describes the hardware, setup methods, and functions of the GI-S Series Safety I/O Terminals.
Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety User's Manual	W645	NXR-SXD1204□-CST	Learning how to use the NXR-S Series Simple Logic Safety I/O Block.	Describes the hardware, setup methods, and functions of the NXR-S Series Simple Logic Safety I/O Block.
Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for EtherNet/IP User's Manual	W646	NXR-SXD1204-EIT		
NX-series Safety Control Unit Instructions Reference Manual	Z931	NX-SL□□□□	Learning about the specifications of instructions for the Safety CPU Unit.	Describes the instructions for the Safety CPU Unit.
NX-series Digital I/O Units User's Manual	W521	NX-ID□□□□ NX-IA□□□□ NX-OC□□□□ NX-OD□□□□ NX-MD□□□□	Learning how to use NX-series Digital I/O Units.	The hardware, setup methods, and functions of the NX-series Digital I/O Units are described.
NX-series Analog I/O Units User's Manual for Analog Input Units and Analog Output Units	W522	NX-AD□□□□ NX-DA□□□□	Learning how to use NX-series Analog Input Units and Analog Output Units.	The hardware, setup methods, and functions of the NX-series Analog Input Units and Analog Output Units are described.
NX-series Analog I/O Units User's Manual for Temperature Input Units and Heater Burnout Detection Units	W566	NX-TS□□□□ NX-HB□□□□	Learning how to use NX-series Temperature Input Units and Heater Burnout Detection Units.	The hardware, setup methods, and functions of the NX-series Temperature Input Units and Heater Burnout Detection Units are described.
NX-series Data Reference Manual	W525	NX-□□□□□□	Referencing lists of the data that is required to configure systems with NX-series Units.	Lists of the power consumptions, weights, and other NX Unit data that is required to configure systems with NX-series Units are provided.
Sysmac Studio Version 1 Operation Manual	W504	SYSMAC -SE2□□□	Learning about the operating procedures and functions of the Sysmac Studio.	Describes the operating procedures of the Sysmac Studio.

Manual name	Cat. No.	Model numbers	Application	Description
NX-series System Units User's Manual	W523	NX-PD1□□□ NX-PF0□□□ NX-PC0□□□ NX-TB□□□X	Learning how to use NX-series System Units	The hardware and functions of the NX-series System Units are described.

Terminology

Term	Description
standard	The generic term for devices, functions, and data that are used for general control purposes as opposed to those that are used for safety measures.
safety function	A function that is executed by the safety control system to achieve a safe state for a machine hazard.
safe state	The status of a device or piece of equipment when the risk of danger to humans has been reduced to an acceptable level.
safety signal	A signal that is used for safety controls. In this safety control system, the data type of a variable determines whether a signal is related to the safety controls. Broadly speaking, there are two data types: safety data types and standard data types.
standard signal	A signal or data that is used for general control purposes.
Safety data type	The data type for a safety signal.
Standard data type	The data type for a standard signal.
safety reaction time	The time required for the system to enter a safe state in a worst-case scenario after the occurrence of a safety-related input (press of an emergency stop pushbutton switch, interruption of a light curtain, opening of a safety door, etc.) or device failure. The reaction time of the system includes the reaction times of sensors and actuators, just like the reaction time for a Controller or network.
safety control	A type of control that uses devices, functions, and data that are designed with special safety measures.
standard control	A type of control that use devices, functions, and data that are designed for general control purposes. This term is used to differentiate from a safety control
safety process data communications	A type of I/O data communications that is used for safety control purposes.
standard process data communications	A type of I/O data communications that is used for standard control purposes.
Safety I/O connection	A type of connections that is used for safety process data communications.
CIP Safety connection	Safety I/O connection that is used to transmit safety process data by the communication protocol called CIP Safety. CIP Safety originator connection and CIP Safety target connection are available depending on the roles of communications.
CIP Safety originator connection	A CIP Safety connection when an own node is a CIP Safety originator.
CIP Safety target connection	A CIP Safety connection when an own node is a CIP Safety target.
CIP Safety originator	A role in CIP Safety communications. A CIP Safety originator manages a CIP Safety connection for a CIP Safety target. CIP Safety originator exists in a connection unit, and not in a device unit.
CIP Safety target	A role in CIP Safety communications. A CIP Safety target receives a request to open a CIP Safety connection from a CIP Safety originator. CIP Safety target exists in a connection unit, and not in a device unit.
single-cast connection	A safety process data communications method in CIP Safety. A CIP Safety originator and a CIP Safety target communicate one-to-one in this connection. You can apply this setting for both of input data and output data.
multi-cast connection	A safety process data communications method in CIP Safety. A CIP Safety target sends the input data of the CIP Safety target in multi-cast to multiple CIP Safety originators in this connection. This is a connection type you can set only for input data of a CIP Safety target. You cannot apply this setting for output data.
FSoE master connection	Master safety I/O connection that is used to transmit safety process data by the communication protocol called FSoE.
safety master connection	The generic term for the CIP Safety originator connection and the FSoE master connection.
exposing global variables to the Communication Control Unit	Exposing specified global variables to the Communication Control Unit to allow the exchange of standard signals between the standard controller and the Safety CPU Unit. Exposed variables can be transmitted to the standard controller via tag data links.
Safety Control Unit	The generic term for a Unit that is used in safety controls.
Safety CPU Unit	A CPU Unit that is used for safety controls. This is a type of NX Unit.

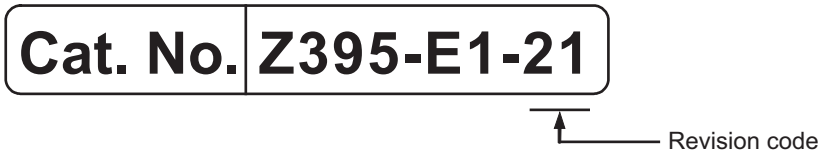
Term	Description
Safety I/O Unit	An I/O Unit that is used for safety controls. This is a type of NX Unit.
safety input device	An input device that is designed with special safety measures for use in safety controls. The generic term for safety input devices, such as emergency stop pushbutton switches and safety switches.
safety output device	An output device that is designed with special safety measures for use in safety controls. The generic term for safety output devices, such as safety relays.
EtherNet/IP Slave Terminal	An EtherNet/IP Slave Unit Terminal is a building-block slave that is created by mounting a group of NX Units.
Communication Control Unit	The generic term for the interface units to have CIP Safety communications on a network between the Safety CPU Unit and CIP Safety on EtherNet/IP devices.
Safety Network Controller	The generic term for the building-block type safety controllers that have mounted the Safety Control Unit with the Communication Control Unit.
Safety program	User programming for safety controls in the Safety CPU Unit. This term is used to differentiate from the user program of the standard controller. Safety programs are programmed in the FBD language.
FBD language	The abbreviation for the function block diagram programming language. This is a graphical language used to program algorithms with connecting lines that represent the flow of inputs and data, and rectangular boxes that represent functions or function blocks. Unlike the ladder diagram language, the FBD language does not have bus bars, and the connecting lines represent the flow of inputs and data rather than the power flow. Algorithms are executed in order from top to bottom in units that are called networks. A network consists of configuration elements that use connecting lines to connect inputs to outputs. The FBD language does not have an END instruction. Execution for the task period ends when the last network is executed. You use the FBD language to write safety programs for the Safety CPU Unit.
user program	All of the programs that are created by the user. User program refers to the programs for standard controls of the standard controller and the safety program of the Safety CPU Unit.
operating mode	The status of the Safety CPU Unit, when it is in normal operation, that the user changes to run or check the operation of the Safety CPU Unit. There are the three modes: PROGRAM mode, DEBUG mode, and RUN mode. You can use DEBUG mode only when the Sysmac Studio is online with the Safety CPU Unit.
safety validation	The process of appending confirmation information to the safety application data if safety validation testing demonstrates that the safety controls meet the required specifications of a safety system. You execute the safety validation from the Sysmac Studio when the Safety CPU Unit is in DEBUG mode. The validated safety programs are automatically transferred to the non-volatile memory of the Safety CPU Unit.
DEBUG mode	The mode that is used to debug unvalidated safety programs. DEBUG mode is only available when the Sysmac Studio is online with the Safety CPU Unit. Use this mode to check that the safety programs and external devices operate correctly. After you confirm that the system meets the required specifications, perform the safety validation. This will enable you to change to RUN mode. When you change from PROGRAM mode to DEBUG mode, the unvalidated safety programs are automatically transferred to the main memory of the Safety CPU Unit.
DEBUG mode (RUN)	A status that indicates that an unvalidated safety program is in execution in DEBUG mode. You can control BOOL variables, use forced refreshing, and change present values.
DEBUG mode (STOPPED)	A status that indicates that an unvalidated safety program is stopped in DEBUG mode. You can control BOOL variables, use forced refreshing, and change present values.
PROGRAM mode	A mode indicates that execution of the safety program is stopped. You cannot control BOOL variables, use forced refreshing, or change present values.
RUN mode	A mode that indicates that execution of the validated safety programs is in progress. Unlike DEBUG mode (RUN), the validated safety programs in the non-volatile memory of the Safety CPU Unit are executed. You cannot control BOOL variables, use forced refreshing, or change present values.
before safety validation	A status that indicates that safety validation has not been performed on the safety application data from the Sysmac Studio because it has not yet been determined whether the safety controls meet the required specifications of the safety system.

Term	Description
after safety validation	A status indicates that safety validation has been performed on the safety application data from the Sysmac Studio because it has been determined that the safety controls meet the required specifications of the safety system.
CPU Rack	A Rack to which a CPU Unit or Communication Control Unit is mounted. For NX-series CPU Units to which NX Units can be connected, a CPU Rack has a CPU Unit with NX Units and an End Cover mounted to it. For NX-series Communication Control Units, a CPU Rack has a Communication Control Unit with NX Units and an End Cover mounted to it.
CPU Rack settings	It consists of the following data: • Configuration information • Unit operation settings • Unit application data
configuration information	It consists of the following data: • Unit configuration information • I/O allocation information
I/O allocation information	The set of information that specifies the I/O data to be processed by I/O refreshing. On the Sysmac Studio, this is shown as configuration information and includes the Unit configuration information.
Unit configuration information	The set of information that specifies the configuration of the NX Units that are connected to the NX bus master. On the Sysmac Studio, this is shown as configuration information and includes the I/O allocation information.
safety application data	The data that contains the settings that are used to operate the NX-series Safety Control Units. It consists of the safety programs, safety task, and variables. You use the Sysmac Studio to create this data, and then transfer and execute it on the Safety CPU Unit. On the Sysmac Studio, this data is shown as the slave parameters. The location where the safety application data is stored on the Safety CPU Unit depends on whether the safety programs have been validated. (Unvalidated safety programs are stored in the main memory, while validated safety programs are stored in the non-volatile memory.)
safety input function	A function that evaluates whether the signals that are input on a safety input terminal are normal or abnormal. Specific safety evaluation functions include test pulse evaluation and dual channel evaluation. When the evaluation result shows an abnormality, the safety input data is made inactive (OFF).
safety output function	A function that evaluates whether the values of safety output data and the output signals on safety output terminals are normal or abnormal. Specific safety evaluation functions include test pulse evaluation and dual channel evaluation. When the evaluation result shows an abnormality, the output signal on the safety output terminal is turned OFF.
dual channel evaluation	This function uses a pair of safety input or safety output terminals as redundant terminals that are checked for consistency to evaluate the status of the safety input or safety output.
single channel	The input or output is used as a single point.
dual channels	Two inputs or outputs are used as a pair of points for redundancy.
test pulse evaluation	This function outputs a test pulse that is used to evaluate a safety input or safety output for failures or wiring errors with the connected external device.
change tracking	A pin is used to manage whether the safety application data has been changed after the finalized data is created.
UNID	An ID assigned to a device so that it can be uniquely identified by all the networks on the safety system for CIP Safety communications. An UNITD is a 10-byte value, consisting of a 6-byte Safety Network Number and a 4-byte Node ID.
Safety Network Number (SNN)	A number assigned to a safety network so that it can be uniquely identified for CIP Safety communications. The Safety Network Number is set for the NX bus, the built-in EtherNet/IP ports 1 and 2.

Term	Description
Node ID	An ID assigned to each of devices on a network so that the devices with the same Safety Network Number (SNN) can be uniquely identified for CIP Safety communications. The Safety CPU Unit is the only CIP Safety device on the NX bus, and the Node ID is always *1*. For a CIP Safety device on an EtherNet/IP network, its IP address is used as the Node ID.

Revision History

A manual revision code appears as a suffix to the catalog number on the front and back covers of the manual.



Revision code	Date	Revised content
01	April 2018	Original production
02	July 2018	• Made changes accompanying the upgrade to NX-SL5700 unit version 1.3. • Made revisions accompanying with addition of the NX-SL5500. • Made revisions accompanying the upgrade to Sysmac Studio version 1.24.
03	August 2018	Added PFH values.
04	October 2018	• Made revisions accompanying the appearance change of the indicators. • Corrected mistakes.
05	April 2019	• Made revisions accompanying the appearance change of the indicators. • Modified the model of the recommended communication cables. • Made revisions accompanying the upgrade to Sysmac Studio version 1.27. • Added the Shipbuilding Standards (Class NK, LR) • Corrected mistakes.
06	July 2019	• Made revisions accompanying the upgrade to Sysmac Studio version 1.29. • Corrected mistakes.
07	January 2020	• Made revisions accompanying the upgrade to Sysmac Studio version 1.31. • Corrected mistakes.
08	April 2020	• Made changes accompanying the upgrade toNX-SL5500/NX-SL5700unit version 1.4. • Made revisions accompanying the upgrade to Sysmac Studio version 1.40. • Corrected mistakes.
09	July 2020	• Made revisions accompanying the upgrade to Sysmac Studio version 1.41. • Corrected mistakes.
10	April 2021	• Made revisions accompanying the upgrade to Sysmac Studio version 1.45. • Corrected mistakes.
11	April 2022	• Made revisions accompanying the upgrade to Sysmac Studio version 1.49. • Corrected mistakes.
12	June 2022	Corrected mistakes.
13	October 2022	Revisions for adding safety precautions regarding security.
14	April 2023	• Made revisions accompanying the release of NX502 CPU Units. • Made revisions accompanying the upgrade to Sysmac Studio version 1.54.
15	October 2023	Made revisions accompanying the upgrade to Sysmac Studio version 1.56.
16	June 2024	• Made revisions accompanying the addition of D40A-2 Non-contact Door Switch. • Added troubleshooting description for safety input. • Corrected mistakes.
17	April 2025	• Made revisions accompanying the upgrade to Sysmac Studio version 1.62.

Revision code	Date	Revised content
18	July 2025	• Made revisions accompanying the addition of precautions for correct use when setting TUNID to the target device.
19	April 2026	• Corrected mistakes.
20	July 2026	• Made revisions accompanying the upgrade to Sysmac Studio version 1.67.
21	October 2026	• Corrected mistakes.

1

Overview

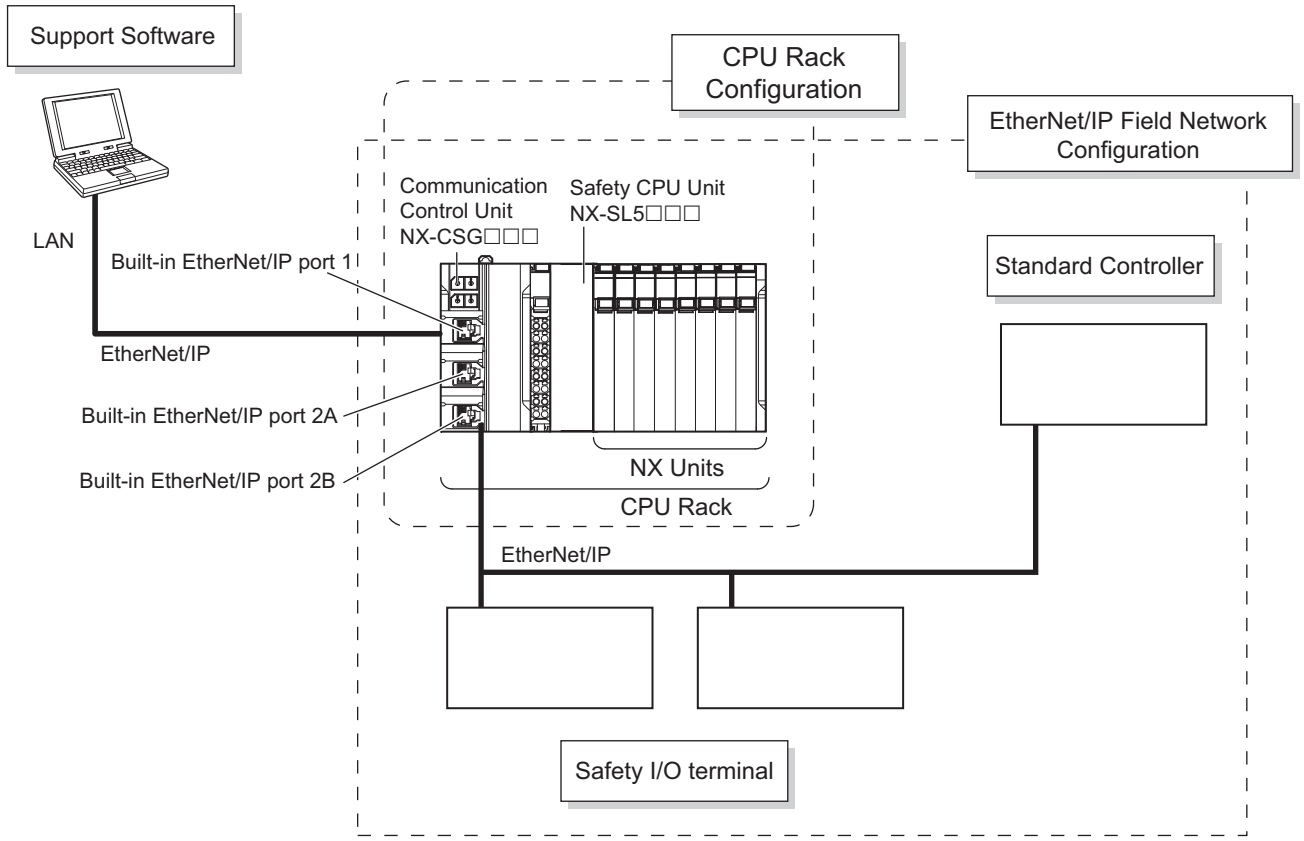
This section describes the overview of Safety Network Controller.

1-1 Overview of the Safety Network Controller 1-2
1-1-1 Features 1-2
1-1-2 Introduction to the System Configurations 1-4
1-2 Procedure 1-7
1-2-1 Overall Procedure 1-7
1-2-2 Detailed Procedures 1-8

1-1 Overview of the Safety Network Controller

1-1-1 Features

The NX-series Safety Network Controller is a safety controller lined up as part of Sysmac devices. By combining the NX-series Safety Control Unit with the NX-series Communication Control Unit, it can be utilized as a safety controller which has the CIP Safety on EtherNet/IP Communications functions.
You use the integrated development environment that is provided by the Sysmac Studio Automation Software to build the safety control system, and perform all settings, programming, and debugging of the Safety Control Unit / Communication Control Unit.



CIP Safety on EtherNet/IP Is Supported

You can configure a system that uses CIP Safety on EtherNet/IP communications on a network between Controllers or on a field network when you use a Safety Control Unit together with a Communication Control Unit (NX-CSG□□□). This system enables CIP Safety-based communications between devices that support CIP Safety on EtherNet/IP and other Safety CPU Units.

Feature EtherNet/IP Communications Port

The Communication Control Unit (NX-CSG□□□) provides an EtherNet/IP communications port.

In addition to CIP Safety on EtherNet/IP, you can use tag data links and TCP/UDP message communications as a interface with the standard controllers.

The Standard Unit of NX-series Available

In addition to Safety I/O Units, the standard NX Units such as NX-series Digital I/O Units and Analog I/O Units can be connected. You can exchange data easily between Safety CPU Units and these Units.

Excellent Connectability with OMRON Safety I/O Devices

You can directly connect OMRON's wide lineup of Safety I/O Devices to Safety I/O Units without using any special units.

Support for the IEC 61131-3 Programming Environment

● Program Languages Based on the IEC 61131-3 International Standard

Programming is possible with the FBD language, which is part of the programming language specifications of IEC 61131-3. And the safety function blocks that are defined in PLCopen® TC5 Safety are also supported.

● Programming with Variables

Programming with variables eliminates the need to specify memory addresses so that you can create user programs that are not dependent on any hardware considerations, such as the model of the Controller or the system configuration. This allows you to reuse user programming, even for different Controller models or system configurations.

Complete Advanced Validation

● Checking Safety Programs and Safety Parameters

You can verify beforehand whether your safety programs (user program for safety controls that runs on the Safety CPU Unit) and safety parameters (parameters that are used for safety controls) meet the validity and safety aspects that are outlined below.

- Validity and safety issues related to function block diagram programs, such as missing or incorrect connection for function blocks
- Safety issues, such as the incorrect connection of a standard input to a safety input parameter of a function block
- Validity of the safety task period

These checks help to prevent design regression and help to ensure the reliability of the safety designs.

● Debugging

You can connect the Sysmac Studio to perform various types of debugging, including monitoring, changing present values, and forced refreshing.

1-1-2 Introduction to the System Configurations

Safety Network Controller supports the following system configurations.

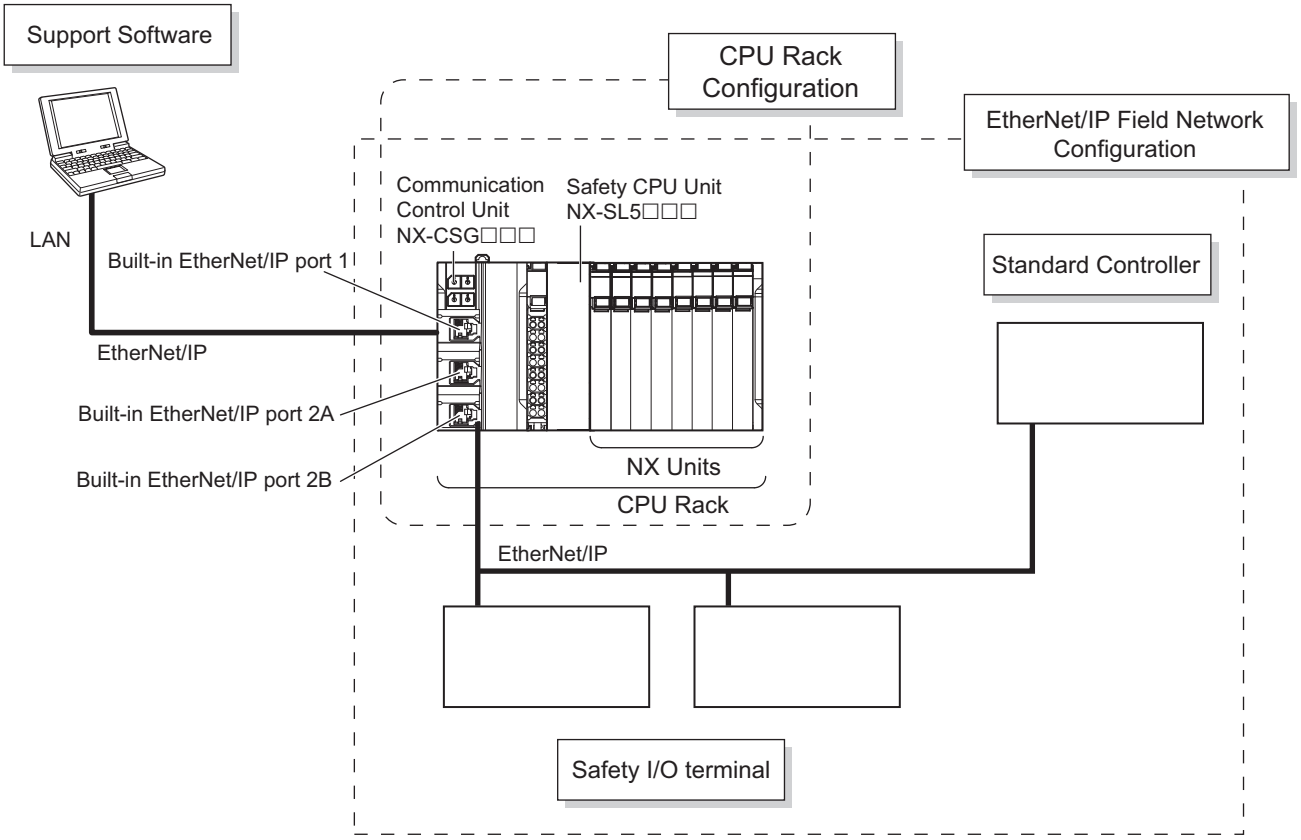
Basic Configurations

The Safety Network Controller basic configurations include CPU Rack configuration, EtherNet/IP field network configuration, and the Support Software.

- CPU Rack Configuration
  NX-SL5□□□ Safety CPU Unit, one type of NX Units, is mounted to the CPU Rack of Communication Control Unit to build a Safety Network Controller.
  NX-SI□□□□ and NX-SO□□□□ Safety I/O Units, types of NX Units, are mounted to the CPU Rack of Communication Control Unit to enable to use safety I/O control from Safety CPU Unit.
  With NX-series Digital I/O Units and Analog I/O Units mounted to the CPU Rack of Communication Control Unit, you can perform standard I/O control via the Safety CPU Unit.
  An NX bus can mount up to 32 NX Units including Power Supply Units.

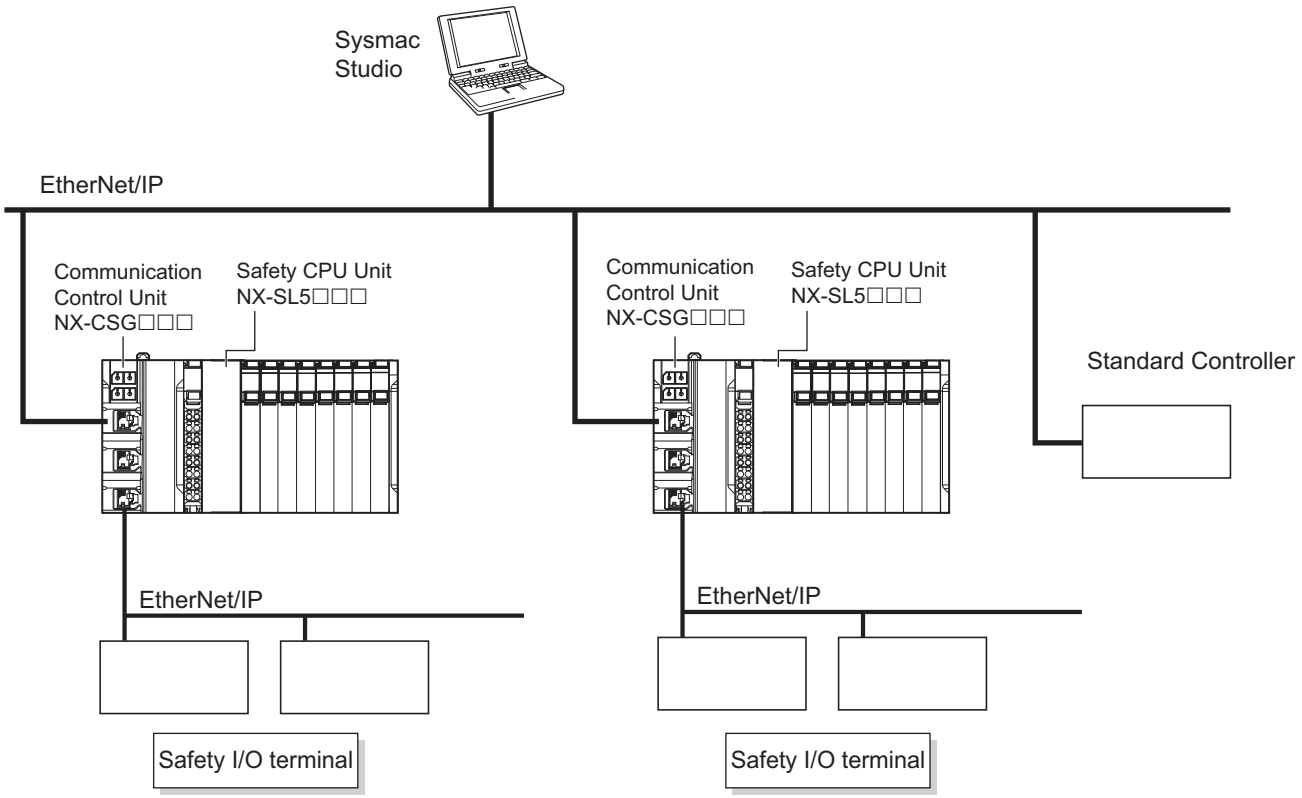
- EtherNet/IP Field Network Configuration
  You can communicate with Safety I/O Terminals via CIP Safety on EtherNet/IP by connecting the built-in EtherNet/IP port of the Communication Control Unit to the EtherNet/IP network. You can also communicate with standard controllers via tag data links or TCP/UDP message communications at the same time.

- Support Software
  The Support Software is connected to the built-in EtherNet/IP port of Communication Control Unit with an Ethernet cable.
  Refer to *3-7-2 Connection* on page 3-62 for details on the connection configuration of the Support Software.



Network Configuration between Controllers

The Safety Network Controller can perform CIP Safety on EtherNet/IP communications with other Safety Network Controllers on the same network when the built-in EtherNet/IP port on the Communication Control Unit is connected to the EtherNet/IP network.


Sysmac
Studio
EtherNet/IP
Communication
Control Unit
NX-CSG□□□
Safety CPU Unit
NX-SL5□□□
Communication
Control Unit
NX-CSG□□□
Safety CPU Unit
NX-SL5□□□
Standard Controller
EtherNet/IP
EtherNet/IP
Safety I/O terminal
Safety I/O terminal

1-2 Procedure

1-2-1 Overall Procedure

Use the following procedure to build a safety control system.

Step 1. System Design
- Step 1-1 Determining Safety Measures by Performing Risk Assessment
- Step 1-2 Selecting Safety Devices
- Step 1-3 Selecting Network Devices
- Step 1-4 Designing the Interface between Standard Controls and Safety Controls
- Step 1-5 Designing the Interface between Safety Controls
- Step 1-6 Designing Device Security

Step 2. Software Design
- Step 2-1 Designing I/O Devices and Processing
- Step 2-2 Designing Safety Programs

Step 2. Hardware Design
- Step 2-1 Determining Wiring for Communications, Power Supply, and External I/O Devices

Step 3 Calculating and Verifying Safety Response Performance
- Step 3-1 Calculating and Verifying Safety Communication Performance
- Step 3-2 Calculating Safety Reaction Times
- Step 3-3 Calculating Safety Distance and Verifying Fulfillment of Required Specifications

Step 4. Software Settings and Programming
- Step 4-1 Creating the Safety Network Controller Configuration
- Step 4-2 Configuring the CIP Safety Communications Settings
- Step 4-3 Configuring the Communications Settings with Standard Controllers
- Step 4-4 Assigning Safety I/O Terminals to the Connected Devices
- Step 4-5 Assigning Device Variables to I/O Ports
- Step 4-6 Exposing Variables to Standard Controllers
- Step 4-7 Programming
- Step 4-8 Offline Debugging

Step 5. Installation and Wiring
- Step 5-1 Installation
- Step 5-2 Wiring the Unit Power Supply and the I/O
- Step 5-3 Wiring the Ethernet Cables
- Step 5-4 Connecting the Computer That Runs the Support Software

Step 6. Checking Operation
- Step 6-1 Transferring Data to the Controller
- Step 6-2 Checking Operation Using the Controller
- Step 6-3 Performing Safety Validation Testing
- Step 6-4 Validating Safety from the Sysmac Studio
- Step 6-5 Setting the Safety Password

Step 7. Operation, Maintenance, and Inspection
- Step 7-1 Operation
- Step 7-2 Troubleshooting Errors If They Occur
- Step 7-3 Inspection and Replacement

1-2-2 Detailed Procedures

Step 1. System Design

Procedure	Description	Reference
Step 1-1 Determining Safety Measures by Performing Risk Assessment	• Identify potential danger factors and perform risk assessment. • Study and decide on measures to reduce risks.	---
Step 1-2 Selecting Safety Devices	Select the safety devices for inputs, logic, and outputs of the safety controls.	*Section 2 System Configuration and Configuration Devices* on page 2-1 *Section 3 Specifications of Configuration Units* on page 3-1
Step 1-3 Selecting Network Devices	In consideration of the network bandwidth, select an Ethernet switch, a twisted-pair cable, and a connector to configure the Ethernet network.	*Selecting the Network Devices* on page 5-39
Step 1-4 Designing the Interface between Standard Controls and Safety Controls	Design the interface between the standard controls and safety controls.	*7-8 Exposing Variables to Standard Controllers* on page 7-53 *6-1-4 Introduction to Tag Data Links* on page 6-4
Step 1-5 Designing the Interface between Safety Controls	Design the interface between safety controls.	*7-5 CIP Safety Communication Settings* on page 7-21
Step 1-6 Designing Device Security	Determine a safety password.	*9-10-1 Setting the Safety Password* on page 9-53

Step 2. Software Design

Procedure	Description	Reference
Step 2-1 Designing I/O Device and Processing	Design the configuration of the I/O devices and I/O Units. • Safety I/O devices • Standard I/O devices • Program contents	*6-3 Safety I/O Function* on page 6-16
		
Step 2-2 Designing Safety Programs	Design the POUs (Program Organization Units). • Programs • Function blocks Design of Variables: • Design the data types of the variables (particularly the design of safety data types and standard data types). • Define the variables that you will use in more than one POU and variables that you will use in only specific POUs. • Define the variable names for the device variables that you use to access Safety I/O Units. • Define the attributes of variables, such as the Name attribute. • Design the variables to expose to the user program for the standard controls. • Design the variables to expose to other user program for the safety controls. Design of Data Protection: • Design POUs to protect and access restrictions.	*Section 8 Programming* on page 8-1 *9-10-2 Data Protection* on page 9-54

Step 2. Hardware Design

Procedure	Description	Reference
Step 2-1 Determining Wiring for Communications, Power Supply, and External I/O Devices	Determine the wiring for the communications network, power supply, and safety I/O devices.	*Section 3 Specifications of Configuration Units* on page 3-1 *Section 4 Designing the Power Supply System* on page 4-1 *6-3 Safety I/O Function* on page 6-16 *Section 5 Installation and Wiring* on page 5-1

Step 3. Calculating and Verifying Safety Response Performance

Procedure	Description	Reference
Step 3-1 Calculating Safety Communications Performance	Calculate safety task period, EPI and FSoE WDT, and verify the bandwidth usage.	*Section 10 Calculating Safety Reaction Times* on page 10-1 *Section 11 Communications Load* on page 11-1
		
Step 3-2 Calculating Safety Reaction Times	Calculate the safety reaction time.	*Section 10 Calculating Safety Reaction Times* on page 10-1
		
Step 3-3 Calculating Safety Distance and Verifying Fulfillment of Required Specifications	Calculate the safety distances from the safety reaction times. Check to see if the safety distances meet the requirements. If requirements are not met, reconsider the designs again starting with the system design.	---

Step 4. Software Settings and Programming

Procedure	Description	Reference
Step 4-1 Creating the Safety Network Controller Configuration	On the Sysmac Studio, configure the Communication Control Unit, Safety CPU Units, Safety I/O Units, and the other NX Units.	*7-3 CPU Rack Configuration and Setup* on page 7-5
		
Step 4-2 Configuring the CIP Safety Communications Settings	Configure the CIP Safety communications settings.	*7-4 EtherNet/IP Network Configuration and Setup* on page 7-9
		
Step 4-3 Configuring the Communications Settings with Standard Controllers	Configure the communication settings with standard controllers.	*7-4 EtherNet/IP Network Configuration and Setup* on page 7-9
		
Step 4-4 Assigning Safety I/O Terminals to the Connected Devices	On the parameter setting page for the Safety I/O Units, select the safety I/O devices that are connected to the safety I/O terminals.	*7-6 Setting the Input and Output Functions* on page 7-42
		
Step 4-5 Assigning Device Variables to I/O Ports	Register the device variables in the global variable table.	*7-7 Assigning Variables to I/O Ports* on page 7-46
		

Procedure	Description	Reference
Step 4-6 Exposing Variables to Standard Controllers	Specify variables to be exposed to the standard controllers.	*7-8 Exposing Variables to Standard Controllers* on page 7-53
⇩		
Step 4-7 Programming	Variable Registration: • Register the variables that are used by more than one POU in the global variable table with the Sysmac Studio. • Register the variables that are used in only a specific program in the local variable table for that program. • Register the variables that are used in only a specific function block in the local variable table for that function block. Writing Algorithms for POUs: Write the algorithms for the POUs (programs and function blocks) using the FBD language.	*8-5 Programming Operations* on page 8-27
⇩		
Step 4-8 Offline Debugging	The Simulator is used to debug the program.	*8-9 Offline Debugging* on page 8-100

Step 5. Installation and Wiring

Procedure	Description	Reference
Step 5-1 Installation	Mount the Units on a DIN Track and connect the Units to each other.	*Section 5 Installation and Wiring* on page 5-1
⇩		
Step 5-2 Wiring the Unit Power Supply and the I/O	Wire cables and connectors of the Communication Control Unit, the Safety I/O Units, and the other NX Units.	*Section 5 Installation and Wiring* on page 5-1
⇩		
Step 5-3 Wiring the Ethernet Cables	Connect the Communication Control Unit to the Ethernet network.	*Section 5 Installation and Wiring* on page 5-1
⇩		
Step 5-4 Connecting the Computer That Runs the Support Software	Connect the computer to the built-in EtherNet/IP port on the Communication Control Unit with an Ethernet cable.	*2-2 Connecting the Support Software* on page 2-5 *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)*

Step 6. Checking Operation

Procedure	Description	Reference
Step 6-1 Transferring Data to the Controller	Place the Sysmac Studio online with the Communication Control Unit and transfer the configuration information from a computer to the Controller. Then, change the Safety CPU Unit to DEBUG mode from the Safety CPU Unit Setup and Programming View. This transfers the safety application data to the Safety CPU Unit and enables debugging.	*9-2 Transferring the Configuration Information* on page 9-6 *9-3 Operating Modes of the Safety CPU Unit* on page 9-8 *9-4 Changing to DEBUG Mode* on page 9-13
↓		
Step 6-2 Checking Operation Using the Controller	Check all wiring and the operation of the program to check that the Safety Control Unit operates as intended.	*9-6 Functions for Checking Operation* on page 9-22
↓		
Step 6-3 Performing Safety Validation Testing	Test all safety functions to see if they operate according to designs.	*9-6 Functions for Checking Operation* on page 9-22
↓		
Step 6-4 Validating Safety from Sysmac Studio	After the safety validation testing has been passed, execute the Safety Validation operation from the Sysmac Studio. This transfers the safety application data to the non-volatile memory in the Safety CPU Unit and enables operation.	*9-11 Performing Safety Validation and Operation* on page 9-59
↓		
Step 6-5 Setting the Safety Password	Set the safety passwords.	*9-10 Security Settings* on page 9-53

Step 7. Operation, Maintenance, and Inspection

Procedure	Description	Reference
Step 7-1 Operation	Restart the Safety CPU Unit. If the Safety CPU Unit has a validated user program, the Safety CPU Unit will automatically start in RUN mode.	*9-11 Performing Safety Validation and Operation* on page 9-59
⇩		
Step 7-2 Troubleshooting Errors If They Occur	If an error occurs, use the troubleshooting function of the Sysmac Studio to check the error and determine the cause. Then, remove the error.	*Section 15 Troubleshooting* on page 15-1
⇩		
Step 7-3 Inspection and Replacement	Perform periodic maintenance. If you find any defects or problems during the inspection, replace the affected devices.	*Section 16 Inspection and Maintenance* on page 16-1

2

System Configuration and Configuration Devices

This section describes how to configure the Safety Network Controller system, and provides information on configuration devices in the system.

2-1 Basic Configuration 2-2
2-1-1 CPU Rack Configuration 2-2
2-1-2 EtherNet/IP Field Network Configuration 2-3
2-1-3 Configuration Units 2-3
2-2 Connecting the Support Software 2-5
2-3 Network Configuration between Controllers 2-6

2-1 Basic Configuration

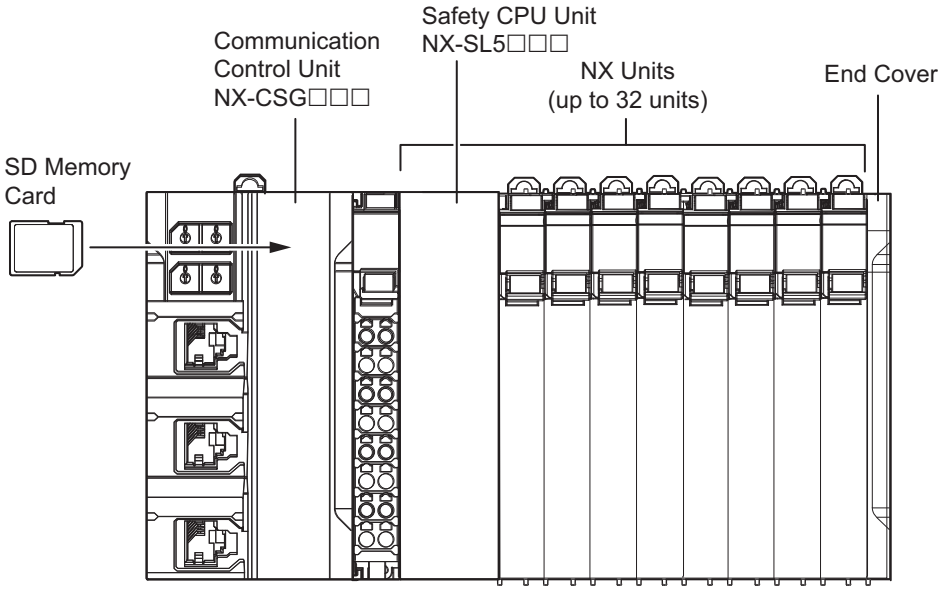
The configuration that includes the Safety CPU Unit, the Communication Control Unit, as well as the Units of which input and output are directly controlled by the Safety CPU Unit and the Communication Control Unit, is called the Basic Configuration.

Basic Configuration is as follows. These configurations can exist together.

- CPU Rack Configuration
- EtherNet/IP Field Network Configuration

2-1-1 CPU Rack Configuration

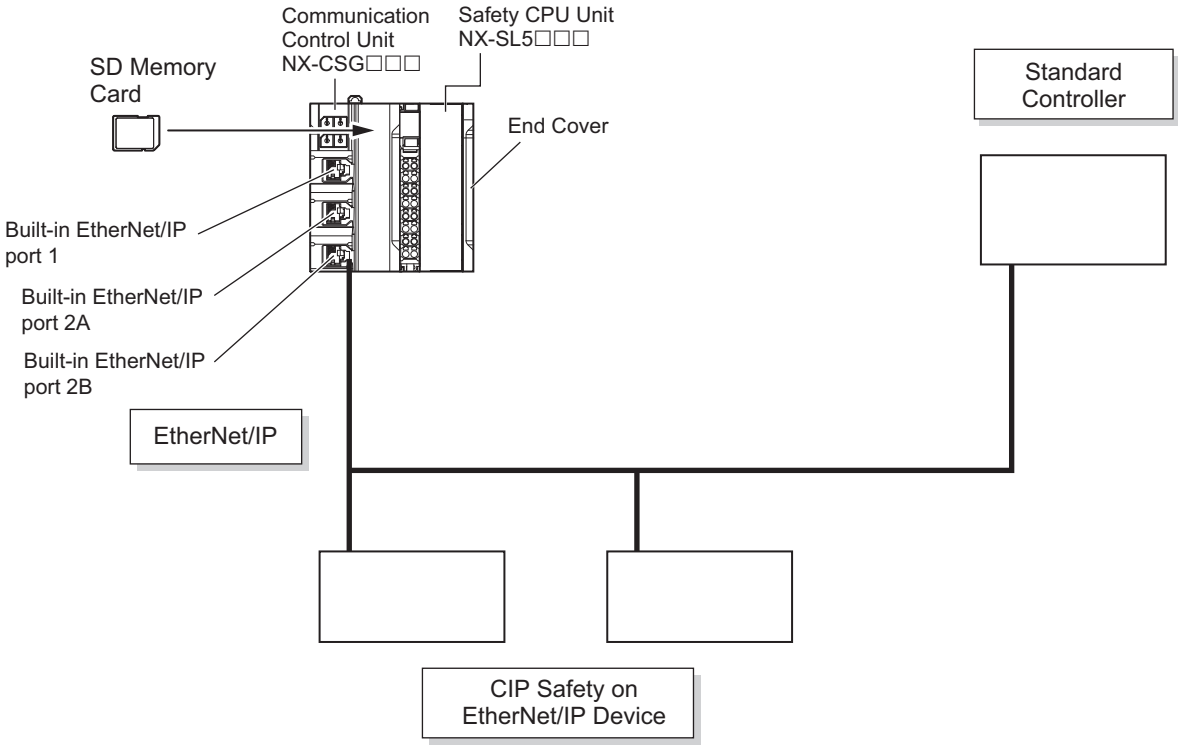
The following shows the CPU Rack Configuration, where NX Units are mounted to a CPU Rack. The CPU Rack is configured with a Communication Control Unit, Safety CPU Unit, Safety I/O Units, other NX Units, and an End Cover mounted to it.
The number of NX Unit connections is up to 32 units.



Configuration		Remarks
Communication Control Unit NX-CSG□□□		One required for every CPU Rack.
End Cover		Must be connected to the right side of the CPU Rack. One end cover is provided with the Communication Control Unit as a standard accessory.
NX Unit	Safety CPU Unit NX-SL5□□□	Up to 32 units can be mounted onto the CPU Rack. One Safety CPU Unit is required for each CPU Rack. Refer to *A-20 Version Information* on page A-115 for the NX Units that you can connect.
	Safety Input Unit	
	Safety Output Unit	
	Other NX Units	
SD Memory Card		Install as required.

2-1-2 EtherNet/IP Field Network Configuration

The EtherNet/IP field network configuration consists of Communication Control Unit, Safety CPU Unit, an End Cover, a device that supports CIP Safety on EtherNet/IP, and a standard controller.
The Safety Network Controller performs communications with devices that support CIP Safety on EtherNet/IP and standard controllers by connecting the built-in EtherNet/IP port of the Communication Control Unit to the EtherNet/IP network.



Configuration		Remarks
Communication Control Unit NX-CSG□□□		One required for every CPU Rack.
End Cover		Must be connected to the right side of the CPU Rack. One End Cover is provided with the Communication Control Unit as a standard accessory.
NX Unit	Safety CPU Unit NX-SL5□□□	One Safety CPU Unit required for every CPU Rack.
SD Memory Card		Install as required.
CIP Safety on EtherNet/IP Device		These are connected to the EtherNet/IP network to which the built-in EtherNet/IP port of the Communication Control Unit is connected.
Standard Controller		

2-1-3 Configuration Units

● Communication Control Unit

The Communication Control Unit has built-in EtherNet/IP ports and relays CIP Safety communications between the Safety CPU Unit and CIP Safety on EtherNet/IP devices. It also supports tag data link communications with standard controllers.
Refer to *3-1 Communication Control Unit* on page 3-2 for the models and specifications of the Communication Control Unit.

● SD Memory Card

When you insert an SD Memory Card into the Communication Control Unit, various data can be saved, backed up, restored and compared using the SD Memory Card.
Refer to *3-6 SD Memory Cards* on page 3-60 for the models and specifications of individual SD Memory Card.

● Safety CPU Unit

This Unit serves as the center of control for the Safety Network Controllers. It is an NX Unit that executes safety programs and safety process data communications.
Refer to *3-2 Safety CPU Unit* on page 3-22 for the models and specifications of Safety CPU Units.

● Safety Input Unit

This is an NX Unit that performs safety input processing.
Refer to *3-3 Safety Input Unit* on page 3-32 for the models and specifications of Safety Input Unit.

● Safety Output Unit

This an NX Unit that performs safety output processing.
Refer to *3-4 Safety Output Unit* on page 3-45 for the models and specifications of Safety Output Unit.

● End Cover

A cover to protect the Communication Control Unit and NX Unit. This is provided with the Communication Control Unit.
Refer to *3-5 End Cover* on page 3-59 for the models and specifications of the end cover.

● Other NX Units

This is an NX Unit that performs standard I/O processing.
Refer to *A-20 Version Information* on page A-115 for the NX Units that you can connect.
Refer to the user's manuals of the each NX Unit for the models and specifications.

● CIP Safety on EtherNet/IP Device

The Safety CPU Unit performs safety controls on devices that are compliant with CIP Safety on EtherNet/IP, such as safety I/O terminals.

● Standard Controller

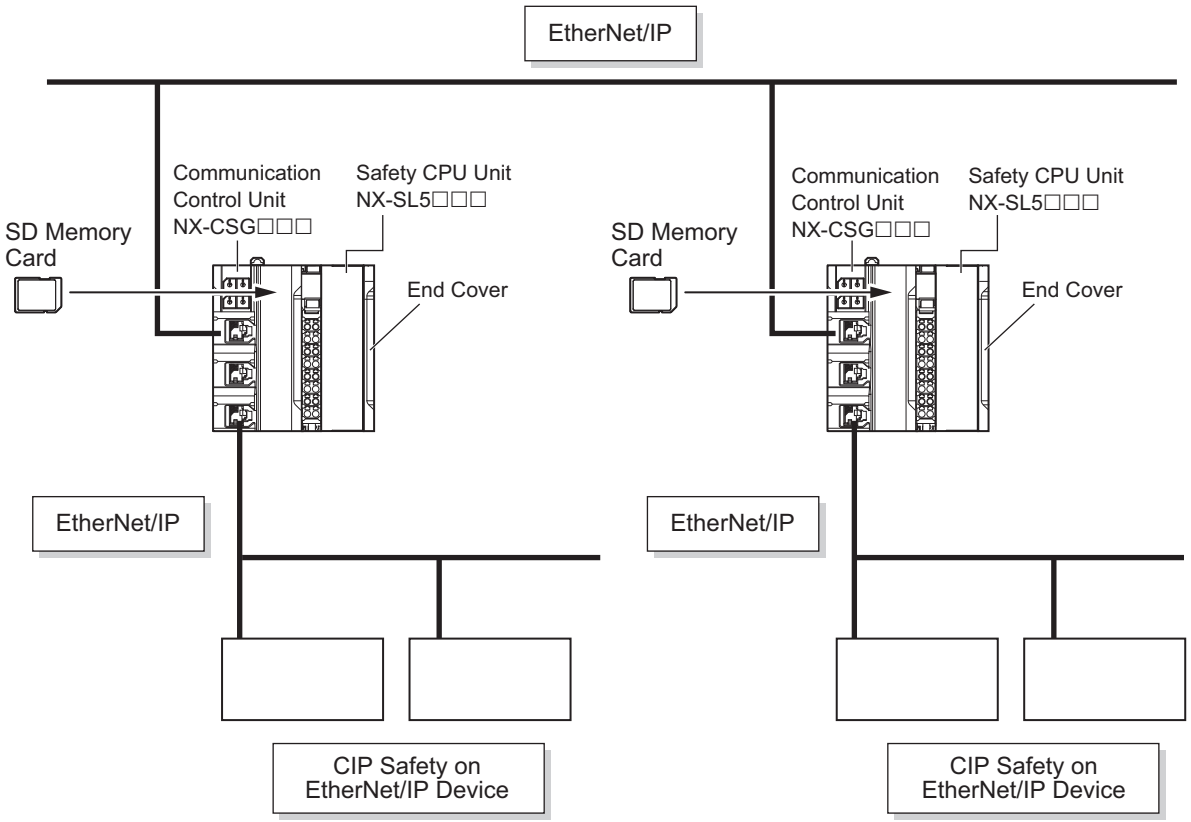
This controller performs I/O communications and message communications with the Safety CPU Unit via the built-in EtherNet/IP port of the Communication Control Unit.

2-2 Connecting the Support Software

The Safety Network Controller and the Support Software can be connected each other via the built-in EtherNet/IP port of the Communication Control Unit. Refer to *3-7-2 Connection* on page 3-62 for information on the connection between Safety Network Controller and the Support Software.

2-3 Network Configuration between Controllers

The network configuration between Controllers consists of multiple Safety Network Controllers. You can configure network between Controllers when you connect the built-in EtherNet/IP ports of Communication Control Unit to the EtherNet/IP network. This network provides CIP Safety on EtherNet/IP communications between multiple network controllers.
For details on configuration devices, refer to *2-1-3 Configuration Units* on page 2-3.



3

Specifications of Configuration Units

This section provides the specifications of the configuration units.

3-1 Communication Control Unit 3-2
3-1-1 Models and Specifications 3-2
3-1-2 Built-in EtherNet/IP Port Specifications 3-7
3-1-3 Part Names and Functions 3-10
3-1-4 Terminal Blocks 3-12
3-1-5 Indicators 3-14
3-1-6 ID Information Indication 3-21

3-2 Safety CPU Unit 3-22
3-2-1 Models and Specifications 3-22
3-2-2 Part Names and Functions 3-26
3-2-3 Indicators 3-27

3-3 Safety Input Unit 3-32
3-3-1 Models and Specifications 3-32
3-3-2 Part Names and Functions 3-38
3-3-3 Indicators 3-40

3-4 Safety Output Unit 3-45
3-4-1 Models and Specifications 3-45
3-4-2 Part Names and Functions 3-52
3-4-3 Indicators 3-55

3-5 End Cover 3-59
3-5-1 Models and Specifications 3-59

3-6 SD Memory Cards 3-60
3-6-1 Models and Specifications 3-60
3-6-2 Purpose 3-60

3-7 Support Software 3-61
3-7-1 Product Model 3-61
3-7-2 Connection 3-62

3-8 PFH 3-63

3-1 Communication Control Unit

This section describes the models and specifications of the Communication Control Unit as well as the names and functions of the parts.

3-1-1 Models and Specifications

This section describes the specifications of the Communication Control Unit.

Models and Outline of Specifications

The models and outline of specifications of the Communication Control Unit are given below.

Model	Supported communications protocol	Number of communications connectors	Network variables
NX-CSG320	EtherNet/IP*1	3	2*2

*1. Routing of the CIP Safety protocol is supported.

*2. PORT1 is an independent port. PORT2A and PORT2B are the ports with a built-in Ethernet switch.

General Specifications

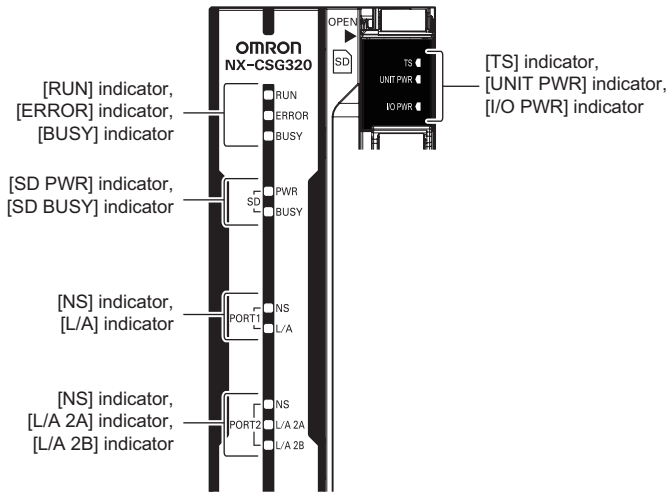
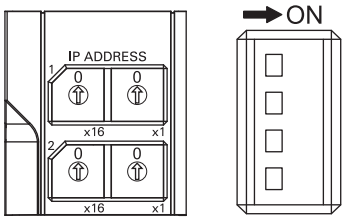
This section provides the general specifications of the Communication Control Unit.

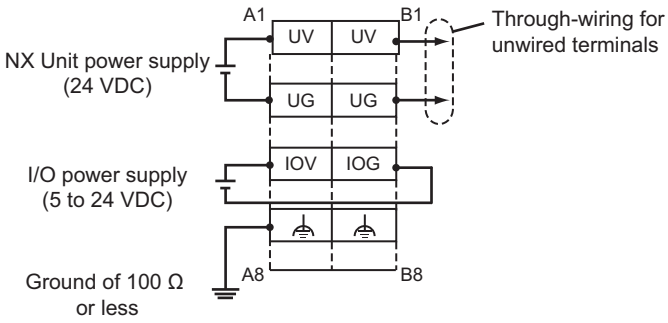
Item		Specification
Enclosure		Mounted in a panel (open type)
Grounding method		Ground to 100 Ω or less
Operating environment	**Ambient operating temperature**	0 to 55°C
	Ambient operating humidity	10% to 95% (with no condensation or icing)
	Atmosphere	Must be free from corrosive gases
	Ambient storage temperature	−25 to 70°C (with no condensation or icing)
	Altitude	2,000 m max.
	Pollution degree	2 or less: Meets IEC 61010-2-201
	Noise immunity	Conforms to IEC 61131-2, 2 kV (power supply line)
	Insulation class	CLASS III (SELV)
	Overvoltage category	Category II: Meets IEC 61010-2-201
	EMC immunity level	Zone B
	Vibration resistance	Conforms to IEC 60068-2-6 5 to 8.4 Hz with amplitude of 3.5 mm 8.4 to 150 Hz, acceleration of 9.8 m/s^2 100 min. in each X, Y, and Z directions (10 sweeps of 10 min. each = 100 min. total)
	Shock resistance	Conforms to IEC 60068-2-27 147 m/s^2 3 times in each X, Y, and Z directions
	Insulation resistance	20 MΩ between isolated circuits (at 100 VDC)
	Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
Installation method		DIN Track mounting (IEC 60715 TH35-7.5/TH35-15)

Individual Specifications

This section provides the individual specifications of Communication Control Unit.

● NX-CSG320

Unit name	Communication Control Unit
Model	NX-CSG320
Indicators	[RUN] indicator, [ERROR] indicator, [BUSY] indicator, [SD PWR] indicator, [SD BUSY] indicator, [NS] indicator x 2, [L/A] indicator, [L/A 2A] indicator, [L/A 2B] indicator, [TS] indicator, [UNIT PWR] indicator, [I/O PWR] indicator 
Hardware switch settings	[IP ADDRESS 1] Switch (x16, x1), [IP ADDRESS 2] Switch (x16, x1), DIP Switch 
Dimensions[*1]	72 × 100 × 90 mm (W × H × D)
Weight[*2]	390 g
Number of NX Units that you can connect	32 units or less
Number of communications that can be set between NX Units	254 ports max.[*6]

Unit power supply	**Power supply voltage**	24 VDC (20.4 to 28.8 VDC)
	Unit power consumption*3	5.95 W
	Inrush current*4	For cold start at room temperature: 10 A max./0.1 ms max. and 2.5 A max./150 ms max.
	Current capacity of power supply terminal*5	4 A
	Isolation method	No isolation: Between the Unit power supply terminal and internal circuit
Power supply to the NX Unit power supply	**NX Unit power supply capacity**	10 W max.
	NX Unit power supply efficiency	80%
	Isolation method	No isolation: Between the Unit power supply terminal and NX Unit power supply
I/O power supply to NX Units	**Power supply voltage**	5 to 24 VDC (4.5 to 28.8 VDC)
	Maximum I/O power supply current	4 A
Current consumption from I/O power supply		10 mA max. (24 VDC)
External connection terminals		Screwless clamping terminal block (8 terminals)
Terminal connection diagram		UV/UG: Unit power supply terminals IOV/IOG: I/O power supply terminals 
Accessories		End cover (NX-END02): 1 pc.
Installation orientation and restrictions		Only upright installation orientation

*1. Includes the End Cover, and does not include projecting parts.
*2. Includes the End Cover. The weight of the End Cover is 82 g.
*3. Includes the SD Memory Card. The NX Unit power consumption to NX Units is not included.
*4. This is the inrush current value when the power supply turns ON after it has been OFF.

The inrush current may vary depending on the operating condition and other conditions. Therefore, select fuses, breakers, and external power supply devices that have enough margin in characteristic and capacity, considering the condition under which the devices are used.
Especially when you turn the power ON/OFF through a switch inserted to the external DC power supply, cycling power ON-OFF-ON within one second will cause the inrush current of approx. 30 A/0.3 mA to occur since the inrush current limiter circuit fails to limit the current.

*5. The amount of current that can be passed constantly through the terminal. Do no exceed this current value when you use a through-wiring for the Unit power supply.

*6. The actual configurable number can be calculated as follows: 254 - <Number of CIP Safety connections configured> - <Number of FSoE connections configured>

3-1-2 Built-in EtherNet/IP Port Specifications

The following table shows the specifications of the built-in EtherNet/IP port of the Communication Control Unit.

Item		Specification
		NX-CSG□□□
Communications protocol		TCP/IP or UDP/IP
Supported services		Sysmac Studio connection, tag data links, CIP message communications, FTP server, automatic clock adjustment (NTP client), SNMP (agent), DNS (client), BOOTP (client), TCP/UDP message service
Number of logical ports		2 (With IP routing function)
Physical layer		100Base-TX or 10Base-T (100Base-TX is recommended.)*1
Transmission specifications	Media access method	CSMA/CD
	Modulation	Baseband
	Transmission paths	Star form
	Baud rate	100 Mbps (100BASE-TX)
	Transmission media	Shielded twisted-pair (STP) cable, Category 5, 5e or higher
	Transmission distance	100 m max. (distance between hub and node)
	Number of cascade connections	The built-in switching ports support up to 50 nodes. There is no limitation when an external Ethernet switch is used.
CIP Safety routing	Maximum number of routable CIP Safety connections	254 total For multi-cast connections, 128 total

Item		Specification
		NX-CSG□□□
CIP service: Tag data links (cyclic communications)	Number of connections	32/Logical ports (total of 64 with two logical ports)
	Packet interval (refresh cycle)	1 to 10,000 ms in 1-ms increments
		Packet intervals can be set independently for each connection. (Data is refreshed over the network at preset intervals and does not depend on the number of nodes.)
	Allowed communications bandwidth per Unit	12000 pps*2
		Note: The heartbeat and CIP Safety routing are included.
	Number of registrable tags	1024/Logical ports (total of 2048 with two logical ports)
	Tag types	Network variables
	Number of tags per connection (= 1 tag set)	32 (31 tags if Controller status is included in the tag set.)
	Maximum link data size per node	46,208 bytes/Logical ports 92,416 bytes total
	Maximum data size per connection	1,444 bytes*3
		Data concurrency is maintained within each connection.
	Number of registrable tag sets	32 per port (1 connection = 1 tag set) (total of 40*4 with two logical ports)
	Maximum size of 1 tag set	1,444 bytes (Two bytes are used if Controller status is included in the tag set.)
	Multi-cast packet filter*5	Supported.
CIP message service: Explicit messages*6	Class 3 (number of connections)	Connections: 16/Logical ports (total of 32 with two logical ports) (server only)
	UCMM (unconnected)	Maximum number of clients that can communicate at one time: 16 per port (total of 32 with two logical ports) Maximum number of servers that can communicate at one time: 16 per port (total of 32 with two logical ports)
TCP/UDP message service	Maximum number of clients that can communicate at one time	16 per port (total of 32 with two logical ports)
	Maximum message size	Request: 492 bytes Response: 496 bytes
SNMP	Agent	SNMPv1, SNMPv2c
	MIB	MIB-II
EtherNet/IP conformance test		Conforms to CT14
Ethernet interface		10BASE-T or 100BASE-TX Auto negotiation or fixed settings

*1. If tag data links are being used, use 100Base-TX.

*2. Here, pps means “packets per second” and indicates the number of packets that can be processed in one second.

*3. To use a data size of 505 bytes or higher, the system must support a large forward open (an optional CIP specification). The CS, CJ, NJ, and NX-series Units support a large forward open, but before connecting to nodes of other companies, confirm that those devices also support it.

*4. If more than 40 tag sets are registered in total, the *Tag Data Link, Too Many Tag Sets Registered (840E0000 hex)* event will occur.

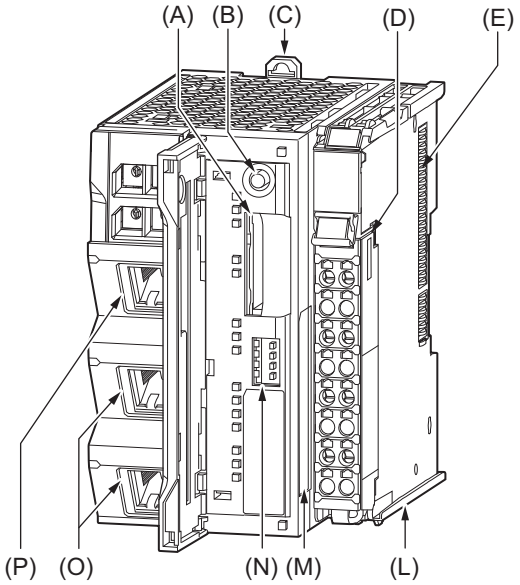
*5. Because the built-in EtherNet/IP port is equipped with an IGMP client (version 2), unnecessary multicast packets can be filtered out by an Ethernet switch that supports IGMP Snooping.

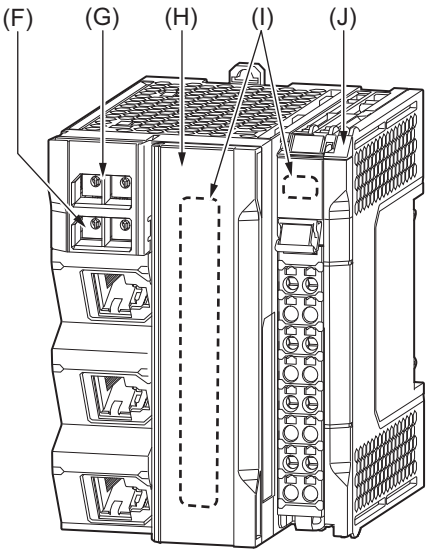
*6. The built-in EtherNet/IP port uses the TCP/UDP port numbers shown in the following table.
Do not set the same port number for more than one TCP/UDP service.

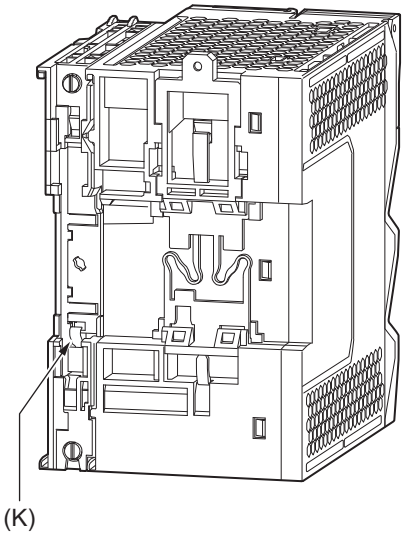
Service	Type	Port number	Remarks
Tag data links	UDP	2222	Fixed values
Used by system	UDP	2223, 2224	
	TCP	9610	
CIP messages	TCP	44818	
FTP client (Data transfer port)	TCP	20	
DNS client	TCP/UDP	53	
BOOTP client	UDP	68	
HTTP server	TCP	80	
Used by system, other	TCP/UDP	9600	You can change the port number in the Unit Settings on the Sysmac Studio.
FTP client (Control port)	TCP	21	
TCP/UDP message service	TCP/UDP	64000	
NTP client	UDP	123	
SNMP agent	UDP	161	
SNMP trap	UDP	162	

3-1-3 Part Names and Functions

This section provides the part names and functions of Communication Control Unit.







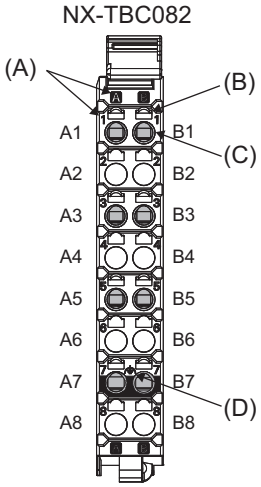
Letter	Name	Function
(A)	SD Memory Card connector	Connects the SD Memory Card to the Communication Control Unit.
(B)	SD Memory Card power supply switch	Turns OFF the power supply so that you can remove the SD Memory Card. Refer to *5-2-8 Installing and Removing the SD Memory Card* on page 5-21.
(C)	DIN Track mounting hooks	These hooks are used to mount the Unit to a DIN Track.
(D)	Terminal Block	Used for wiring the power supply and functional grounding wire.
(E)	NX bus connector	This connector is used to connect the Communication Control Unit to the NX Unit on the right of the Communication Control Unit.

Letter	Name	Function
(F)	IP Address Switch 2 (x16, x1)	Used for setting an IP address for the built-in EtherNet/IP port (PORT2A and PORT2B). Use the rotary switches and specify a two-digit hexadecimal number. Refer to *7-4-1 Setting IP Addresses* on page 7-9.
(G)	IP Address Switch 1 (x16, x1)	Used for setting an IP address for the built-in EtherNet/IP port (PORT1). Use the rotary switches and specify a two-digit hexadecimal number. Refer to *7-4-1 Setting IP Addresses* on page 7-9.
(H)	SD Memory Card cover	A cover for the SD Memory Card DIP switch area. It opens in the horizontal direction.
(I)	Operation Status Indicators	Show the operation status of Communication Control Unit by multiple indicators.
(J)	End Cover	A cover to protect the Communication Control Unit and NX Unit. One End Cover is provided with the Communication Control Unit as a standard accessory.
(K)	DIN Track contact plate	This plate is used to contact the functional ground terminal with a DIN Track.
(L)	Unit hookup guides	These guides are used to mount NX Units or End Cover.
(M)	ID Information Indication	Shows the ID information of the Unit.
(N)	DIP Switch	Used for backups. Normally, turn OFF all of the pins. Refer to *13-2 SD Memory Card Backups* on page 13-10.
(O)	Built-in EtherNet/IP Port (PORT2)	Connects the built-in EtherNet/IP with an Ethernet cable. PORT2 consists of two RJ45 connectors (PORT2A and PORT2B) and has a built-in Ethernet switch.
(P)	Built-in EtherNet/IP Port (PORT1)	Connects the built-in EtherNet/IP with an Ethernet cable.

3-1-4 Terminal Blocks

The terminal blocks on the Communication Control Unit are removable screwless clamping terminal blocks that allow you to easily connect and remove the wiring.
Use the NX-TBC082 for the Communication Control Unit.
Connect the Unit power supply, I/O power supply, and ground wire to the screwless clamping terminal block.
For details on wiring, refer to *5-3 Wiring* on page 5-32.

Terminal Block Part Names and Functions



8-terminal type

Letter	Name	Function
(A)	Terminal number indications	The terminal numbers are given by column letters A and B, and row numbers 1 to 8. The combination of the "column" and "row" gives the terminal numbers from A1 to A8 and B1 to B8. The terminal number indicators are the same regardless of the number of terminals on the terminal block, as shown above.
(B)	Release hole	Insert a flat-blade screwdriver into these holes to connect or remove the wires.
(C)	Terminal hole	The wires are inserted into these holes.
(D)	Ground terminal mark	This mark indicates the ground terminals.

Terminal Blocks come in three types depending on the number of terminals that can be used. There are 8-terminal, 12-terminal, and 16-terminal Terminal Blocks.
Only the 8-terminal type terminal block is compatible with Communication Control Unit.
To prevent incorrect insertion, terminal blocks in any other types besides the 8-terminal type cannot be mounted.

Additional Information

The 8-terminal type does not have terminal holes and release holes for following terminal numbers.
- A2, A4, A6, A8, B2, B4, B6, and B8

Applicable Terminal Blocks for Each Model

Current capacity of power supply terminals and applicable terminal blocks for each model of Communication Control Unit are shown in the following table.

Unit model number	Current capacity of power supply terminal for the Unit		Terminal block			
	Unit power supply	I/O power supply	Terminal block model	Number of terminals	Ground terminal mark	Terminal current capacity
NX-CSG320	4 A		NX-TBC082	8	Provided	10 A

Precautions for Correct Use

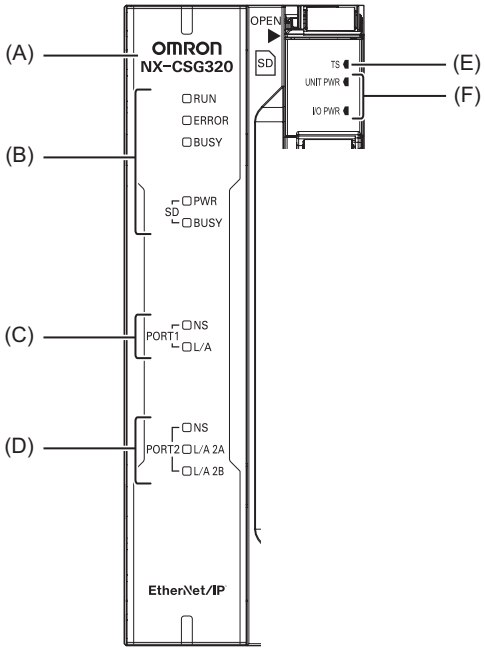
Current capacity of power supply terminal for NX-CSG320 is 4 A or less. Make sure that each current rating of the Unit power supply and I/O power supply does not change if you mount an NX-TBC082 Terminal Block that has terminal current capacity of 10 A.

3-1-5 Indicators

This section describes the indicators of Communication Control Unit.

Note that the appearance of the indicators is different for the Unit with the lot number representing the date on or before March 19, 2019, from that representing the date on or after March 20, 2019. This manual shows the indicators for lot numbers representing the date on or after March 20, 2019.

For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-20.
Refer to *Notation of Unit Versions on Products* on page 44 for how to identify the lot number of the Unit.



Letter	Name	Function
(A)	Model number display	Displays the model information of Communication Control Unit.
(B)	Communication Control Unit Status Indicators	The indicators show the current operating status of Communication Control Unit.
(C)	Built-in EtherNet/IP Status Indicators (PORT1)	The indicators show the communications status of Built-in EtherNet/IP Port (PORT1).
(D)	Built-in EtherNet/IP Status Indicators (PORT2)	The indicators show the communications status of Built-in EtherNet/IP Port (PORT2).
(E)	NX Bus Status Indicators	These indicators show the communications status with Communication Control Unit and NX Units.
(F)	Power Status Indicators	Show the power supply status of the Unit and I/O power supply.

Communication Control Unit Status Indicators

These indicators show the major operating status of Communication Control Unit.

Precautions for Safe Use

- Never turn OFF the power supply to the Communication Control Unit when the BUSY indicator is flashing. While the BUSY indicator is flashing, a backup of the setting values into the built-in non-volatile memory is in progress. If you turn the power OFF during that time, the backup will fail. In addition, the controller error in the major fault level occurs at the next start-up, which causes the operation to stop.
- Never turn the power OFF or remove the SD Memory Card while the card is in use (SD BUSY indicator is flashing). This may cause data corruption, and the data may not work as intended. To remove the SD Memory Card from the Communication Control Unit while the power supply is ON, press the SD Memory Card power supply switch first. Make sure that the SD BUSY Indicator and the SD PWR Indicator are turned OFF before you remove the SD Memory Card.

The status indicators for the Communication Control Unit (RUN, ERROR, BUSY, SD PWR, and SD BUSY indicators) allow you to check the operating status of Communication Control Unit.
For details on how to check the operating status of the Communication Control Unit, refer to *15-1 Operation after an Error* on page 15-2.

The meaning of the indicators is shown below.

● RUN Indicator

The RUN indicator shows the operating status of Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The Unit is operating normally.
		Flashing	The Unit is starting up.
---		Not lit	The CPU reset is in progress or any of the following errors is present. • Major fault level Controller error • CPU Unit Watchdog Timer Error

● ERROR Indicator

The ERROR indicator shows the error status of Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Red		Lit	Any of the following errors was detected during self-diagnosis. • Major fault level Controller error • CPU error
		Flashing (at 1-s intervals)	Any of the following errors was detected during self-diagnosis. • Partial fault level Controller error • Minor fault level Controller error
---		Not lit	Operating normally or resetting CPU, or observation occurred.

● BUSY Indicator

The BUSY indicator shows the status of access to the built-in non-volatile memory of Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Flashing	Built-in non-volatile memory of Communication Control Unit access in progress.
---		Not lit	Built-in non-volatile memory of Communication Control Unit access not in progress.

● SD PWR Indicator

The SD PWR indicator shows the status of power supplied to the SD Memory Card of Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	Power is currently supplied to the SD Memory Card, and the SD Memory Card is available for use.
		Flashing	A backup, restore or verification operation is in progress.
---		Not lit	Power feeding for the SD Memory Card is currently suspended, the SD Memory Card is not inserted, or the file format of the inserted SD Memory Card is not supported.

● SD BUSY Indicator

The SD BUSY indicator shows the status of access to the SD Memory Card of Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Flashing	SD Memory Card access in progress.
---		Not lit	SD Memory Card access not in progress.

Built-in EtherNet/IP Status Indicators (PORT1)

These indicators show the operation status of the built-in EtherNet/IP port (PORT1) of the Communication Control Unit.

The meaning of the indicators is shown below.

● NS Indicator

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	CIP Connections are established.
		Flashing (at 1-s intervals)	CIP Connections are not established.
Red		Lit	The same IP address is used more than once.
		Flashing (at 1-s intervals)	A communications error occurred.
---		Not lit	The main power is OFF or reset.

● L/A Indicator

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Lit	The link was established.
		Flashing	The link was established and data communications are in progress.
---		Not lit	The link was not established. • The cable was not connected • The main power is OFF or reset

Built-in EtherNet/IP Status Indicators (PORT2)

These indicators show the operation status of the built-in EtherNet/IP port (PORT2) of the Communication Control Unit.

The meaning of the indicators is shown below.

● NS Indicator

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	CIP Connections are established.
		Flashing (at 1-s intervals)	CIP Connections are not established.
Red		Lit	The same IP address is used more than once.
		Flashing (at 1-s intervals)	A communications error occurred.
---		Not lit	The main power is OFF or reset.

● L/A 2A Indicator

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Lit	The link was established.
		Flashing	The link was established and data communications are in progress.
---		Not lit	The link was not established. • The cable was not connected • The main power is OFF or reset

● L/A 2B Indicator

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Lit	The link was established.
		Flashing	The link was established and data communications are in progress.
---		Not lit	The link was not established. • The cable was not connected • The main power is OFF or reset

NX Bus Status Indicators

These indicators show the communications status of Communication Control Unit and NX Units.

The meaning of the indicators is shown below.

● TS Indicator

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The Unit is operating normally.
		Flashing (at 1-s intervals)	The initialization is in progress.
Red		Lit	A hardware error, WDT error, or other critical error has occurred.
		Flashing (at 1-s intervals)	An NX bus communications error, I/O allocation information data error, or other recoverable minor error caused by the NX bus has occurred.
---		Not lit	One of the following: • There is no Unit power supply • Restarting the Unit • Waiting for initialization to start

Power Status Indicators

These indicators show the power supply status of Communication Control Unit.

The meaning of the indicators is shown below.

● UNIT PWR Indicator

The UNIT PWR indicator displays the status of the Unit power supply.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	Power is currently supplied from the Unit power supply.
---		Not lit	Power is currently not supplied from the Unit power supply.

● I/O PWR Indicator

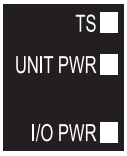
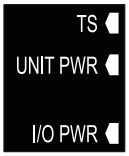
The I/O PWR indicator displays the status of I/O power supply.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The I/O power is supplied.
---		Not lit	The I/O power is not supplied.

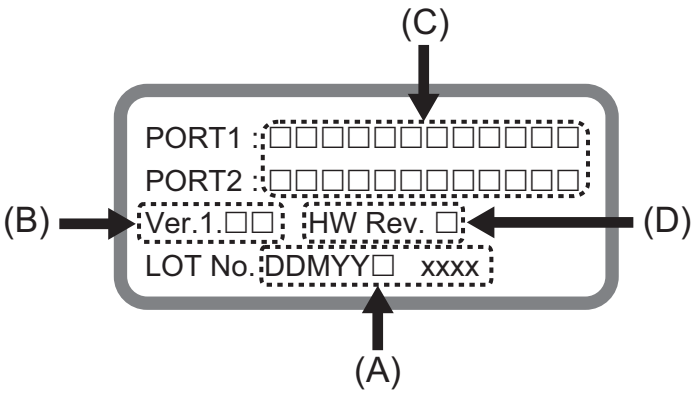
Differences in Appearance of the Indicators

The appearance of the indicators is different for the Unit with the lot number representing the date on or before March 19, 2019, from that representing the date on or after March 20, 2019.
The following table shows how the appearance of the indicators is different depending on the lot number.

Indicator	Description	Lot number	
		On or before March 19, 2019	On or after March 20, 2019
TS indicator UNIT PWR indicator I/O PWR indicator	The shape of the light emitting parts is changed from a square to a pentagon.		

3-1-6 ID Information Indication

ID Information of Communication Control Unit is given on the ID information indication on the left side of the Unit.



Letter	Name	Function
(A)	Lot number and serial number	Shows the lot number and the serial number of the this Unit. DDMYY: Lot number, □: For use by OMRON, SSSS: Serial number For M, 1: January to 9: September, X: October, Y: November, Z: December.
(B)	Unit version	Shows the unit version of the this Unit.
(C)	MAC addresses	Shows the MAC addresses of the built-in EtherNet/IP port (port 1 and port 2) on the this Unit.
(D)	Hardware revision	Shows the hardware revision of the this Unit.*1

*1. The hardware revision is not displayed for the Unit that the hardware revision is in blank.

3-2 Safety CPU Unit

This section describes the models and specifications of the Safety CPU Units as well as the names and functions of the parts.

3-2-1 Models and Specifications

The Safety CPU Unit specifications are described below.

Models

The following table specifies the list of Safety CPU Unit models.

Model	Maximum number of safety I/O points	Program capacity	Number of safety I/O connections	I/O refreshing method
NX-SL5500	1,024 points	2,048 KB	128	Free-Run refreshing
NX-SL5700	2,032 points	4,096 KB	254	Free-Run refreshing

General Specifications

This section provides the general specifications of the Safety CPU Unit.

Item		Specification
Enclosure		Mounted in a panel (open)
Grounding method		Ground to 100 Ω or less
Operating environment	**Ambient operating temperature**	0 to 55°C
	Ambient operating humidity	10% to 95% (with no condensation or icing)
	Atmosphere	Must be free from corrosive gases.
	Ambient storage temperature	−25 to 70°C (with no condensation or icing)
	Altitude	2,000 m max.
	Pollution degree	2 or less: Meets IEC 61010-2-201
	Noise immunity	Conforms to IEC 61131-2, 2 kV (power supply line)
	Insulation class	CLASS III (SELV)
	Overvoltage category	Category II: Meets IEC 61010-2-201
	EMC immunity level	Zone B
	Vibration resistance	Conforms to IEC 60068-2-6 5 to 8.4 Hz with amplitude of 3.5 mm 8.4 to 150 Hz, acceleration of 9.8 m/s^2 100 min. in each X, Y, and Z directions (10 sweeps of 10 min. each = 100 min. total)
	Shock resistance	Conforms to IEC 60068-2-27 147 m/s^2, 3 times in each X, Y, and Z directions
Installation method		DIN Track (IEC 60715 TH35-7.5/TH35-15)

Individual Specifications

This section provides the individual specifications of the Safety CPU Unit.

● Datasheet Items for Safety CPU Unit

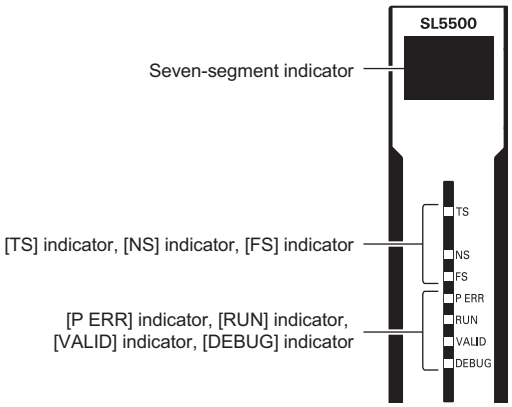
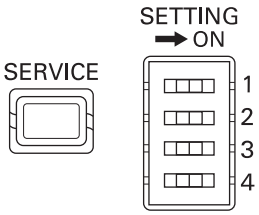
The following table gives the meaning of the datasheet items for the Safety CPU Unit.

Item	Description
Maximum number of safety I/O points	This is the number of safety I/O points that Safety CPU Unit can control.
Program capacity	This is the capacity of the safety programs in the Unit.
Number of safety I/O connections*1	This is the maximum number of Safety I/O connections that can be set to this Unit. The value is the total number of CIP Safety originator connections, CIP Safety target connections, and FSoE master connections.
Number of CIP Safety originator connections*2	This is the maximum number of CIP Safety originator connections that can be set to this Unit.
Number of CIP Safety target connections*2	This is the maximum number of CIP Safety target connections that can be set to this Unit.
Number of originators that can be connected with a multi-cast connection	When this unit is a CIP Safety target, it is the number of CIP Safety originators that can be connected with a multi-cast connection by a single CIP Safety target connection.
CIP Safety maximum data size per connection	This is the maximum data size per connection for CIP Safety.
Number of FSoE master connections	It is the maximum number of FSoE master connections that can be configured to this unit.
I/O refreshing method	The I/O refreshing methods that are used by the Unit.
External connection terminals	The type of terminal block and connector that is used for connecting the Unit. This specification includes the number of terminals for a screwless clamping terminal block.
Indicators	The type of indicators on the Unit and the layout of those indicators.
Hardware switch settings	It is the type and layout of hardware switches for the Unit.
Dimensions (mm)	These are the external dimensions of the Unit. The dimensions are given in the form W × H × D. The dimensions are given in "millimeters".
I/O power supply method	The method for supplying I/O power for the Unit. The supply method is determined for each Unit. The power can be supplied either from the NX bus or from an external source.
Current capacity of I/O power supply terminal	The current capacity of the I/O power supply terminals (IOV/IOG) of the Unit. Do not exceed this value when supplying the I/O power to the connected external devices.
NX Unit power consumption	The power consumption of the NX Unit power supply of the Unit.
Current consumption from I/O power supply	The current consumption from I/O power supply of the Unit. This value does not include the load current of any external connection loads or the current consumption of any connected external devices.
Weight	The weight of the Unit.
Installation orientation and restrictions	This is the installation orientation of the Unit. Any restrictions to specifications that result from the installation orientation are also given.

*1. Refer to *6-1-5 Calculating the Number of Connections* on page 6-9 for how to calculate the number of connections.

*2. The number of CIP Safety connections that can be actually set depends on the maximum number of routable CIP Safety connections of the Communication Control Unit.
For NX-CSG320, the maximum number of routable CIP Safety connections is 254.

● NX-SL5500

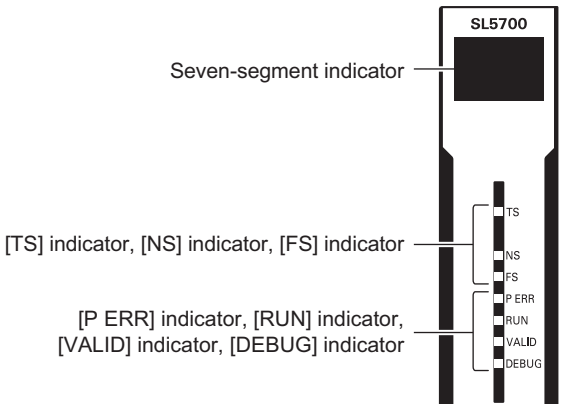
Item	Specification
Maximum number of safety I/O points	1,024 points
Program capacity	2,048 KB
Number of safety I/O connections	128
Number of CIP Safety originator connections	128
Number of CIP Safety target connections	4
Number of originators that can be connected with a multi-cast connection	8
CIP Safety maximum data size per connection	16 bytes
Number of FSoE master connections	128
I/O refreshing method	Free-Run refreshing
External connection terminals	None
Indicators	[TS] indicator, [NS] indicator, [FS] indicator, [P ERR] indicator, [RUN] indicator, [VALID] indicator, [DEBUG] indicator, seven-segment indicator 
Hardware switch settings	[SERVICE] switch, [SETTING] switch 
Dimensions (mm)	30 × 100 × 71 mm (W × H × D)
I/O power supply method	Not supplied.
Current capacity of I/O power supply terminal	No I/O power supply terminals
NX Unit power consumption*1	3.35 W max.
Current consumption from I/O power supply	No consumption
Weight	130 g max.

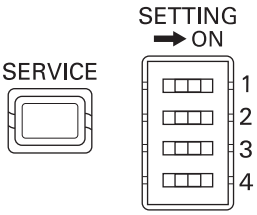
Item	Specification
Installation orientation and restrictions*2	Installation orientation: Upright installation Restriction: None.

*1. The cable length for the Units (Communication Control Unit and the Power Supply Unit for NX Units) that supply power to the corresponding Unit must be up to 20 m.

*2. Only NX502 CPU Units, NX102 CPU Units, and Communication Control Units can be connected. NX1P2 CPU Units or Communications Coupler Units cannot be connected.

● NX-SL5700

Item	Specification
Maximum number of safety I/O points	2,032 points
Program capacity	4,096 KB
Number of safety I/O connections	254
Number of CIP Safety originator connections	254
Number of CIP Safety target connections	4
Number of originators that can be connected with a multi-cast connection	8
CIP Safety maximum data size per connection	16 bytes
Number of FSoE master connections	254
I/O refreshing method	Free-Run refreshing
External connection terminals	None
Indicators	[TS] indicator, [NS] indicator, [FS] indicator, [P ERR] indicator, [RUN] indicator, [VALID] indicator, [DEBUG] indicator, seven-segment indicator 

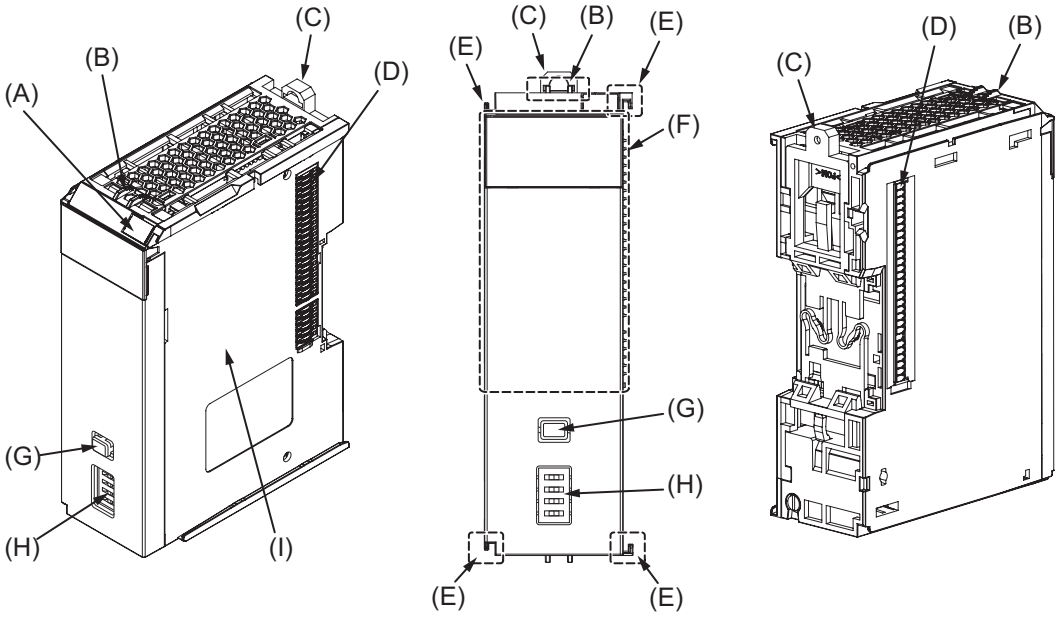
Item	Specification
Hardware switch settings	[SERVICE] switch, [SETTING] switch 
Dimensions (mm)	30 × 100 × 71 (W × H × D)
I/O power supply method	Not supplied.
Current capacity of I/O power supply terminals	No I/O power supply terminals
NX UnitPower consumption*1	3.35 W
Current consumption from I/O power supply	No consumption
Weight	130 g max.
Installation orientation and restrictions*2	Installation orientation: Upright installation Restriction: None.

*1. The cable length for the Units (Communication Control Unit and Power Supply Unit for NX Units) that supply power to the corresponding Unit must be up to 20 m.

*2. Only NX502 CPU Units, NX102 CPU Units, and Communication Control Units can be connected. NX1P2 CPU Units or Communications Coupler Units cannot be connected.

3-2-2 Part Names and Functions

This section describes the names and functions of the Safety CPU Unit components.



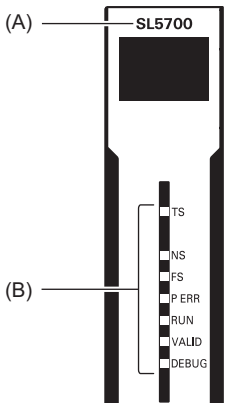
Letter	Name	Function
(A)	Marker attachment locations	The locations where markers are attached. The markers made by OMRON are installed for the factory setting. Commercially available markers can also be installed. Refer to *5-2-7 Attaching Markers* on page 5-20.
(B)	Protrusions for removing the Unit	The protrusions to hold when removing the Unit.
(C)	DIN Track mounting hook	This hook is used to mount the NX Unit to a DIN Track.
(D)	NX bus connector	This is the NX-series bus connector.
(E)	Unit hookup guides	These guides are used to connect two Units.
(F)	Indicators	The indicators show the current operating status and power supply status of the Safety CPU Unit. Refer to *3-2-3 Indicators* on page 3-27.
(G)	Service switch	This switch is used for the start trigger of various functions.
(H)	DIP switch	This switch is used for the Safety Unit Restore and the safety data logging function. Refer to *12-1-2 Safety Unit Restore Function* on page 12-3 for details on the Safety Unit Restore. Refer to *14-3 Safety Data Logging Operation Procedure* on page 14-6 for details on the Safety Data Logging function.
(I)	Unit specifications	The specifications of the Safety CPU Unit are given.

3-2-3 Indicators

The Safety CPU Unit has indicators that show the current operating status and communications status.

⚠ WARNING

Do not use the status of the indicators on the NX-series Safety Control Units for safety operations.
This will compromise the safety functions of the Unit and may cause serious injury in the event of an accident.

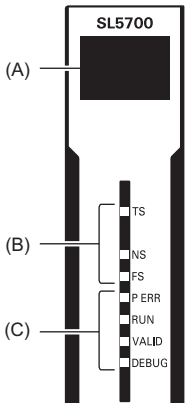


Letter	Name	Function
(A)	Model number display	Displays part of the model number of the Safety CPU Unit.

Letter	Name	Function
(B)	Indicators	Show the current operating status and communications status of the Safety CPU Unit.

Safety CPU Unit Operation Status Indicators

Indicators to show the operation status of the Safety CPU Unit are located in the center of the front side of the Safety CPU Unit.



Letter	Name
(A)	• Seven-segment indicator
(B)	• [TS] indicator • [NS] indicator • [FS] indicator
(C)	• [P ERR] indicator • [RUN] indicator • [VALID] indicator • [DEBUG] indicator

The following section describes the specifications of each indicator.

● TS Indicator

The TS indicator shows the current status of the Safety CPU Unit and the communications status with the Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The Unit is operating normally.
		Flashing (at 2-s intervals)	Initialization is in progress (from when the power supply is turned ON until RUN or PROGRAM mode is entered), or I/O allocation information data is being downloaded from the Sysmac Studio.
Red		Lit	A hardware error, WDT error, or other critical error has occurred.
		Flashing (at 1-s intervals)	An NX bus communications error, I/O allocation information data error, or other recoverable minor error that is attributed to the NX bus has occurred.

Color	Status		Meaning
---		Not lit	• There is no Unit power supply • The Unit is restarting • Waiting for initialization to start

● NS Indicator

The NS indicator shows the CIP Safety communications status of the Safety CPU Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The CIP Safety connections are established.
		Flashing (at 1-s intervals)	The CIP Safety connections are not established.
Red		Flashing (at 1-s intervals)	A CIP Safety communications error occurred.*1
---		Not lit	The CIP Safety communications are not executed.

*1. For approximately 30 seconds after the power supply to the Safety CPU Unit is turned ON, the *CIP Safety Target Does Not Exist* is not registered as an error. During that time, the NS indicator will flash red.

● FS Indicator

The FS indicator shows the FSoE communications status of the Safety CPU Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	All FSoE connections are established.
		Flashing (at 1-s intervals)	The FSoE connections are being established.
Red		Flashing (at 1-s intervals)	An FSoE communications error occurred.*1
---		Not lit	FSoE communications are not executed.

*1. For approximately 30 seconds after the power supply to the Safety CPU Unit is turned ON, a *FSoE Master Connection Not Established Error* event is not registered as an error if the Safety I/O Units do not exist. During that time, the FS indicator will flash green.

● P ERR Indicator

The P ERR indicator shows the error status of the running program or settings of the Safety CPU Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Red		Lit	The safety program, CIP Safety communications, and FSoE communications stopped due to the running program or settings, which resulted in error.
		Flashing (at 1-s intervals)	Local error occurred in the running program.

Color	Status		Meaning
---		Not lit	No errors in the running program or settings

● RUN Indicator

The RUN indicator shows the execution status of the programs for the Safety CPU Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	Execution of a safety program is in progress (operation is in progress in RUN mode, or DEBUG mode (RUN)).
		Flashing (at 1-s intervals)	Initialization is in progress (from when the power supply is turned ON until RUN or PROGRAM mode is entered).
---		Not lit	Operation is in progress in PROGRAM mode or DEBUG mode (STOPPED), or a fatal fault has occurred.

● DEBUG Indicator

The DEBUG indicator shows the status whether the debug function can be executed on Safety CPU Unit.
Refer to *8-9-3 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing* on page 8-103 for the debug function of Safety CPU Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Lit	Operation is in progress in DEBUG mode. (the debug function can be executed)
---		Not lit	Operation is in progress in a mode other than DEBUG mode or a fatal fault has occurred. (the debug function cannot be executed)

● VALID Indicator

The VALID indicator shows whether safety validation has been performed on the safety application data in the Safety CPU Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Yellow		Lit	Safety application data from the execution of the safety validation is stored in the non-volatile memory.
---		Not lit	Safety application data from the execution of the safety validation is not stored in the non-volatile memory, or a fatal fault has occurred.

● Seven-segment Indicator

The two-digit seven-segment indicator shows the detailed information on the Safety CPU Unit.

Item	Meaning
At normal operation	It shows the lowest one byte of the safety signature for the safety program that is operating. If the safety signature is not confirmed, "—" is displayed. While a CIP Safety originator connection is being established, the indicator flashes. When all the CIP Safety originator connections are established, the indicator is lit.
When an error occurs	Refer to *15-2-5 Troubleshooting Errors in the Safety Control Unit* on page 15-35.
When a signature code is checked	Refer to *A-14 Checking the Signature Code on the Seven-segment Indicator* on page A-104.
When the Safety Unit Restore is executed	Refer to *12-1-2 Safety Unit Restore Function* on page 12-3.
When the Safety Data Logging is executed	Refer to *14-4 Checking the Logging Status* on page 14-7.

3-3 Safety Input Unit

This section describes the models and specifications of the Safety Input Units as well as the names and functions of the parts.

3-3-1 Models and Specifications

The Safety Input Unit specifications are described below.

Models

The following table specifies the list of Safety Input Unit models.

Model	Number of safety input points	Number of test output points	Internal I/O common	Rated input voltage	OMRON Special Safety Input Devices	Number of safety slave connections	I/O refreshing method
NX-SIH400	4 points	2 points	Sinking inputs (PNP)	24 VDC	Can be connected.	1	Free-Run refreshing
NX-SID800	8 points	2 points	Sinking inputs (PNP)	24 VDC	Cannot be connected.	1	Free-Run refreshing

General Specifications

This section provides the general specifications of the Safety Input Unit.

Item	Specification
Enclosure	Mounted in a panel (open)
Grounding method	Ground to 100 Ω or less

Item		Specification
Operating environment	**Ambient operating temperature**	0 to 55°C
	Ambient operating humidity	10% to 95% (with no condensation or icing)
	Atmosphere	Must be free from corrosive gases.
	Ambient storage temperature	−25 to 70°C (with no condensation or icing)
	Altitude	2,000 m max.
	Pollution degree	2 or less: Meets IEC 61010-2-201
	Noise immunity	Conforms to IEC 61131-2, 2 kV (power supply line)
	Insulation class	CLASS III (SELV)
	Overvoltage category	Category II: Meets IEC 61010-2-201
	EMC immunity level	Zone B
	Vibration resistance	Conforms to IEC 60068-2-6 5 to 8.4 Hz with amplitude of 3.5 mm 8.4 to 150 Hz, acceleration of 9.8 m/s^2 100 min. in each X, Y, and Z directions (10 sweeps of 10 min. each = 100 min. total)
	Shock resistance	Conforms to IEC 60068-2-27 147 m/s^2, 3 times in each X, Y, and Z directions
	Isolation method	Photocoupler isolation
	Insulation resistance	20 MΩ between isolated circuits (at 100 VDC)
	Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
Installation method		DIN Track (IEC 60715 TH35-7.5/TH35-15)

Individual Specifications

This section provides the individual specifications of the Safety Input Unit.

● Datasheet Items for Safety Input Unit

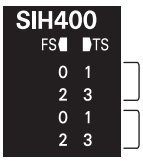
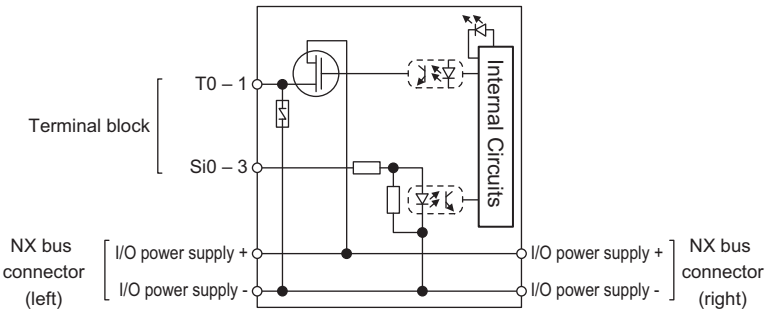
The following table gives the meaning of the datasheet items for the Safety Input Units.

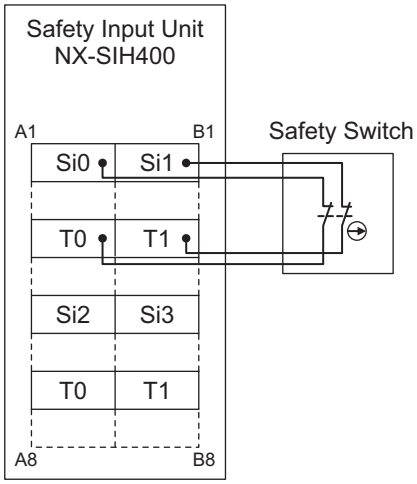
Item	Specification
Number of safety input points	This is the number of safety input points on the Unit.
Number of test output points	This is the number of test output points on the Unit. The test output points are used with the safety input terminals.
Internal I/O common	This is the polarity that the Unit uses to connect to input devices.
Rated input voltage	This is the rated input voltage of the Unit.
OMRON Special Safety Input Devices	This tells whether the Unit supports the connection of OMRON Special Safety Input Devices (D40A-2 Non-contact Door Switches, E3FS Single Beam Safety Sensors, etc.).
Number of safety slave connections	This is the number of slave connections that the Unit can have through FSoE. You can perform communications with one FSoE master device per connection.
I/O refreshing method	This is the I/O refreshing method for the Unit.
External connection terminals	This is the type of terminal block and connector that is used to wire the Unit. This specification includes the number of terminals for a screwless clamping terminal block.

Item	Specification
Indicators	This gives the names and the layout of the indicators on the Unit.
Safety input current	This is the input current at the rated voltage of the safety inputs on the Unit.
Safety input ON voltage	This is the input voltage at which the safety inputs on the Unit turn ON.
Safety input OFF voltage/OFF current	These are the input voltage and input current at which the safety inputs on the Unit turn OFF.
Test output type	This is the polarity that the Unit uses to connect to devices.
Test output rated current	This is the maximum load current for each test output on the Unit.
Test output ON residual voltage	This is the residual voltage when the test output on the Unit is ON.
Test output leakage current	This is the leakage current when the test output on the Unit is OFF.
Dimensions (mm)	These are the external dimensions of the Unit. The dimensions are given in the form W × H × D. The dimensions are given in "millimeters".
Isolation method	This is the method that is used to isolate the input circuits from the internal circuits of the Unit.
Insulation resistance	This is the insulation resistance between the input circuits and the internal circuits of the Unit.
Dielectric strength	This is the dielectric strength between the input circuits and the internal circuits of the Unit.
I/O power supply method	This is the method that is used to supply I/O power to the Unit.
Current capacity of I/O power supply terminal	This is the current capacity of the I/O power supply terminals (IOV/IOG) on the Unit. When you supply I/O power to external devices that are connected to the Unit, make sure that the total power does not exceed this value.
NX Unit power consumption	This is the power consumption of the Unit from the NX bus power supply.
Current consumption from I/O power supply	This is the current consumption of the Unit from the I/O power supply. This value does not include the load current of any external connection loads or the current consumption of any connected external devices.
Weight	This is the weight of the Unit.
Circuit layout	This is the internal circuits of the Unit.
Terminal connection diagram	This is the connection diagram between the Unit and connected external devices.
Installation orientation and restrictions	This is the installation orientation of the Unit. If the installation orientation imposes any restrictions on the specifications, those restrictions are also described.
Protective functions	These are the protective functions that are supported by the Unit.

● NX-SIH400

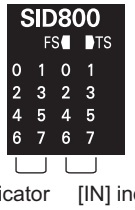
Item	Specification
Number of safety input points	4 points
Number of test output points	2 points
Internal I/O common	PNP (sinking inputs)
Rated input voltage	24 VDC (20.4 to 28.8 VDC)
OMRON Special Safety Input Devices	Can be connected.
Number of safety slave connections	1
I/O refreshing method	Free-Run refreshing
External connection terminals	Screwless clamping terminal block (8 terminals)

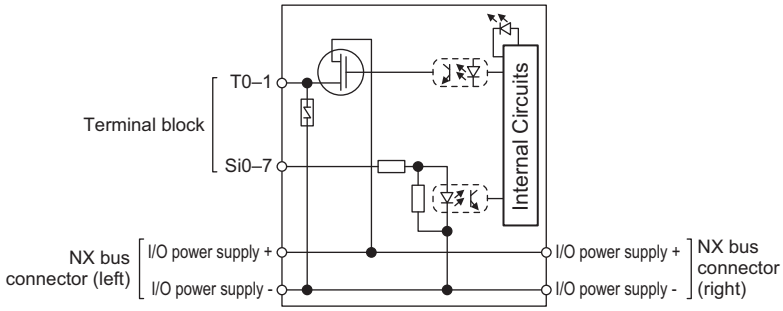
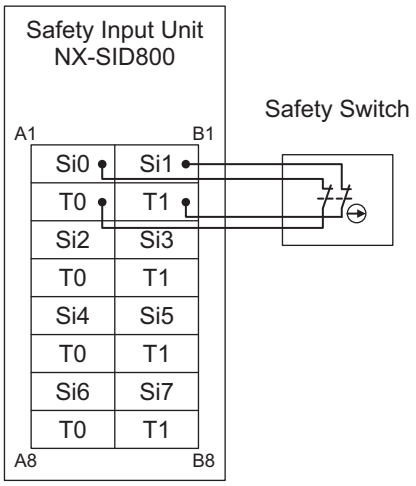
Item	Specification
Indicators	[TS] indicator, [FS] indicator, [IN] indicator, [IN ERR] indicator 
Safety input current	4.5 mA typical
Safety input ON voltage	11 VDC min.
Safety input OFF voltage/OFF current	5 VDC max./1 mA max.
Test output type	Sourcing outputs (PNP)
Test output rated current	25 mA max.
Test output ON residual voltage	1.2 V max. (IOV and all output terminals)
Test output leakage current	0.1 mA max.
Dimensions (mm)	12 × 100 × 71 (W × H × D)
Isolation method	Photocoupler isolation
Insulation resistance	20 MΩ min. between isolated circuits (at 100 VDC)
Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
I/O power supply method	Power supplied from the NX bus
Current capacity of I/O power supply terminals	No applicable terminals.
NX Unit power consumption	• Connected to a CPU Unit or a Communication Control Unit 1.10 W max. • Connected to a Communications Coupler Unit 0.70 W max.
Current consumption from I/O power supply	20 mA max.
Weight	70 g max.
Circuit layout	

Item	Specification
Terminal connection diagram	Si0 to Si3: Safety input terminals T0, T1: Test output terminals  Refer to *6-3-1 Safety Input Function* on page 6-16 for details.
Installation orientation and restrictions	Installation orientation: • Connected to a CPU Unit or a Communication Control Unit *1 Possible in the upright installation orientation. • Connected to a Communications Coupler Unit Six possible orientations. Restriction: Maximum ambient temperature is 50°C for any orientation other than upright installation.
Protective functions	Overvoltage protection circuit and short detection (test outputs)

*1. Only NX502 CPU Units, NX102 CPU Units, and Communication Control Units can be connected. NX1P2 CPU Units cannot be connected.

● NX-SID800

Item	Specification
Number of safety input points	8 points
Number of test output points	2 points
Internal I/O common	PNP (sinking inputs)
Rated input voltage	24 VDC (20.4 to 28.8 VDC)
OMRON Special Safety Input Devices	Cannot be connected.
Number of safety slave connections	1
I/O refreshing method	Free-Run refreshing
External connection terminals	Screwless clamping terminal block (16 terminals)
Indicators	[TS] indicator, [FS] indicator, [IN] indicator, [IN ERR] indicator  [IN ERR] indicator [IN] indicator
Safety input current	3.0 mA typical
Safety input ON voltage	15 VDC min.

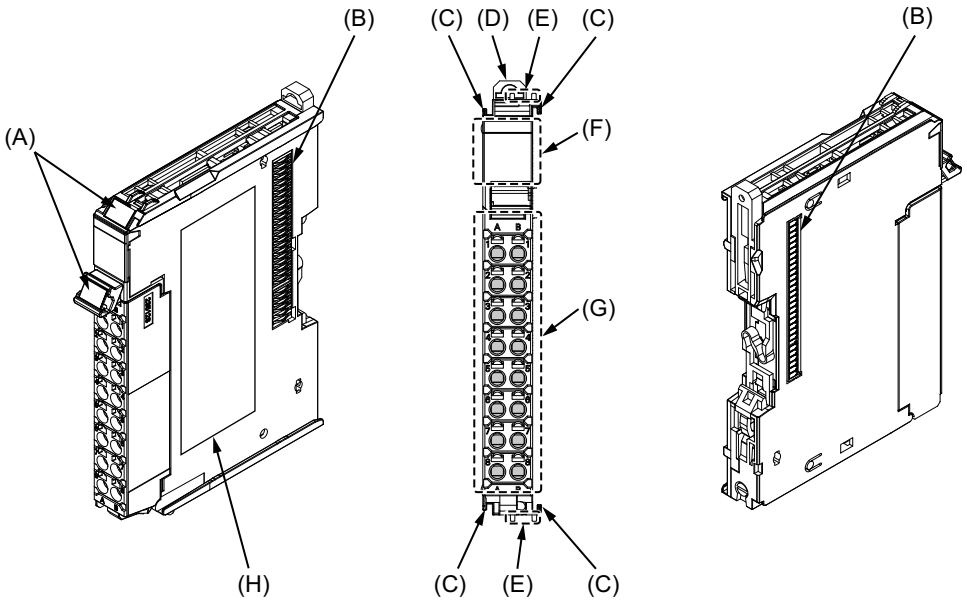
Item	Specification
Safety input OFF voltage/OFF current	5 VDC max./1 mA max.
Test output type	Sourcing outputs (PNP)
Test output rated current	50 mA max.
Test output ON residual voltage	1.2 V max. (IOV and all output terminals)
Test output leakage current	0.1 mA max.
Dimensions (mm)	12 × 100 × 71 (W × H × D)
Isolation method	Photocoupler isolation
Insulation resistance	20 MΩ min. between isolated circuits (at 100 VDC)
Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
I/O power supply method	Power supplied from the NX bus
Current capacity of I/O power supply terminals	No applicable terminals.
NX Unit power consumption	• Connected to a CPU Unit or a Communication Control Unit 1.10 W max. • Connected to a Communications Coupler Unit 0.75 W max.
Current consumption from I/O power supply	20 mA max.
Weight	70 g max.
Circuit layout	
Terminal connection diagram	Si0 to Si7: Safety input terminals T0, T1: Test output terminals  Refer to *6-3-1 Safety Input Function* on page 6-16 for details.

Item	Specification
Installation orientation and restrictions	Installation orientation: • Connected to a CPU Unit or a Communication Control Unit *1 Possible in the upright installation orientation. • Connected to a Communications Coupler Unit Six possible orientations. Restriction: Maximum ambient temperature is 50°C for any orientation other than upright installation.
Protective functions	Overvoltage protection circuit and short detection (test outputs)

*1. Only NX502 CPU Units, NX102 CPU Units, and Communication Control Units can be connected. NX1P2 CPU Units cannot be connected.

3-3-2 Part Names and Functions

This section provides the names and functions of the parts of the Safety Input Unit.

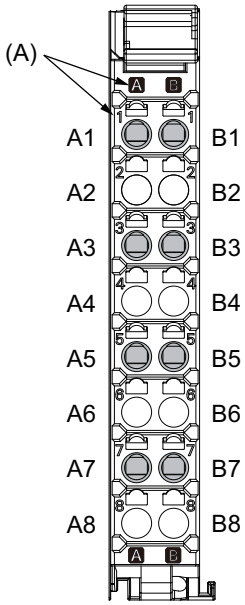


Letter	Name	Function
(A)	Marker attachment location	The locations where markers are attached. The markers made by OMRON are installed for the factory setting. Commercially available markers can also be installed. Refer to *5-2-7 Attaching Markers* on page 5-20.
(B)	NX bus connector	This is the NX-series bus connector.
(C)	Unit hookup guides	These guides are used to connect two Units.
(D)	DIN Track mounting hooks	These hooks are used to mount the NX Unit to a DIN Track.
(E)	Protrusions for removing the Unit	The protrusions to hold when removing the Unit.
(F)	Indicators	The indicators show the current operating status of the Safety Input Unit or signal input status. Refer to *3-3-3 Indicators* on page 3-40.
(G)	Terminal block	The terminal block is used to connect external devices.
(H)	Unit specifications	The specifications of the Safety Input Unit are given here.

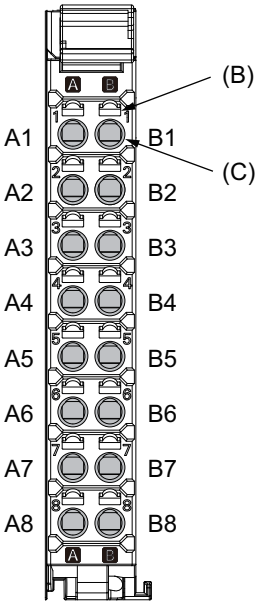
Terminal Blocks

There are two models of screwless clamping terminal blocks: NX-TB□□□2 and NX-TB□□□1. The following models of Terminal Blocks can be mounted to Safety Input Units.

NX-TB□□□2

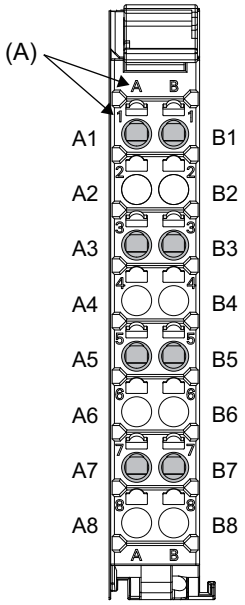


8-terminal type

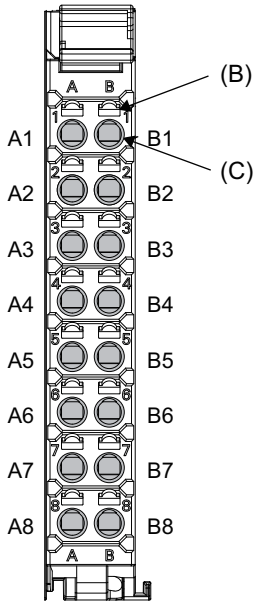


16-terminal type

NX-TB□□□1



8-terminal type



16-terminal type

Letter	Name	Function
(A)	Terminal number indications	The terminal numbers are given by column letters A and B, and row numbers 1 to 8. The combination of the "column" and "row" gives the terminal numbers from A1 to A8 and B1 to B8. The terminal number indicators are the same regardless of the number of terminals on the terminal block, as shown above.
(B)	Release holes	Insert a flat-blade screwdriver into these holes to connect or remove the wires.
(C)	Terminal holes	The wires are inserted into these holes.

Terminal Blocks for Safety Input Units come in two types depending on the number of terminals that can be used. There are 8-terminal and 16-terminal Terminal Blocks.
The terminal block must have the same number of terminals that the Unit is designed for.



Additional Information

The 8-terminal type does not have terminal holes and release holes for the following terminals.
- A2, A4, A6, A8, B2, B4, B6, and B8.

There are two types of Terminal Blocks in terms of current capacity, 10 A for the NX-TB□□□2 Terminal Blocks and 4 A for the NX-TB□□□1 Terminal Blocks.
To differentiate between the two types of Terminal Blocks, use the terminal number column indications.
The Terminal Block with white letters on a dark background is the NX-TB□□□2 Terminal Block.
You can mount either type of Terminal Block to a Unit with a terminal current capacity of 4 A max.
You can only mount the NX-TB□□□2 Terminal Block to the Units that the current capacity specification of the terminals is greater than 4 A.

- Applicable Terminal Blocks for Each Unit Model

The following table gives the Terminal Blocks that are applicable to each Unit.

Unit model number	Terminal block			
	Model number	Number of terminals	Ground terminal mark	Current capacity
NX-SIH400	NX-TBA081	8	Not provided	4 A
	NX-TBA082			10 A
NX-SID800	NX-TBA161	16	Not provided	4 A
	NX-TBA162			10 A



Precautions for Correct Use

You can mount either NX-TB□□□1 or NX-TB□□□2 Terminal Block to a Unit with a terminal current capacity of 4 A.
Even if you mount an NX-TB□□□2 Terminal Block, the current specification does not change because the terminal current capacity of the Unit is 4 A.
Refer to the I/O power supply terminal current capacities given in *Individual Specifications* on page 3-33 for the terminal current capacity specifications of the Units.
Refer to *A-11 List of Screwless Clamping Terminal Block Models* on page A-93 or the model numbers of the Terminal Blocks.

3-3-3 Indicators

This section describes the indicators of the Safety Input Unit.

⚠ WARNING

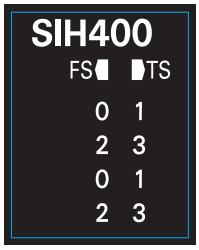
Do not use the status of the indicators on the NX-series Safety Control Units for safety operations.
This will compromise the safety functions of the Unit and may cause serious injury in the event of an accident.



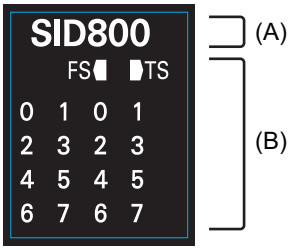
The appearance of the indicators is different depending on whether the lot number of the Unit represents the date of or before September 19, 2018, or the date of or after September 20, 2018. In this manual, indicators for lot numbers of or after September 20, 2018 are shown.

For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-44.
Refer to *Notation of Unit Versions on Products* on page 44 for how to identify the lot number of the Unit.

The indicator pattern depends on the number of input points, as shown below.



Unit with 4 I/O Points



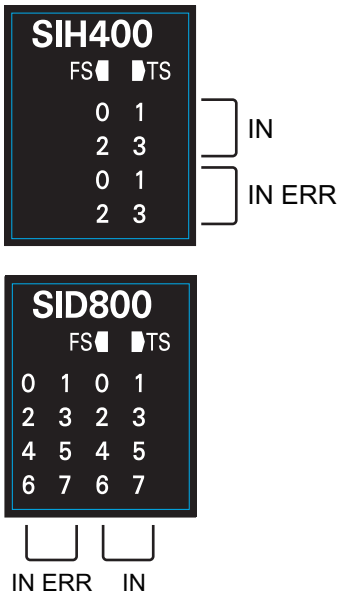
Unit with 8 I/O Points

Letter	Name	Function
(A)	Model number display	Displays part of the model number of the Safety I/O Units. The model number indication is red on all Safety Control Units.
(B)	Indicators	Show the current operating status and communications status of the Safety I/O Units.

Safety Input Unit Operation Status Indicators

Indicators to show the operation status of the Safety Input Unit are located in the center of the front side of the Safety Input Unit.

The following section describes the specifications of each indicator.



● TS Indicator

The TS indicator shows the current status of the Safety Input Unit and its communications status with the Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The Unit is operating normally.
		Flashing (at 2-s intervals)	Initializing, or I/O allocation information data is being downloaded from the Sysmac Studio.
Red		Lit	A hardware error, WDT error, or other critical error has occurred.
		Flashing (at 1-s intervals)	An NX bus communications error, I/O allocation information data error, or other recoverable minor error that is attributed to the NX bus has occurred.
---		Not lit	• There is no Unit power supply • Restarting the Unit • Waiting for initialization to start

● FS Indicator

The FS indicator shows the FSoE communications status and safety function status of the Safety Input Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The FSoE connections are established and there are no errors in any Safety I/O Units functions.
		Flashing (at 1-s intervals)	The FSoE connections are being established.
Red		Flashing (at 1-s intervals)	An FSoE communications error, safety input terminal error, or other minor error has occurred.

Color	Status		Meaning
---		Not lit	Power is not being supplied or a fatal fault has occurred.

● IN Indicator

The IN indicator shows the signal input status of the safety input terminal.

The following table lists the possible states for this indicator and what they mean.
The table shows an example of safety input terminal Si01. The safety input terminal number is lit or not lit.

Color	Status		Meaning
Yellow		Lit	The safety input terminal is ON and there are no errors.
---		Not lit	The safety input terminal is OFF or an error has occurred.



Additional Information

If the lot number of the Unit represents the date of or before September 19, 2018, the indicators have square-shaped light emitters. For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-44.

Color	Status		Meaning
Yellow		Lit	The safety input terminal is ON and there are no errors.
---		Not lit	The safety input terminal is OFF or an error has occurred.

● IN ERR Indicator

The IN ERR indicator shows the error status of the safety input terminal.

The following table lists the possible states for this indicator and what they mean.
The table shows an example of safety input terminal Si01. The safety input terminal number is lit, flashing or not lit.

Color	Status		Meaning
Red		Lit	An error has occurred in the safety input terminal.
		Flashing (at 1-s intervals)	An error has occurred in the safety input terminal for the other channel of the dual channel I/O.
---		Not lit	There are no errors in the safety input terminal.

Additional Information

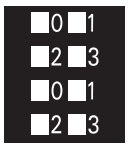
If the lot number of the Unit represents the date of or before September 19, 2018, the indicators have square-shaped light emitters. For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-44.

Color	Status		Meaning
Red		Lit	An error has occurred in the safety input terminal.
		Flashing (at 1-s intervals)	An error has occurred in the safety input terminal for the other channel of the dual channel I/O.
---		Not lit	An error has occurred in the safety input terminal.

Refer to *15-2-5 Troubleshooting Errors in the Safety Control Unit* on page 15-35 for details on the relationship between the errors of the Safety Input Unit and the indicators.

Differences in Appearance of the Indicators

The appearance of the indicators is different depending on whether the lot number of the Unit represents the date of or before September 19, 2018, or the date of or after September 20, 2018.
The following table shows how the appearance of the indicators is different depending on the lot number.

Indicator	Description	Lot number	
		Date of or before Sep.19, 2018	Date of or after Sep. 20, 2018
TS indicator FS indicator	The shape of the light emitting parts is changed from a square to a pentagon.		
IN indicator IN ERR indicator	Square-shaped light emitters of the indicators are changed to light-emitting terminal numbers.		

3-4 Safety Output Unit

This section describes the models and specifications of the Safety Output Units as well as the names and functions of the parts.

3-4-1 Models and Specifications

The Safety Output Unit specifications are described below.

Models

The following table specifies the list of the Safety Output Unit models.

Model	Number of safety output points	Internal I/O common	Maximum load current	Rated voltage	Number of safety slave connections	I/O refreshing method
NX-SOH200	2 points	Sourcing outputs (PNP)	2.0 A/point, 4.0 A/Unit at 40°C 2.5 A/Unit at 55°C	24 VDC	1	Free-Run refreshing
NX-SOD400	4 points	Sourcing outputs (PNP)	0.5 A/point and 2.0 A/Unit	24 VDC	1	Free-Run refreshing

General Specifications

This section provides the general specifications of the Safety Output Unit.

Item	Specification
Enclosure	Mounted in a panel (open)
Grounding method	Ground to 100 Ω or less

Item		Specification
Operating environment	**Ambient operating temperature**	0 to 55°C
	Ambient operating humidity	10% to 95% (with no condensation or icing)
	Atmosphere	Must be free from corrosive gases.
	Ambient storage temperature	−25 to 70°C (with no condensation or icing)
	Altitude	2,000 m max.
	Pollution degree	2 or less: Meets IEC 61010-2-201
	Noise immunity	Conforms to IEC 61131-2, 2 kV (power supply line)
	Insulation class	CLASS III (SELV)
	Overvoltage category	Category II: Meets IEC 61010-2-201
	EMC immunity level	Zone B
	Vibration resistance	Conforms to IEC 60068-2-6 5 to 8.4 Hz with amplitude of 3.5 mm 8.4 to 150 Hz, acceleration of 9.8 m/s^2 100 min. in each X, Y, and Z directions (10 sweeps of 10 min. each = 100 min. total)
	Shock resistance	Conforms to IEC 60068-2-27 147 m/s^2, 3 times in each X, Y, and Z directions
	Isolation method	Photocoupler isolation
	Insulation resistance	20 MΩ between isolated circuits (at 100 VDC)
	Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
Installation method		DIN Track (IEC 60715 TH35-7.5/TH35-15)

Individual Specifications

This section provides the individual specifications of the Safety Output Unit.

● Datasheet Items for Safety Output Unit

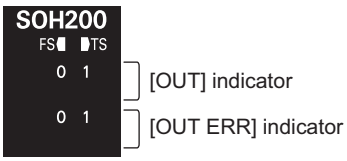
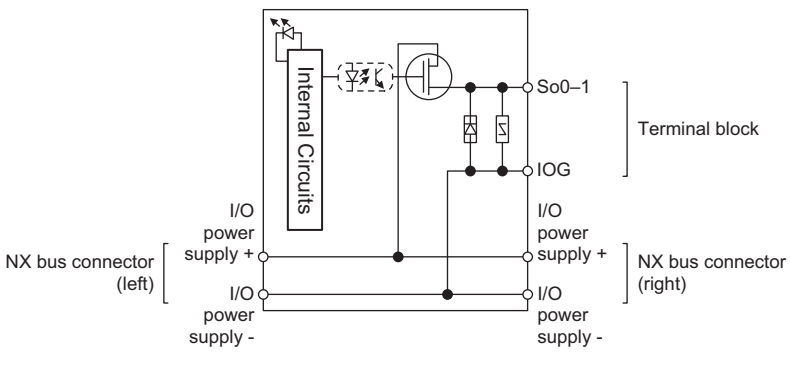
The following table gives the meaning of the datasheet items for the Safety Output Units.

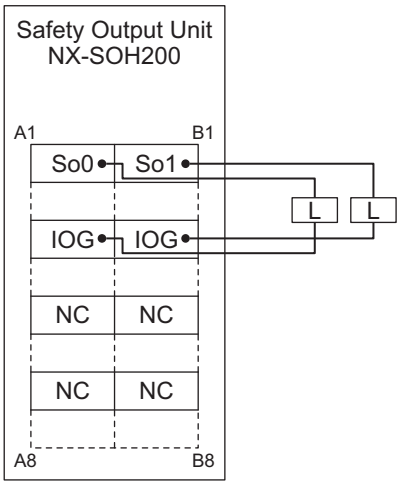
Item	Specification
Number of safety output points	This is the number of safety output points on the Unit.
Internal I/O common	This is the polarity that the Unit uses to connect to output devices.
Maximum load current	This is the maximum load current for outputs on the Unit. A specification is given for each output and each Unit.
Rated voltage	This is the rated voltage of the outputs on the Unit.
Number of safety slave connections	This is the number of slave connections that the Unit can have through FSoE. You can perform communications with one FSoE master device per connection.
I/O refreshing method	The I/O refreshing methods that are used by the Unit.
External connection terminals	The type of terminal block and connector that is used for connecting the Unit. This specification includes the number of terminals for a screwless clamping terminal block.
Indicators	This gives the names and the layout of the indicators on the Unit.

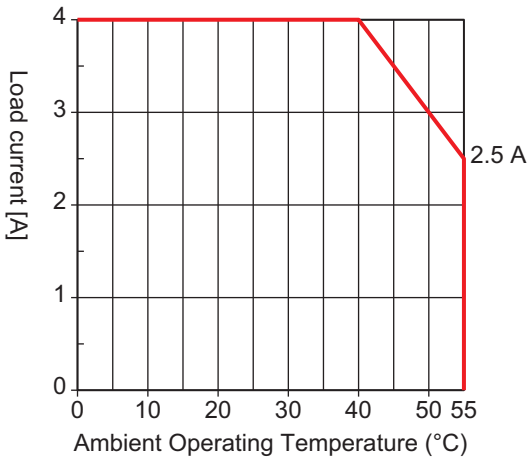
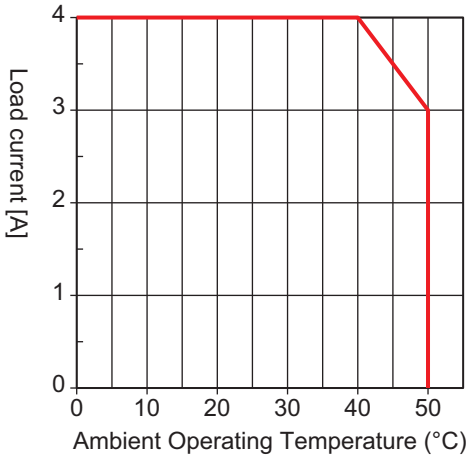
Item	Specification
Safety output rated current	This is the maximum load current for safety outputs on the Unit. The inrush current of the external connection load must be lower than this value.
Safety output ON residual voltage	This is the residual voltage when a safety output on the Unit is ON.
Safety output OFF residual voltage	This is the residual voltage when a safety output on the Unit is OFF.
Safety output leakage current	This is the leakage current when a safety output on the Unit is OFF.
Dimensions (mm)	These are the external dimensions of the Unit. The dimensions are given in the form W × H × D. The dimensions are given in millimeters.
Isolation method	This is the method that is used to isolate the output circuits from the internal circuits of the Unit.
Insulation resistance	This is the insulation resistance between the output circuits and the internal circuits of the Unit.
Dielectric strength	This is the dielectric strength between the output circuits and the internal circuits of the Unit.
I/O power supply method	The method for supplying I/O power for the Unit.
Current capacity of I/O power supply terminal	This is the current capacity of the I/O power supply terminals (IOV/IOG) on the Unit. When you supply I/O power to external devices that are connected to the Unit, make sure that the total power does not exceed this value.
NX Unit power consumption	This is the power consumption of the Unit from the NX bus power supply.
Current consumption from I/O power supply	This is the current consumption of the Unit from the I/O power supply. This value does not include the load current of any external connection loads or the current consumption of any connected external devices.
Weight	This is the weight of the Unit.
Circuit layout	This is the internal circuits of the Unit.
Terminal connection diagram	This is the connection diagram between the Unit and external devices.
Installation orientation and restrictions	This is the installation orientation of the Unit. If the installation orientation imposes any restrictions on the specifications, those restrictions are also described.
Protective functions	These are the protective functions that are supported by the Unit.

● NX-SOH200

Item	Specification
Number of safety output points	2 points
Internal I/O common	PNP (sourcing outputs)
Maximum load current	2.0 A/point 4.0 A/Unit at 40°C 2.5 A/Unit at 55°C The maximum load current depends on the installation orientation and ambient temperature.
Rated input voltage	24 VDC (20.4 to 28.8 VDC)
Number of safety slave connections	1
I/O refreshing method	Free-Run refreshing

Item	Specification
External connection terminals	Screwless clamping terminal block (8 terminals)
Indicators	[TS] indicator, [FS] indicator, [OUT] indicator, [OUT ERR] indicator 
Safety output ON residual voltage	1.2 V max. (between IOV and all output terminals)
Safety output OFF residual voltage	2 V max. (between IOG and all output terminals)
Safety output leakage current	0.1 mA max.
Dimensions (mm)	12 × 100 × 71 (W × H × D)
Isolation method	Photocoupler isolation
Insulation resistance	20 MΩ min. between isolated circuits (at 100 VDC)
Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
I/O power supply method	Power supplied from the NX bus
Current capacity of I/O power supply terminals	IOG: 2 A/terminal max.
NX Unit power consumption	• Connected to a CPU Unit or a Communication Control Unit 1.05 W max. • Connected to a Communications Coupler Unit 0.70 W max.
Current consumption from I/O power supply	40 mA max.
Weight	65 g max.
Circuit layout	

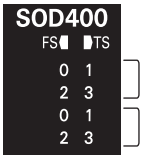
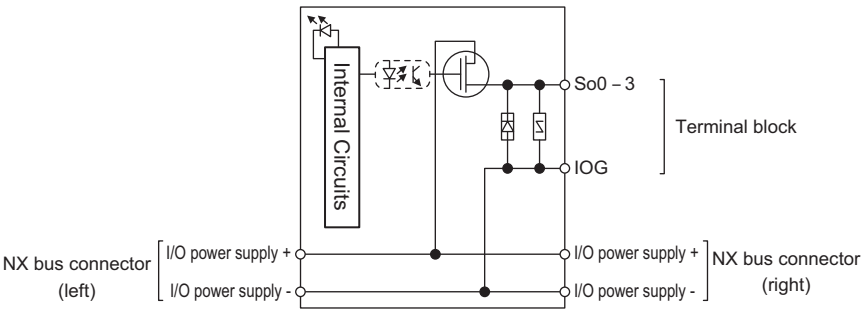
Item	Specification
Terminal connection diagram	So0 to So1: Safety output terminals IOG: I/O power supply 0 V  Refer to *6-3-2 Safety Output Function* on page 6-38 for details.

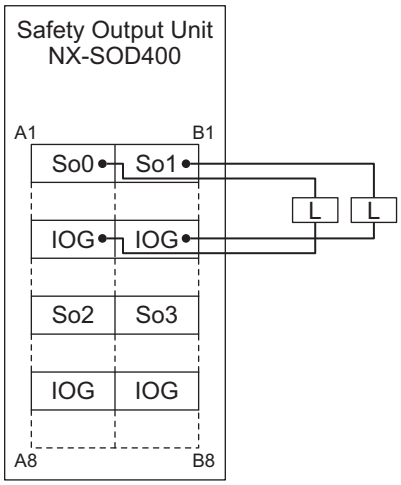
Item	Specification
Installation orientation and restrictions	Installation orientation: • Connected to a CPU Unit or a Communication Control Unit*1 Possible in the upright installation orientation. • Connected to a Communications Coupler Unit Six possible orientations. Restriction: For upright installation, the ambient temperature is restricted as shown below according to the total Unit load current.  For all installation orientations other than upright installation, the ambient temperature is restricted as shown below according to the total Unit load current. 
Protective functions	Overvoltage protection circuit and short detection

*1. Only NX502 CPU Units, NX102 CPU Units, and Communication Control Units can be connected. NX1P2 CPU Units cannot be connected.

● NX-SOD400

Item	Specification
Number of safety output points	4 points
Internal I/O common	PNP (sourcing outputs)
Maximum load current	0.5 A/point and 2.0 A/Unit
Rated input voltage	24 VDC (20.4 to 28.8 VDC)
Number of safety slave connections	1

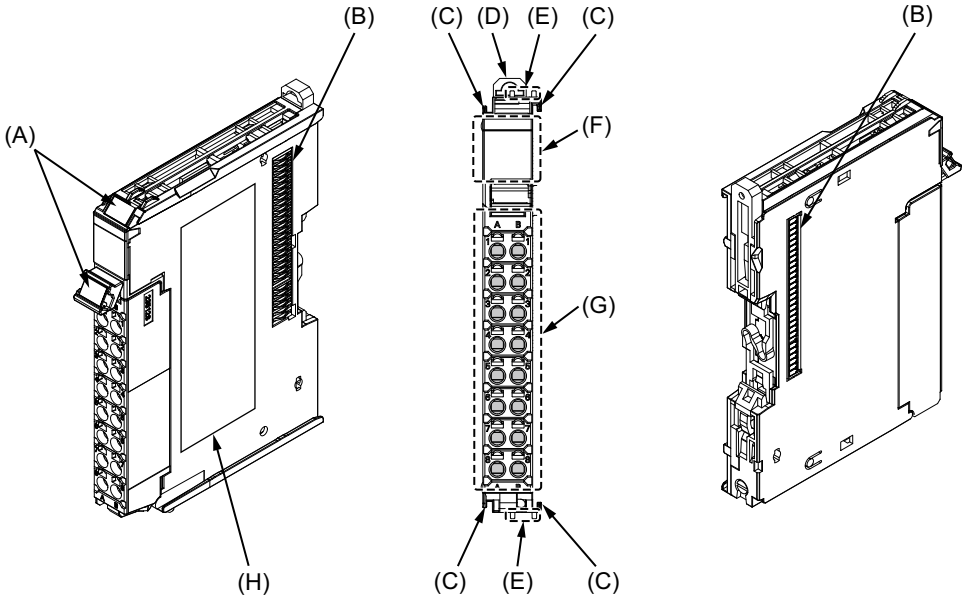
Item	Specification
I/O refreshing method	Free-Run refreshing
External connection terminals	Screwless clamping terminal block (8 terminals)
Indicators	[TS] indicator, [FS] indicator, [OUT] indicator, [OUT ERR] indicator 
Safety output ON residual voltage	1.2 V max. (between IOV and all output terminals)
Safety output OFF residual voltage	2 V max. (between IOG and all output terminals)
Safety output leakage current	0.1 mA max.
Dimensions (mm)	12 × 100 × 71 (W × H × D)
Isolation method	Photocoupler isolation
Insulation resistance	20 MΩ min. between isolated circuits (at 100 VDC)
Dielectric strength	510 VAC between isolated circuits for 1 minute at a leakage current of 5 mA max.
I/O power supply method	Power supplied from the NX bus
Current capacity of I/O power supply terminals	IOG (A3 and B3): 2 A/terminal max. IOG (A7 and B7): 0.5 A/terminal max.
NX Unit power consumption	• Connected to a CPU Unit or a Communication Control Unit 1.10 W max. • Connected to a Communications Coupler Unit 0.75 W max.
Current consumption from I/O power supply	60 mA max.
Weight	65 g max.
Circuit layout	

Item	Specification
Terminal connection diagram	So0 to So3: Safety output terminals IOG: I/O power supply 0 V  Refer to *6-3-2 Safety Output Function* on page 6-38 for details.
Installation orientation and restrictions	Installation orientation: • Connected to a CPU Unit or a Communication Control Unit*1 Possible in the upright installation orientation. • Connected to a Communications Coupler Unit Six possible orientations. Restriction: None.
Protective functions	Overvoltage protection circuit and short detection

*1. Only NX502 CPU Units, NX102 CPU Units, and Communication Control Units can be connected. NX1P2 CPU Units cannot be connected.

3-4-2 Part Names and Functions

This section provides the names and functions of the parts of the Safety Output Unit.

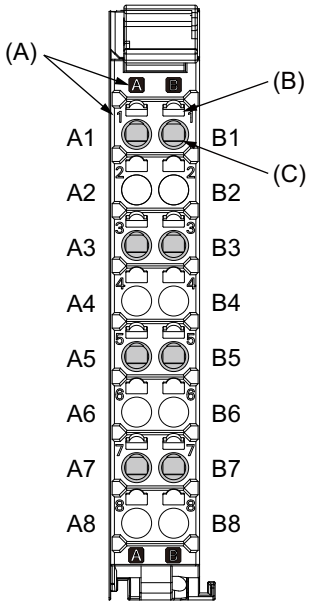


Letter	Name	Function
(A)	Marker attachment location	The locations where markers are attached. The markers made by OMRON are installed for the factory setting. Commercially available markers can also be installed. Refer to *5-2-7 Attaching Markers* on page 5-20.
(B)	NX bus connector	This is the NX-series bus connector.
(C)	Unit hookup guides	These guides are used to connect two Units.
(D)	DIN Track mounting hook	This hook is used to mount the NX Unit to a DIN Track.
(E)	Protrusions for removing the Unit	The protrusions to hold when removing the Unit.
(F)	Indicators	The indicators show the current operating status of the Safety Output Unit or signal I/O status. Refer to *3-4-3 Indicators* on page 3-55.
(G)	Terminal block	The terminal block is used to connect external devices.
(H)	Unit specifications	The specifications of the Safety Output Unit are given.

Terminal Blocks

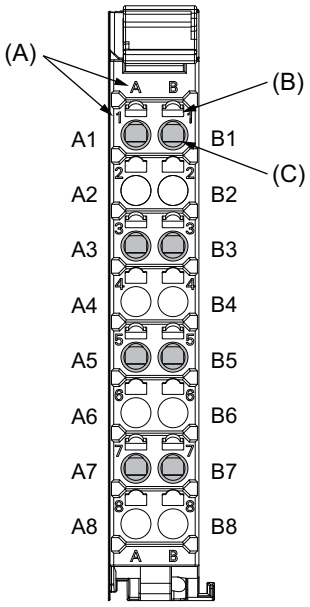
There are two models of screwless clamping terminal blocks: NX-TB□□□2 and NX-TB□□□1. The following models of Terminal Blocks can be mounted to Safety Output Units.

NX-TB□□□2



8-terminal type

NX-TB□□□1



8-terminal type

Letter	Name	Function
(A)	Terminal number indications	The terminal numbers are given by column letters A and B, and row numbers 1 to 8. The combination of the "column" and "row" gives the terminal numbers from A1 to A8 and B1 to B8. The terminal number indicators are the same regardless of the number of terminals on the terminal block, as shown above.
(B)	Release hole	Insert a flat-blade screwdriver into these holes to connect or remove the wires.
(C)	Terminal hole	The wires are inserted into these holes.

Only 8-terminal type blocks can be inserted to the terminal blocks of Safety Output Units.
To prevent incorrect insertion, terminal blocks in any other types besides the 8-terminal type cannot be mounted.

Additional Information

The 8-terminal type does not have terminal holes and release holes for following terminal numbers.
- A2, A4, A6, A8, B2, B4, B6, and B8.

There are two types of Terminal Blocks in terms of current capacity, 10 A for the NX-TB□□□2 Terminal Blocks and 4 A for the NX-TB□□□1 Terminal Blocks.
To differentiate between the two types of Terminal Blocks, use the terminal number column indications.
The Terminal Block with white letters on a dark background is the NX-TB□□□2 Terminal Block.
You can mount either type of Terminal Block to a Unit with a terminal current capacity of 4 A.
You can only mount the NX-TB□□□2 Terminal Block to the Units that the current capacity specification of the terminals is greater than 4 A.

- Applicable Terminal Blocks for Each Unit Model
  The following table gives the Terminal Blocks that are applicable to each Unit.

Unit model number	Terminal block			
	Model	Number of terminals	Ground terminal mark	Current capacity
NX-SOH200	NX-TBA081	8	Not provided	4 A
	NX-TBA082			10 A
NX-SOD400	NX-TBA081	8	Not provided	4 A
	NX-TBA082			10 A

Precautions for Correct Use

You can mount either NX-TB□□□1 or NX-TB□□□2 Terminal Blocks to the Units that the current capacity specification of the terminals is 4 A or less.
Even if you mount an NX-TB□□□2 Terminal Block, the current specification does not change because the terminal current capacity of the Unit is 4 A.
Refer to the I/O power supply terminal current capacities given in *Individual Specifications* on page 3-46 for the terminal current capacity specifications of the Units.
Refer to *A-11 List of Screwless Clamping Terminal Block Models* on page A-93 for information on the models of terminal blocks.

3-4-3 Indicators

This section describes the indicators of the Safety Output Unit.

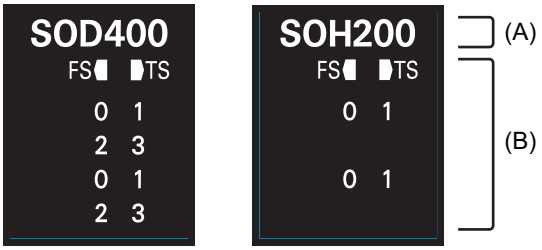
⚠ WARNING

Do not use the status of the indicators on the NX-series Safety Control Units for safety operations.
This will compromise the safety functions of the Unit and may cause serious injury in the event of an accident.

The appearance of the indicators is different depending on whether the lot number of the Unit represents the date of or before September 19, 2018, or the date of or after September 20, 2018. In this manual, indicators for lot numbers of or after September 20, 2018 are shown.

For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-58.
Refer to *Notation of Unit Versions on Products* on page 44 for how to identify the lot number of the Unit.

The indicator pattern depends on the number of output points, as shown below.



Unit with 4 I/O Points | Unit with 2 I/O Points

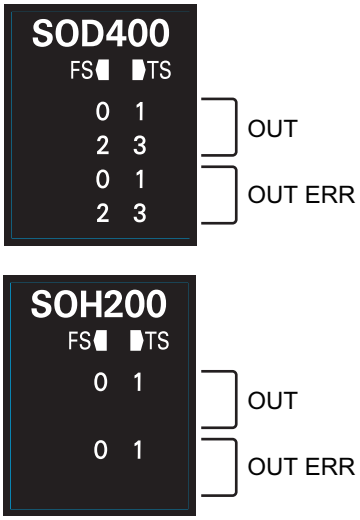
Letter	Name	Function
(A)	Model number display	Displays part of the model number of the Safety I/O Units. The model number indication is red on Safety Control Units.

Letter	Name	Function
(B)	Indicators	Show the current operating status and communications status of the Safety I/O Units.

Safety Output Unit Operation Status Indicators

There are the indicators to show the operation status of Safety Output Unit in the center of the front side of the Safety Output Unit.

The following section describes the specifications of each indicator.



● TS Indicator

The TS indicator shows the current status of the Safety Output Unit and its communications status with the Communication Control Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The Unit is operating normally.
		Flashing (at 2-s intervals)	Initialization is in progress, or I/O allocation information data is being downloaded from the Sysmac Studio.
Red		Lit	A hardware error, WDT error, or other critical error has occurred.
		Flashing (at 1-s intervals)	An NX bus communications error, I/O allocation information data error, or other recoverable minor error that is attributed to the NX bus has occurred.
---		Not lit	• There is no Unit power supply • The Unit is restarting • Waiting for initialization to start

● FS Indicator

The FS indicator shows the FSoE communications status and safety function status of the Safety Output Unit.

The following table lists the possible states for this indicator and what they mean.

Color	Status		Meaning
Green		Lit	The FSoE connections are established and there are no errors in any Safety I/O Units functions.
		Flashing (at 1-s intervals)	The FSoE connections are being established.
Red		Flashing (at 1-s intervals)	An FSoE communications error, safety output terminal error, or other minor error has occurred.
---		Not lit	Power is not being supplied or a fatal fault has occurred.

● OUT Indicator

The OUT indicator shows the signal input status of the safety output terminal.

The following table lists the possible states for this indicator and what they mean.
The table shows an example of safety output terminal So01. The safety output terminal number is lit or not lit.

Color	Status		Meaning
Yellow		Lit	Safety output terminal is ON and there are no errors.
---		Not lit	Safety output terminal is OFF or an error has occurred.



Additional Information

If the lot number of the Unit represents the date of or before September 19, 2018, the indicators have square-shaped light emitters. For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-44.

Color	Status		Meaning
Yellow		Lit	Safety output terminal is ON and there are no errors.
---		Not lit	Safety output terminal is OFF or an error has occurred.

● OUT ERR Indicator

The OUT ERR indicator shows the error status of the safety output terminals.

The following table lists the possible states for this indicator and what they mean.
The table shows an example of safety output terminal So01. The safety output terminal number is lit, flashing or not lit.

Color	Status		Meaning
Red		Lit	An error has occurred in the safety output terminal.
		Flashing (at 1-s intervals)	An error has occurred in the safety output terminal for the other channel of the dual channel I/O.
---		Not lit	There are no errors in the safety output terminal.

Additional Information

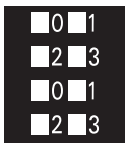
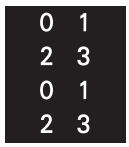
If the lot number of the Unit represents the date of or before September 19, 2018, the indicators have square-shaped light emitters. For details on the differences in appearance of the indicators, refer to *Differences in Appearance of the Indicators* on page 3-44.

Color	Status		Meaning
Red		Lit	An error has occurred in the safety output terminal.
		Flashing (at 1-s intervals)	An error has occurred in the safety output terminal for the other channel of the dual channel I/O.
---		Not lit	There are no errors in the safety output terminal.

Refer to *15-2-5 Troubleshooting Errors in the Safety Control Unit* on page 15-35 for details on the relationship between errors of the Safety Output Unit and the indicators.

Differences in Appearance of the Indicators

The appearance of the indicators is different depending on whether the lot number of the Unit represents the date of or before September 19, 2018, or the date of or after September 20, 2018.
The following table shows how the appearance of the indicators is different depending on the lot number.

Indicator	Description	Lot number	
		Date of or before Sep.19, 2018	Date of or after Sep. 20, 2018
TS indicator FS indicator	The shape of the light emitting parts is changed from a square to a pentagon.		
OUT indicator OUT ERR indicator	Square-shaped light emitters of the indicators are changed to light-emitting terminal numbers.		

3-5 End Cover

This section describes the model and specifications of the end cover.

3-5-1 Models and Specifications

The specifications of the End Cover are described below.

Item	Specification
Model	NX-END02
Dimensions (mm)	6 × 100 × 71 (W × H × D)
Weight	82 g

3-6 SD Memory Cards

This section describes the models, specifications, and application of the SD Memory Cards.

3-6-1 Models and Specifications

Refer to *Specification of Supported SD Memory Cards, Folders, and Files* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for details.

3-6-2 Purpose

You can use the SD Memory Card for the following applications.

Function	Description
FTP Server	Read and write files in the SD Memory Card from an FTP client on EtherNet/IP.
SD Memory Card Backups	Back up, restore, and verify data in the Communication Control Unit.
Safety Unit Restore	Restore the data of Safety CPU Unit.
Safety Data Logging	Save the setting file and log file of Safety Data Logging.

3-7 Support Software

The Support Software is a software package that provides an integrated development environment to design, program, debug, and maintain NX-series Satefy Network Controllers. Refer to *A-20 Version Information* on page A-115 for combinations of the available Support Software and its versions.
This section describes the models and connecting methods of the Sysmac Studio.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on the operating environment including computers where you can use the Sysmac Studio.

3-7-1 Product Model

Sysmac Studio products are presented in DVD media and license formats.
To purchase a new Sysmac Studio, you need to purchase both the DVD media and the license. The same DVD media works for all the licenses. You can purchase additional licenses without the DVD.
The DVD media is not included in the license version.

DVD Media

Product	32 bit/64 bit	Model
Sysmac Studio Standard Edition Ver.1.□□	32 bit	SYSMAC-SE200D
	64 bit	SYSMAC-SE200D-64

Licenses

Product	Configuration software	Number of licenses	Model
Sysmac Studio Standard Edition*1 Ver.1.□□	Sysmac Studio The following Support Software is also included. Network Configurator CX-Integrator CX-Protocol CX-Designer CX-ConfiguratorFDT Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for information on other software.	1	SYSMAC-SE201L
		3	SYSMAC-SE203L
		10	SYSMAC-SE210L
		30	SYSMAC-SE230L
		50	SYSMAC-SE250L
Sysmac Studio Safety Edition*2 Ver.1.□□		1	SYSMAC-FE001L

*1. You can design, program, debug, and maintain the NJ/NX-series Controllers and NY-series Industrial computers in addition to NX-series Safety Network Controllers.
*2. You can design, program, debug, and maintain NX-series Safety Network Controllers and EtherNet/IP Slave Terminals.

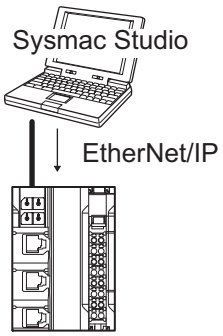
3-7-2 Connection

You can connect online the Sysmac Studio to the Communication Control Unit in the following ways. Refer to *7-4-1 Setting IP Addresses* on page 7-9 for details.

Configuration

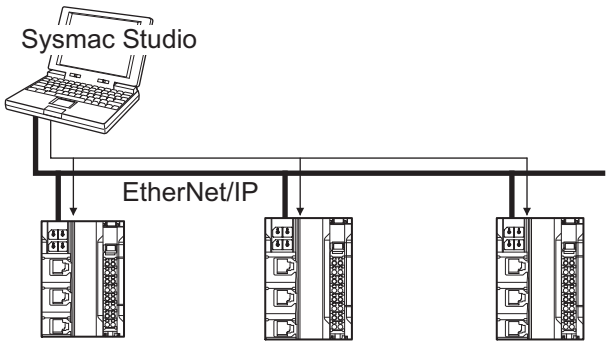
● Connection with EtherNet/IP

- 1:1 Connection



- A direct connection is made from the computer that runs Sysmac Studio. You do not need to specify the IP address or connection device.
- You can make the connection whether or not an Ethernet switch is used.
- Support for Auto-MDI enables the use of cross cables or straight cables if a direct connection is made.
- 1:1 connection is possible only for the built-in EtherNet/IP port 1.

- 1:N Connection



- Directly specify the IP address of the remote device.

3-8 PFH

This section gives the PFH (PFH_D) values of the NX-series Safety CPU Unit and the Safety I/O Units.

Precautions for Correct Use

Go to the following URL for the most recent PFH values: http://www.ia.omron.com/support/sistemalibrary/index.html

Additional Information

The NX-series Safety Control Unit is a Type B subsystem that is defined by IEC 61508 with HFT = 1 and SFF > 90%.

Safety CPU Unit

Model	PFH
NX-SL5500	5.0E-11
NX-SL5700	5.0E-11

Safety Input Unit

Model	PFH
NX-SID800	1.5E-9*1 4.3E-10*2
NX-SIH400	1.4E-9*1 3.1E-10*2

*1. This value includes PFH value of FSoE connection.

*2. This value does not include PFH value of FSoE connection.

Safety Output Unit

Model	PFH
NX-SOD400	1.6E-9*1 5.5E-10*2
NX-SOH200	1.4E-9*1 3.6E-10*2

*1. This value includes PFH value of FSoE connection.

*2. This value does not include PFH value of FSoE connection.

4

Designing the Power Supply System

This section describes how to design the power supply system for the NX-series NX-CSG320 Communication Control Unit.

4-1 Power Supply System 4-2
4-1-1 NX Unit Power Supply and I/O Power Supply 4-2
4-1-2 NX-series Power Supply-related Units 4-3
4-2 Designing the NX Unit Power Supply System 4-9
4-2-1 Procedure for Designing the NX Unit Power Supply System 4-9
4-2-2 Calculation Example for the NX Unit Power Supply 4-10
4-3 Designing the I/O Power Supply System 4-12
4-3-1 I/O Power Supply Method 4-12
4-3-2 Designing the I/O Power Supply from the NX Bus 4-13
4-3-3 Designing the I/O Power Supply from External Sources 4-18
4-3-4 Restrictions on Inrush Current for ON/OFF Operation 4-19
4-4 Selecting External Power Supplies and Protective Devices 4-20
4-4-1 Selecting the Unit Power Supply 4-20
4-4-2 Selecting the I/O Power Supplies 4-22
4-4-3 Selecting Protective Devices 4-23

4-1 Power Supply System

The power supply system for the CPU Rack of the NX-series NX-CSG320 Communication Control Unit consists of two power supply lines: one for NX Unit power and the other for I/O power. Therefore, you need to prepare two separate external power supplies for them.
You may need additional power supply Units for NX Unit power or I/O power according to the total power consumption or the total current consumption of NX Units on the CPU Rack.
Design the power supply system for the CPU Rack of the NX-series NX-CSG320 Communication Control Unit as below.

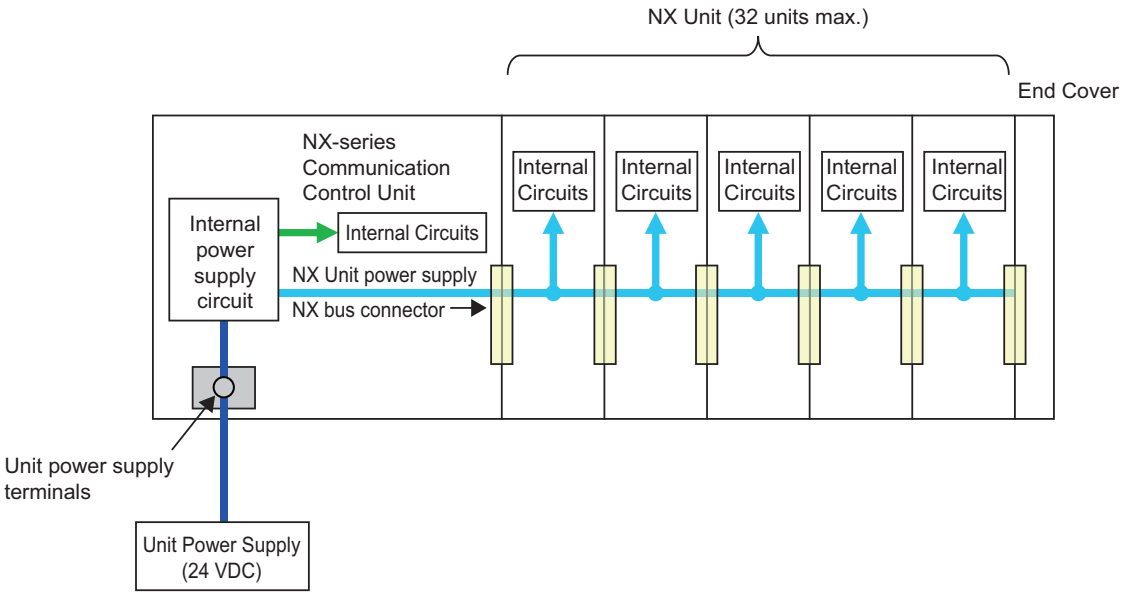
- Calculate the NX Unit power consumption to determine NX Unit power supply specifications, including whether to add additional power supply Units or not.
- Calculate the I/O power current consumption and voltage drop to determine I/O power supply specifications, including whether to add additional power supply Units or not.

4-1-1 NX Unit Power Supply and I/O Power Supply

This section provides details on NX Unit power supply and I/O power supply.

NX Unit Power Supply

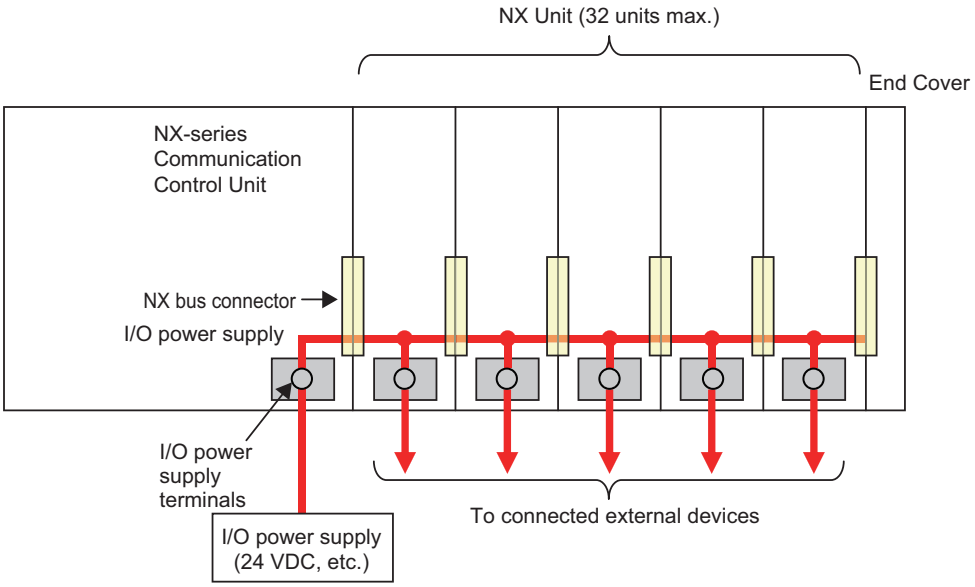
NX Unit power is supplied to the internal circuits of each NX Unit on the CPU Rack of the NX-CSG320 Communication Control Unit.
It is delivered via the Unit power supply terminals of the Communication Control Unit or those of an Additional NX Unit Power Supply Unit. Those terminals are connected to an external power supply device, which is referred to as an Unit power supply.
The Unit power supply provides power for the internal circuits of the Communication Control Unit, as well as NX Unit power for the NX Units.
Up to 10 W of NX Unit power can be delivered to NX Units via the NX bus connectors.



I/O Power Supply

I/O power is supplied to the I/O circuits of each NX Unit on the CPU Rack of the NX-CSG320 Communication Control Unit, as well as to external devices connected to the NX Units.

Some NX Units receive I/O power through the NX bus, and others receive from external devices. If any NX Unit on the CPU Rack receives I/O power through the NX bus, you need to prepare an external I/O power supply device. For details on how to supply I/O power to NX Units, refer to the datasheet included in the user's manuals for the NX Units.
Connect the I/O power supply to the I/O power supply terminals of the Communication Control Unit, or those of an Additional I/O Power Supply Unit.
When connected to the Communication Control Unit, the I/O power supply can provide up to 4 A.
When connected to the Additional I/O Power Supply Unit, it can provide up to 10 A. The I/O power is delivered to NX Units via the NX bus connectors.



Precautions for Correct Use

Make sure to prepare separate power supply devices for NX Unit power and I/O power. Using the same power supply for them may generate noise and result in malfunction.

4-1-2 NX-series Power Supply-related Units

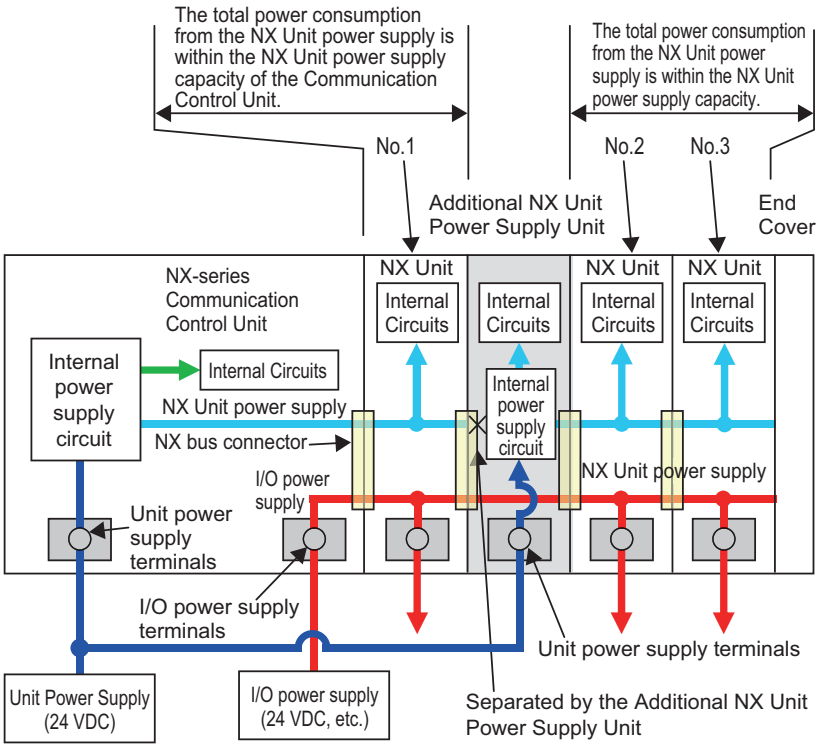
Unit name	Description
Additional NX Unit Power Supply Unit	Supply additional NX Unit power via this Unit if the total power consumption of the internal circuits of the NX Units on the CPU Rack exceeds the NX Unit power supply capacity of the Communication Control Unit.

Unit name	Description
Additional I/O Power Supply Unit	• Supply additional I/O power via this Unit if over 4 A is consumed in total by the I/O circuits of the NX Units on the CPU Rack and external devices connected to the NX Units. • Supply additional I/O power via this Unit if the I/O power voltage goes below the voltage levels specified for the I/O circuits of the NX Units on the CPU Rack or those specified for the connected external devices. • Insert this Unit to separate the I/O power supply line if any NX Unit on the CPU Rack is connected to an external device with a different I/O power supply voltage. • Insert this Unit to separate the I/O power supply line to prevent noise and other factors from affecting the other NX Units.
I/O Power Supply Connection Unit	Add this Unit to provide additional I/O power supply terminals if required to connect external devices to a Digital I/O Unit or Analog I/O Unit.

For the specifications of NX-series power supply-related Units, refer to the *NX-series System Units User's Manual (Cat. No. W523)*. For information on the latest lineup of the NX-series power supply-related Units, refer to the relevant catalogs or OMRON websites, or ask your OMRON representative.

Additional NX Unit Power Supply Unit

You can use Additional NX Unit Power Supply Units to deliver additional supply of NX Unit power when the total power consumption of the internal circuits of NX Units on the CPU Rack exceeds the NX Unit power supply capacity of the Communication Control Unit.
The following figure shows how to use an Additional NX Unit Power Supply Unit. Assume that three NX Units, No.1 to No.3, are connected to the CPU Rack, as shown below. Also assume that only NX Unit No.1 is supplied with adequate NX Unit power because the total power consumption of the internal circuits of the three NX Units exceeds the NX Unit power supply capacity of the Communication Control Unit. In this case, insert an Additional NX Unit Power Supply Unit between NX Units No.1 and No.2. Connect its Unit power supply terminals to the Unit power supply. The NX Unit power is supplied to NX Units No.2 and No.3 via the inserted Additional NX Unit Power Supply Unit, instead of the Communication Control Unit.
More than one Additional NX Unit Power Supply Unit can be connected to the CPU Rack. If adequate NX Unit power is not provided for all the NX Units on the right side of the Additional NX Unit Power Supply Unit, add another Additional NX Unit Power Supply Unit to an appropriate place.
Basically, the NX Unit power supply line connects adjacent NX Units through the NX bus. However, the NX Unit power supply line is separated by an inserted Additional NX Unit Power Supply Unit. In the figure below, the NX Unit power supply line is separated between NX Unit No.1 and the Additional NX Unit Power Supply Unit. However, the I/O power supply line is not separated by the Additional NX Unit Power Supply Unit. Therefore, the I/O power supply line is connected through all the NX Units, No.1 to No.3.



Additional I/O Power Supply Unit

The following explains how to use Additional I/O Power Supply Units.

- Supply additional I/O power via this Unit if over 4 A is consumed in total by the I/O circuits of the NX Units on the CPU Rack and external devices connected to the NX Units.
- Supply additional I/O power via this Unit if the I/O power voltage goes below the voltage levels specified for the I/O circuits of the NX Units on the CPU Rack or those specified for the connected external devices.
- Insert this Unit to separate the I/O power supply line if any NX Unit on the CPU Rack is connected to an external device with a different I/O power supply voltage.
- Insert this Unit to separate the I/O power supply line to prevent noise and other factors from affecting the other NX Units.

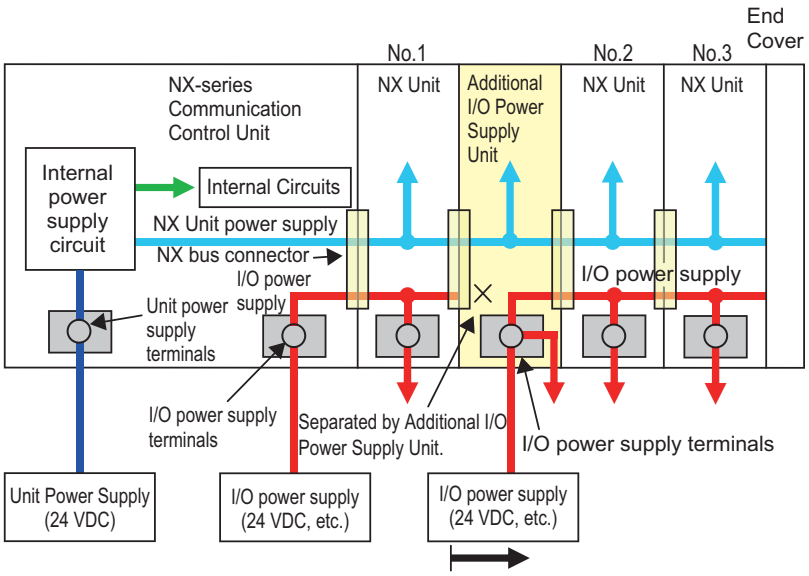
● Additional Supply of I/O Power

You need an Additional I/O Power Supply Unit in the following cases.

- Over 4 A is consumed in total by the I/O circuits of the NX Units on the CPU Rack and external devices connected to the NX Units.
- The I/O power voltage goes below the voltage levels specified for the I/O circuits of the NX Units on the CPU Rack or those specified for the connected external devices.

Assume that three NX Units, No.1 to No.3, are connected to the CPU Rack, as shown below. Also assume that only NX Unit No.1 is supplied with adequate current and voltage because one external I/O power supply device cannot cover the total current consumption of the I/O circuits of the three NX Units, the total current consumption of the connected external devices, or I/O power voltage. In this case, insert another Additional I/O Power Supply Unit between NX Units No.1 and No.2. Connect its I/O power supply terminals to an I/O power supply device which is prepared separately

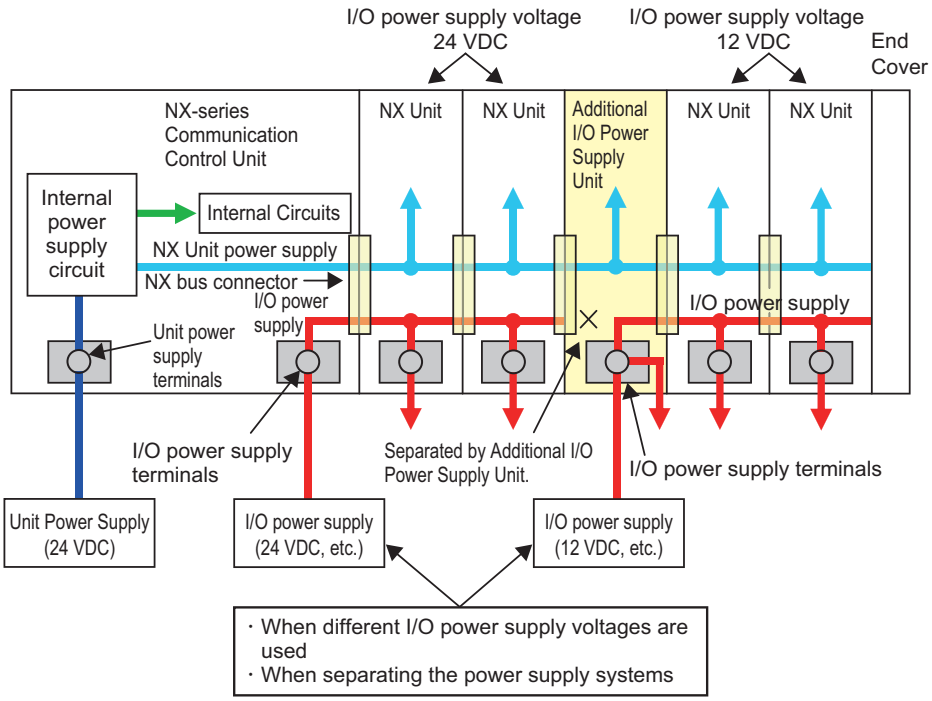
from the existing one. The I/O power is supplied to NX Units No.2 and No.3 via the inserted Additional I/O Power Supply Unit.
More than one Additional I/O Power Supply Unit can be connected to the CPU Rack. If adequate I/O power is not provided for all the NX Units on the right side of the Additional I/O Power Supply Unit, add another Additional I/O Power Supply Unit to an appropriate place.
Basically, the I/O power supply line connects adjacent NX Units through the NX bus. However, the I/O power supply line is separated by an inserted Additional I/O Power Supply Unit. In the figure below, the I/O power supply line is separated between NX Unit No.1 and the Additional I/O Power Supply Unit. However, the NX Unit power supply line is not separated by the Additional I/O Power Supply Unit. Therefore, the NX unit power supply line is connected through all the NX Units, No.1 to No.3, as shown below.



When the I/O power supply becomes the following states for the subsequent NX Units:
- When it exceeds the maximum I/O power supply current (4A)
- When it goes below the voltage specifications of the connected external devices

● Separating the I/O Power Supply Line

Insert an Additional I/O Power Supply Unit to separate the I/O power supply line when you connect an NX Unit on the CPU Rack to an external device with a different I/O power voltage, or when you prevent noise or other factors from affecting other NX Units.
Assume that the CPU Rack contains some NX Units with I/O power voltage of 24 VDC and others with 12 VDC, as shown in the figure below. In this case, insert an Additional I/O Power Supply Unit for the NX Units with 12 VDC. Connect the power supply terminals of the Communication Control Unit to an I/O power supply with 24 VDC, and those of the Additional I/O Power Supply Unit to another I/O power supply with 12 VDC.
Basically, the I/O power supply line connects adjacent NX Units through the NX bus. However, the I/O power supply line is separated by an inserted Additional I/O Power Supply Unit. In the figure below, the I/O power supply line is separated between the NX Units with 24 VDC and the ones with 12 VDC. However, the NX Unit power supply line is connected through all the NX Units.

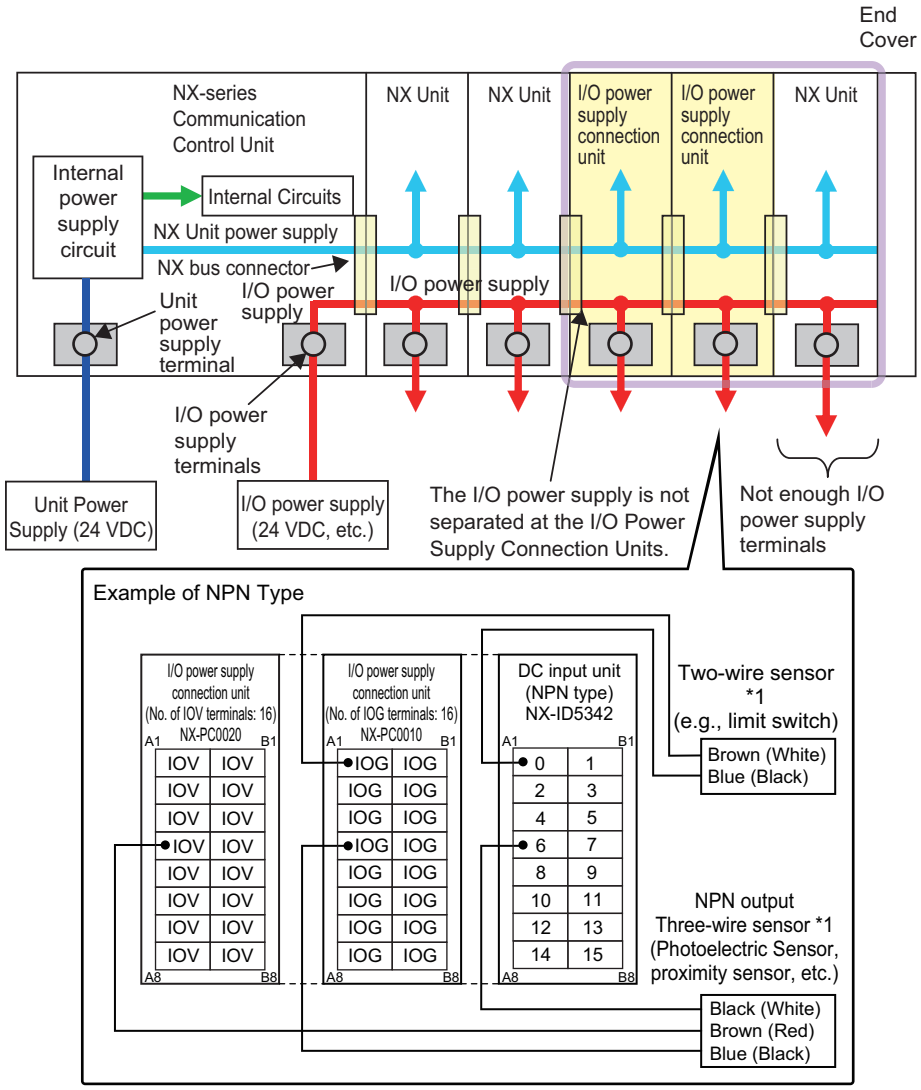


I/O Power Supply Connection Unit

You can add an I/O Power Supply Connection Unit to provide additional I/O power supply terminals if required to connect external devices to a Digital I/O Unit or Analog I/O Unit.

The following figure shows how to use I/O Power Supply Connection Units. Assume that a PNP-type Digital Input Unit, NX-ID5342, is used to input signals from a two-wire sensor and a three-wire sensor with NPN output. The NX-ID5342 Digital Input Unit does not have I/O power terminals. For the Digital Input Unit, you need to prepare IOG terminals for the two-wire sensor, and IOV terminals as well as IOG terminals for the three-wire sensor. Insert two I/O Power Supply Connection Units: one is NX-PC0020 with 16 IOV terminals, and the other is NX-PC0010 with 16 IOG terminals. Wire them as shown in the figure below.

The NX Unit power supply line as well as the I/O power supply line is connected between the I/O Power Supply Connection Units and adjacent NX Units through the NX bus.



*1. Wire colors have been changed according to revisions in the JIS standards for photoelectric and proximity sensors. The colors in parentheses are the wire colors prior to the revisions.

4-2 Designing the NX Unit Power Supply System

This section describes how to design the NX Unit power supply to the CPU Rack of the NX-series NX-CSG320 Communication Control Unit.

4-2-1 Procedure for Designing the NX Unit Power Supply System

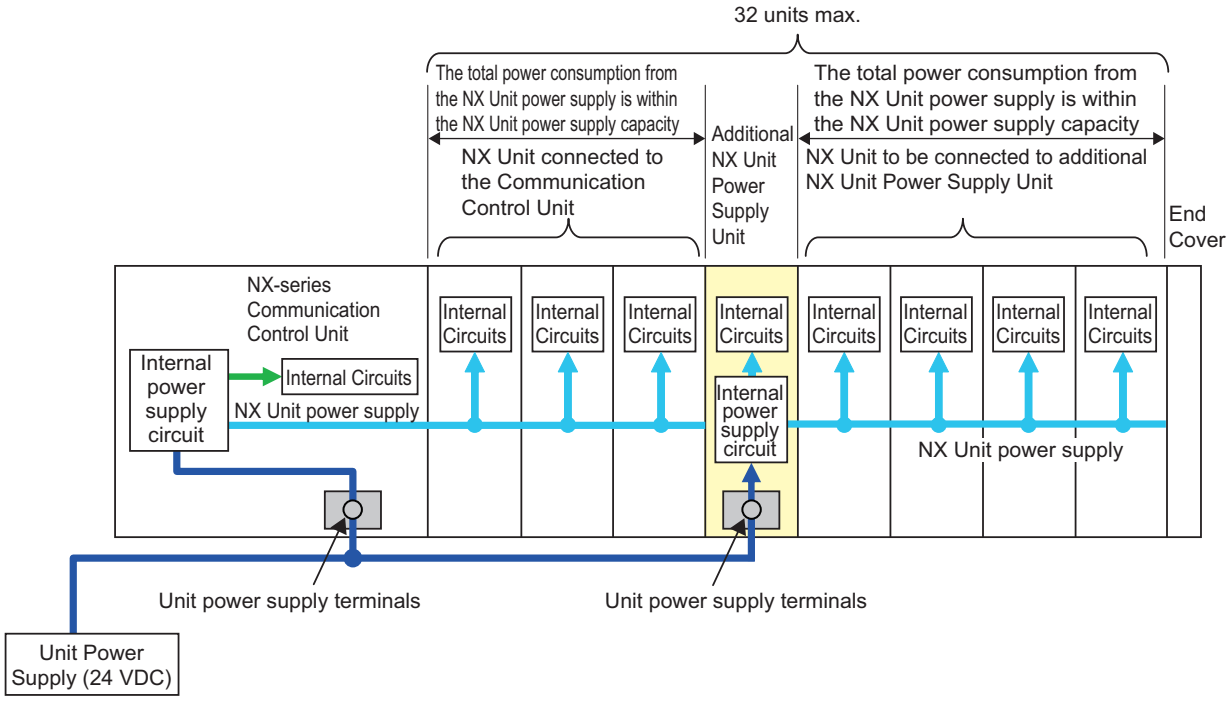
The total power consumption from the NX Unit power supply must not exceed the NX Unit power supply capacity of the Unit that supplies the NX Unit power.
Use the following procedure to design the NX Unit power supply.

1. Calculate the total power consumption from the NX Unit power supply that is required by the NX Units that are connected to the Communication Control Unit.

2. If the total power consumption from the NX Unit power supply exceeds the NX Unit power supply capacity of the Communication Control Unit, add an Additional NX Unit Power Supply Unit to the right of an NX Unit before the capacity is exceeded.

3. Calculate the total power consumption from the NX Unit power supply that is required by the NX Units that are connected after the Additional NX Unit Power Supply Unit. If the total power consumption of those NX Units exceeds the NX Unit power supply capacity of the Additional NX Unit Power Supply Unit, add another Additional NX Unit Power Supply Unit to the right of an NX Unit before the capacity is exceeded.

4. Repeat step 3 until the design conditions for the NX Unit power supply are met.



● NX Unit Power Supply Capacity and Restrictions

The internal power supply circuits of the Communication Control Unit or Additional NX Unit Power Supply Unit supply the NX Unit power to the NX Units.

The NX Unit power supply capacity does not include the NX Unit power consumption of the Additional NX Unit Power Supply Units.

The power supply capacity of the Communication Control Unit is 10 W.

For restrictions on the Additional NX Unit Power Supply Unit, refer to the *NX-series System Units User's Manual* (Cat. No. W523).

Precautions for Correct Use

- Do not exceed the NX Unit power supply capacity. If you exceed the NX Unit power supply capacity, malfunction may occur.
- Use the same Unit power supply to supply the Unit power to the entire CPU Rack. If you supply power from different Unit power supplies, differences in electrical potential may cause unexpected currents in the NX Unit power supply, which may result in failure or malfunction.

4-2-2 Calculation Example for the NX Unit Power Supply

This section provides a calculation example for the NX Unit power supply.

● Unit Configuration Example

Name	Model	Quantity	Power consumption/Unit*1
Communication Control Unit	NX-CSG320	1	5.95 W
Safety CPU Unit	NX-SL5700	1	3.35 W
Safety Input Unit	NX-SID800	3	1.10 W
Safety Output Unit	NX-SOD400	2	1.10 W

*1. For the power consumption of NX Units connected to Communication Control Unit, refer to the user's manuals for the respective NX Units.

● Calculating the Total Power Consumption from the NX Unit Power Supply

Calculate the total power consumption from the NX Unit power supply that is required by the NX Units that are connected to the Communication Control Unit.

Total power consumption from NX Unit power supply [W] = 3.35 W × 1 + 1.10 W × 3 + 1.10 W × 2 = 8.85 W

● Confirming the NX Unit Power Supply Capacity of the Communication Control Unit

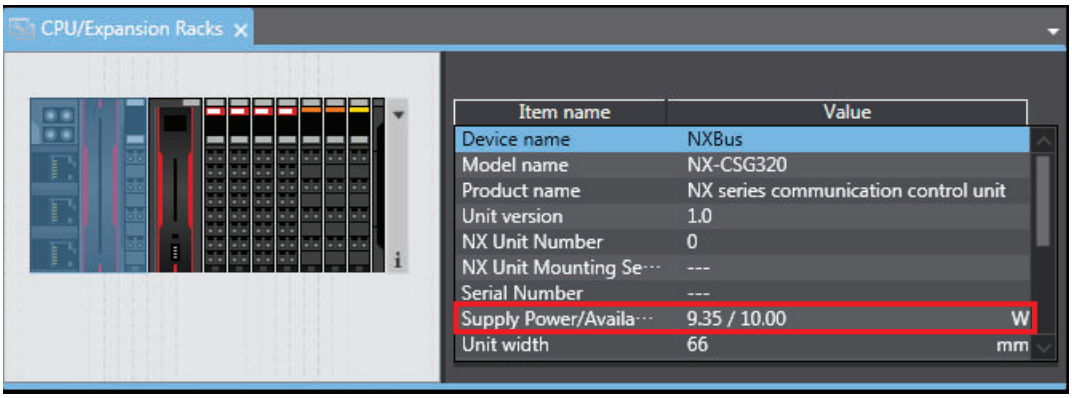
The NX Unit power supply capacity is 10 W max.

Therefore, in this example, the total power consumption from the NX Unit power supply is 8.85 W, and the NX Unit power supply capacity is 10 W max., so the design conditions are met.

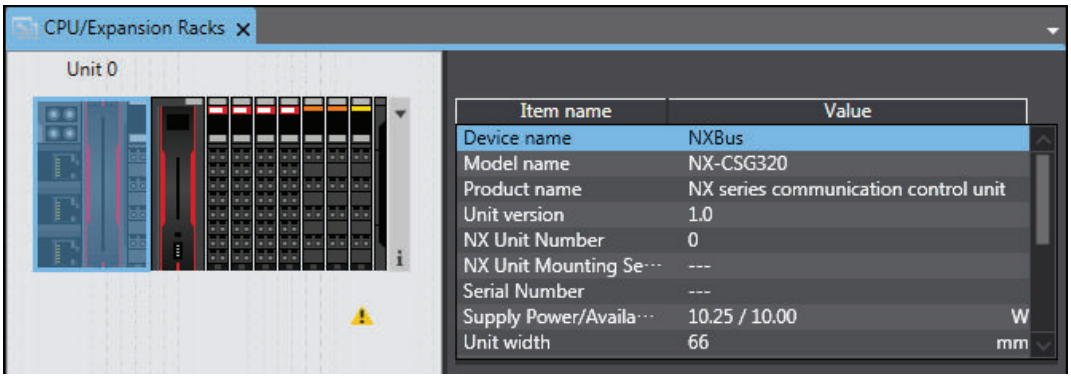
Additional Information

Excess or insufficiency in the NX Unit power supply capacity can be easily checked when the Unit configuration is created on the CPU and Expansion Racks Tab Page on the Sysmac Studio.
Use the following procedure to check the power supply capacity.

On the CPU and Expansion Racks Tab Page on the Sysmac Studio, select the Unit to supply NX Unit power. The power that is supplied by the NX Unit power supply (i.e., the total power consumption) and the power supply capacity are displayed for the **Supply Power/Available Power** parameter.
The following example is for when the NX-CSG320 Communication Control Unit is selected.



If the power to supply exceeds the NX Unit power supply capacity of the Unit that is selected to supply the NX Unit power, a yellow warning icon is displayed by the first NX Unit for which there is not sufficient capacity and also by all the remaining NX Units.



The Sysmac Studio does not consider the I/O power supply design conditions. When actually designing the power supply, refer to *4-3-2 Designing the I/O Power Supply from the NX Bus* on page 4-13.

4-3 Designing the I/O Power Supply System

This section describes how to design the I/O power supply to the NX Units connected to the NX-series NX-CSG320 Communication Control Unit.

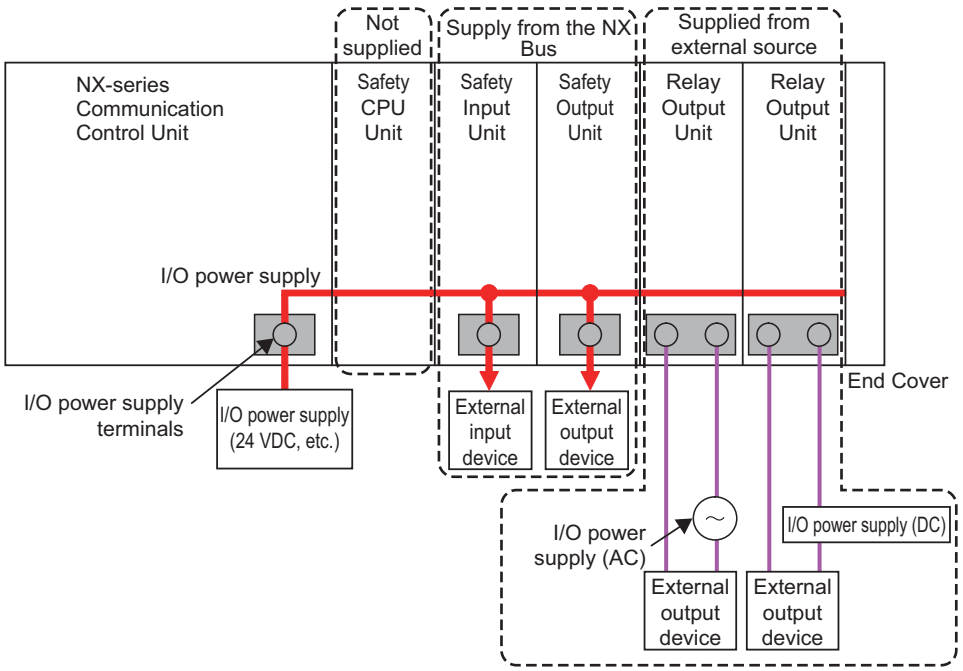
4-3-1 I/O Power Supply Method

There are the following three methods to supply the I/O power supply to the NX Units depending on the type and model of the NX Units.

Supply method	Description
Supply from the NX bus	Power is supplied through the NX bus connectors by connecting an I/O power supply to the I/O power supply terminals on the NX-series Communication Control Unit or an Additional I/O Power Supply Unit.
Supply from external source	Power is supplied to the Units from an external source. I/O power is supplied by connecting an I/O power supply to the terminal blocks on the Units.
No supply	The I/O power supply is not needed when the NX Unit does not use it for the connected external devices, or when power for the interface is generated inside the NX Unit.

Refer to the user's manuals for individual NX Units or to the *NX-series Data Reference Manual (Cat. No. W525)* for the power supply method for specific NX Units.

An example is shown below.



4-3-2 Designing the I/O Power Supply from the NX Bus

Procedure for Designing the I/O Power Supply

Make sure that the following design conditions are met when you design the I/O power supply from the NX bus.

- The total current consumption from the I/O power supply must not exceed the maximum I/O power supply current of the Unit that supplies the I/O power.
- The voltage drop in the I/O power supply must be within the voltage specifications of the I/O circuits of the NX Units and the connected external devices.

Use the following procedure to design the I/O power supply.

1 Calculate the total current consumption from the I/O power supply of the NX Units that are connected to the Communication Control Unit and the Communication Control Unit, and calculate the voltage drop in the I/O power supply.

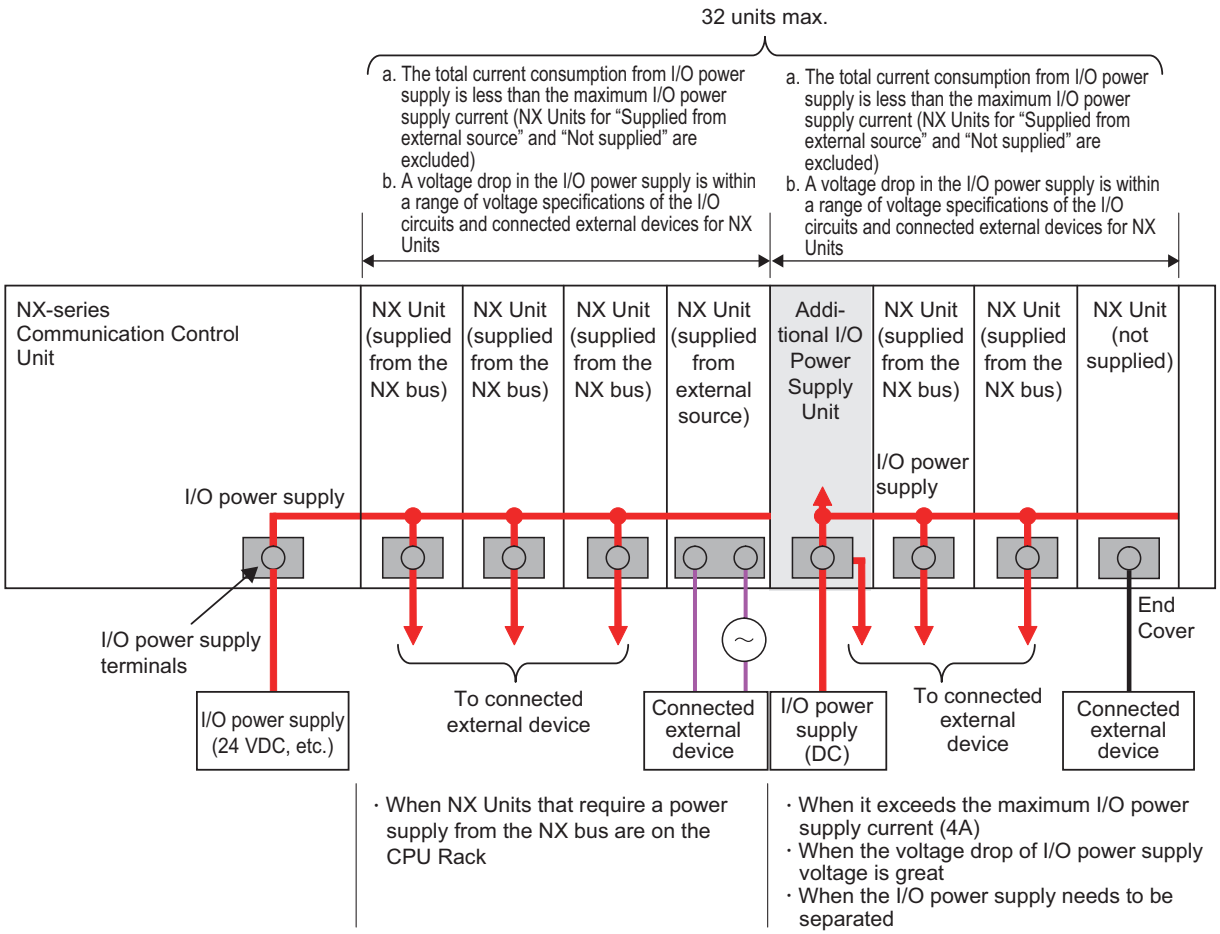
2 Add an Additional I/O Power Supply Unit in either of the following cases, a) or b). Add the Additional I/O Power Supply Unit to the right of the NX Unit for which both a) and b) do not apply.

a) The total current consumption for the I/O power supply exceeds 4 A.
b) Voltage drop in the I/O power supply causes the voltage of the I/O power supply to go below the voltage specifications of the I/O circuits of the NX Units or the connected external devices.

3 Calculate the voltage drop in the I/O power supply after the Additional I/O Power Supply Unit and the total current consumption from the I/O power supply that is required by the Additional I/O Power Supply Unit and by the NX Units that are connected after the Additional I/O Power Supply Unit. Add another Additional I/O Power Supply Unit in either of the following cases, a) or b). Add the Additional I/O Power Supply Unit to the right of the NX Unit for which both a) and b) do not apply.

a) The total current consumption for the I/O power supply exceeds the I/O power supply capacity of the Additional I/O Power Supply Unit.
b) Voltage drop in the I/O power supply causes the voltage of the I/O power supply to go below the voltage specifications of the I/O circuits of the NX Units or the connected external devices.

4 Repeat step 3 until the design conditions for the I/O power supply are met.



● Maximum I/O Power Supply Current

The maximum I/O current refers to the maximum current that can be supplied to the NX Units from I/O power supply terminals of the Communication Control Unit or the I/O power supply connected to the Additional I/O Power Supply Unit via an NX bus connector.

For information on the maximum I/O power current supplied from the Additional I/O Power Supply Unit, refer to the *NX-series System Units User's Manual (Cat. No. W523)*.

Precautions for Safe Use

Use the I/O power current supplied to the CPU Rack from I/O power supply terminals of the NX-CSG320 Communication Control Unit at 4 A or less. Using the currents that are outside of the specifications may cause failure or damage.

Calculating the Total Current Consumption from the I/O Power Supply

The total current consumption from the I/O power supply from the NX bus is the total of the following current consumptions.

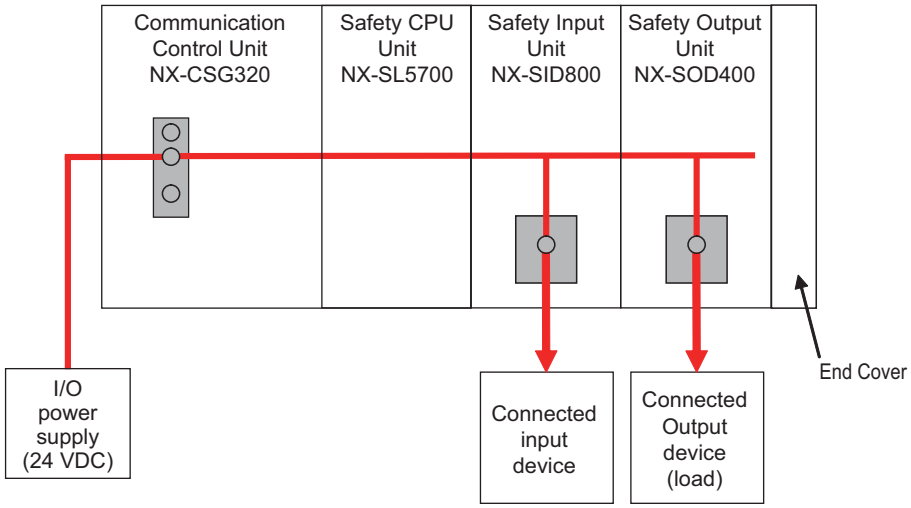
- The current consumption from the I/O power supply that is required for the Communication Control Unit, for the Additional I/O Power Supply Unit, and for the NX Units that are connected to them
- The current consumption between the NX Units and the connected external devices

Current consumption item	Description
Current consumption from I/O power supply	This is the current that is consumed by the internal circuits that operate on the I/O power supply. Specific values are given in the user's manuals for individual Units.
Current consumption between the NX Units and the connected external devices	This is the current that is consumed between the NX Units and the connected external devices. For example, this is the current consumed by a Digital Input Unit to supply power to photoelectric sensors or to turn ON the input circuits in the Digital Input Unit. The current consumption depends on the type of I/O circuit in the NX Unit, the number of I/O points that are used, and the current consumption of the connected external device. It must be calculated for each NX Unit.

● Calculation Example of I/O Power Supply Capacity

An example of calculating the required power supply capacity of the I/O power supply is given below.

Configuration and Conditions



Item		Condition
I/O power supply voltage		24 VDC
Input	Number of inputs used (that turn ON simultaneously)	4 points
	Current consumption of connected input devices	50 mA/point
Output	Number of output points (that turn ON simultaneously)	4 points
	Load current of connected loads	0 mA/point
	Current consumption of connected output devices	50 mA/point

I/O power is supplied to the NX-SID800 and NX-SOD400 from the NX bus.

a. Unit Specifications

Model	Current consumption from I/O power supply	Input current
NX-CSG320	10 mA	---
NX-SL5700	0 mA	---
NX-SID800	20 mA	6 mA/point
NX-SOD400	60 mA	---

b. Calculations

The current consumption from the I/O power supply for each Unit is calculated as follows.

NX-CSG320 Current Consumption	=	(Current consumption from I/O power supply)
	=	10 mA

NX-SL5700 Current Consumption	=	(Current consumption from I/O power supply)
	=	0 mA

NX-SID800 Current Consumption	=	Current consumption from I/O power supply + (Input current × Number of inputs used) + Total current consumption of connected input devices
	=	20 mA + (6 mA × 4 points) + (50 mA × 4 points)
	=	244 mA

NX-SOD400 Current Consumption	=	Current consumption from I/O power supply + Total load current of connected loads + Total current consumption of connected output devices
	=	60 mA + (0 mA × 4 points) + (50 mA × 4 points)
	=	260 mA

The power supply capacity of the I/O power supply is given below.

Power Supply Capacity of I/O Power Supply	=	Current consumed by NX-CSG320 + (Current consumed by NX-SL5700) + (Current consumed by NX-SID800) + (Current consumed by NX-SOD400)
	=	10 mA + 0 mA + 244 mA + 260 mA
	=	514 mA

Calculating the Voltage Drop in the I/O Power Supply

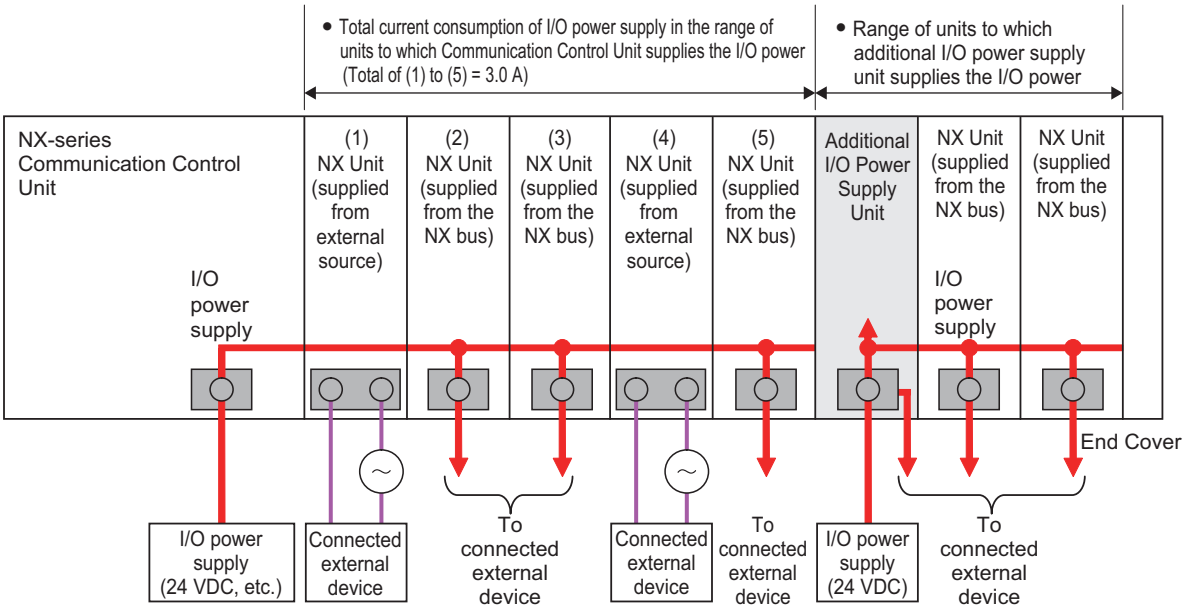
Voltage drop occurs in the Communication Control Units and NX Units due to the contact resistance at the points where Units are connected to each other. Design the I/O power supply system to maintain the voltage specifications of the NX Unit I/O circuits and connected external devices even if the voltage of the I/O power supply drops.

As shown in the following table, the voltage drop per Unit depends on the total current consumption from the I/O power supply.

Total current consumption from the I/O power supply	Voltage drop per Unit
10 A	0.20 V
8 A	0.16 V
6 A	0.12 V
4 A	0.08 V
3 A	0.06 V
2 A	0.04 V
1 A	0.02 V

Here, the following Unit configuration example is used to show how to calculate the I/O power that is supplied by the Additional I/O Power Supply Unit on the right of the Communication Control Unit. You can also use the same calculation procedure to calculate the I/O power supply range for the Additional I/O Power Supply Unit.

Example:



Current consumption from I/O power supply for each unit

(1) : 0.0 A*1 (supplied from the NX bus)
(2),(3) : 0.5 A for each (supplied from the NX bus)
(4) : 0.0 A (supplied from external source)
(5) : 2.0 A (supplied from the NX bus)

*1. The current consumption of the Additional I/O Power Supply Unit is not actually 0 A. However, a value of 0 A is used in this calculation example.

In actual calculations, add the current consumption from the I/O power supply that is given in the *NX-series Data Reference Manual (Cat. No. W525)*.

● Outline

Find the I/O power supply voltage of the NX Unit that is the farthest from the Communication Control Unit. In this example, the I/O power supply voltage of Unit (5) is found.

● Conditions

Assume that an I/O power supply voltage of 24.00 VDC is supplied to the I/O power supply terminals on the Communication Control Unit.

● Procedure

1 Use the following formula to calculate the total current consumption from the I/O power supply.

Total current consumption from the I/O power supply	=	(1) + (2) + (3) + (4) + (5)
	=	0.0 A + 0.5 A + 0.5 A + 0.0 A + 2.0 A
	=	3 A

2 Find the I/O power supply voltage and make sure that it is within the voltage specifications of the I/O circuits of the NX Units and the connected external devices.

I/O power supply voltage at (5)	=	I/O power supply voltage on I/O power supply terminals − Voltage drop per Unit × Number of Units passed through
	=	24.00 V − 0.06 V × 5 Units
	=	23.70 V

Design to Separate the I/O Power Supply

If the I/O power supply voltages of the connected external devices are different, connect an Additional I/O Power Supply Unit at the point where the I/O power supply voltage changes and then perform similar calculations to design a system that meets the power supply conditions. The same method is used to separate the power supply systems. Connect an Additional I/O Power Supply Unit at the point where the power supply systems to be separated and then perform similar calculations to design the overall system to meet the power supply conditions.

4-3-3 Designing the I/O Power Supply from External Sources

Calculate the total current consumption from the I/O power supply for the NX Units to be supplied power from an external source.
Refer to the user's manuals of the NX Units for the total current consumption from the I/O power supply.

4-3-4 Restrictions on Inrush Current for ON/OFF Operation

This section describes the restrictions on inrush current from the I/O power supply that occurs when connected external devices turn ON and OFF.

Inrush Current Restrictions

If inrush current to the I/O power supply occurs when a connected external device turns ON or OFF, do not allow the effective value of the I/O power supply current to exceed the following rated values when the inrush current is added to the current consumption from the I/O power supply.

- Maximum I/O power supply current
- Current capacity of power supply terminals for the I/O power supply

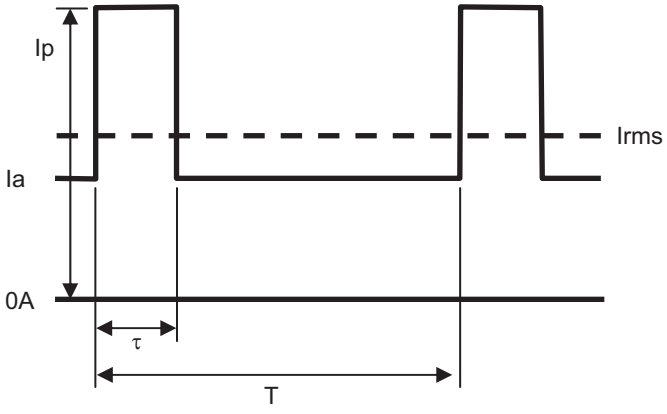
Also, maintain the peak inrush current 20 A maximum and maintain the pulse width 1 s maximum.
Refer to *4-4-3 Selecting Protective Devices* on page 4-23 for the rated values of the items when the CPU Rack is used.

Calculating the Effective Value of the I/O Power Supply Current

The formula to calculate the effective value of the I/O power supply current, Irms, is given below.

$$Irms=\sqrt{Ip^2 \times D+Ia^2 \times (1-D)}$$
$$(D=\tau/T)$$

- Ip: Peak inrush current (A)
- Irms: Effective value of I/O power supply current (A)
- Ia: Total current consumption from the I/O power supply (A)
- D: Inrush current duty
- τ: Inrush current pulse width (s)
- T: Inrush current period (s)



4-4 Selecting External Power Supplies and Protective Devices

This section describes how to select the Unit power supply and the I/O power supply which are the external power supplies for the CPU Rack, and how to select the protective devices.

4-4-1 Selecting the Unit Power Supply

This section describes how to select the Unit power supply for the CPU Rack.

Requirements for Power Supplies

Use an SELV power supply that meets the following conditions for the Unit power supply.

- Has overcurrent protection.
- Has double or reinforced insulation between the input and output.
- Has an output voltage of 24 VDC (20.4 to 28.8 VDC).

Recommended Power Supplies: S8VK-S Series (manufactured by OMRON)

Calculating the Required Power Supply Capacity of the Unit Power Supply

● Formula

This section describes how to calculate the required capacity of the Unit power supply for the CPU Rack.

Required capacity of the Unit power supply for the CPU Rack	=	Total of required Unit power supply capacity for each block

Use the following formula to calculate the required Unit power supply capacity for each block in the CPU Rack.

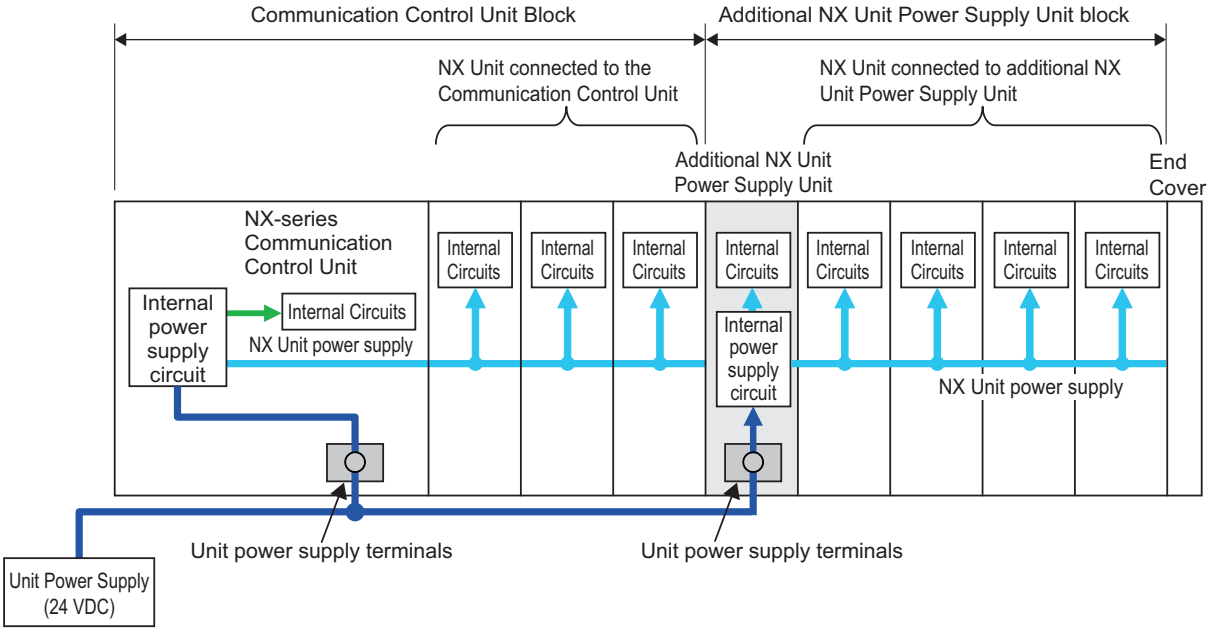
Required Unit power supply capacity of the Communication Control Unit block = (A) + (B)/(C)

Required Unit power supply capacity of an Additional NX Unit Power Supply Unit block = ((D) + (E))/(F)

(A)	Unit power consumption of the Communication Control Unit
(B)	Total NX Unit power consumption of NX Units that are connected to the Communication Control Unit
(C)	NX Unit power supply efficiency of the Communication Control Unit
(D)	NX Unit power consumption of the Additional NX Unit Power Supply Unit
(E)	Total NX Unit power consumption of NX Units that are connected to the Additional NX Unit Power Supply Unit
(F)	NX Unit power supply efficiency of the Additional NX Unit Power Supply Unit

Blocks

A block consists of the Unit that supplies the NX Unit power and the range of Units to which that Unit supplies the NX Unit power.



The total of the required Unit power supply capacity for these two blocks is the required power supply capacity of the Unit power supply for the CPU Rack.

Precautions for Correct Use

Use the same Unit power supply to supply the Unit power to one CPU Rack. If you supply power from different Unit power supplies, differences in electrical potential may cause unexpected currents in the NX Unit power supply, which may result in failure or malfunction.

Calculation Example

This section provides a calculation example for the configuration example that is given in *4-2-2 Calculation Example for the NX Unit Power Supply* on page 4-10.

Name	Model	Quantity	Power consumption/ Unit
Communication Control Unit	NX-CSG320	1	5.95 W
Safety CPU Unit	NX-SL5700	1	3.35 W
Safety Input Unit	NX-SID800	3	1.10 W
Safety Output Unit	NX-SOD400	2	1.10 W

- The NX Unit power supply efficiency of the Communication Control Unit is 80%.

In this configuration example, there is only one block, the Communication Control Unit block.
Required power supply capacity of Unit power supply to CPU Rack
= Required Unit power supply capacity of the Communication Control Unit block
= Unit power consumption of the Communication Control Unit + Total power consumption from NX Unit power supply of NX Units connected to the Communication Control Unit / NX Unit power supply efficiency of the Communication Control Unit

= 5.95 W + (3.35 W × 1 + 1.10 W × 3 + 1.10 W × 2)/0.8
= Approx. 18.5 W

The above is the stationary power consumption during operation. When you select the power supply, consider the inrush current that will flow when the power is turned ON.
Refer to *Section 3 Specifications of Configuration Units* on page 3-1 for information on inrush current specifications.

Precautions for Safe Use

Select an external power supply with sufficient capacity by considering the power supply capacity or inrush current when the power is turned ON. Otherwise, the external power supply may not be turned ON or it may malfunction due to unstable voltage.

4-4-2 Selecting the I/O Power Supplies

This section describes how to select the I/O power supplies for the CPU Rack.

Requirements for Power Supplies

Use an SELV power supply that meets the following conditions for the I/O power supply.

- Has overcurrent protection.
- Has double or reinforced insulation between the input and output.
- Has an output voltage of 5 to 24 VDC (4.5 to 28.8 VDC).*1

*1. Use an output voltage that is appropriate for the I/O circuits of the NX Units and the connected external devices.

Recommended Power Supplies: S8VK-S Series (manufactured by OMRON)

Calculating the Required Power Supply Capacity of the I/O Power Supply for NX Units

Use the calculation method that is described in *4-3-2 Designing the I/O Power Supply from the NX Bus* on page 4-13 and calculate the total current consumption from the I/O power supply and the required power supply capacity of the I/O power supply.
Unlike the Unit power supply, it is not necessary to use only one I/O power supply to supply power to all NX Units on the CPU Rack.

Precautions for Safe Use

Select an external power supply with sufficient capacity by considering the power supply capacity or inrush current when the power is turned ON that is specified in this manual. Otherwise, the external power supply may not be turned ON or malfunction due to unstable power supply voltage.

4-4-3 Selecting Protective Devices

This section describes how to select protective devices (e.g., breakers and fuses) to protect against short circuits and overcurrents in external circuits.
Overcurrent is the current that flows when an excessive load is connected and one of the following ratings is exceeded.

Unit	Item for rating	Rated value
Communication Control Unit	NX Unit power supply capacity	10 W max.
	Current capacity of power supply terminal	4 A max.
Additional NX Unit Power Supply Unit	NX Unit power supply capacity	Refer to the *NX-series System Units User's Manual (Cat. No. W523)*.
	Current capacity of power supply terminal	
Additional I/O Power Supply Unit	Maximum I/O power supply current	
	Current capacity of I/O power supply terminals	

Precautions for Safe Use

Use the I/O power current supplied to the CPU Rack from I/O power supply terminals of the NX-CSG320 Communication Control Unit at 4 A or less. Using the currents that are outside of the specifications may cause failure or damage.

Selecting Protective Devices

Consider the following items when you select protective devices.

- Protective device specifications (breaking/fusing, detection characteristics, steady current value, etc.)
- Inrush current when power is turned ON
- Inrush current when connected external devices turn ON and OFF*1

*1. Refer to *4-3-4 Restrictions on Inrush Current for ON/OFF Operation* on page 4-19 for information on the inrush current when connected external devices are turned ON and OFF.

For the breaking/fusing time, use protective devices that meet the conditions in the following table.

● For Unit Power Supply

Current	Breaking/fusing time
6 A	1 min max.
12 A	15 s max.
21 A	5 s max.
30 A	2.5 s max.

● For I/O Power Supply

The following values apply when the current capacity of power supply terminal is 10 A.

Current	Breaking/fusing time
14 A	1 min max.
28 A	9 s max.

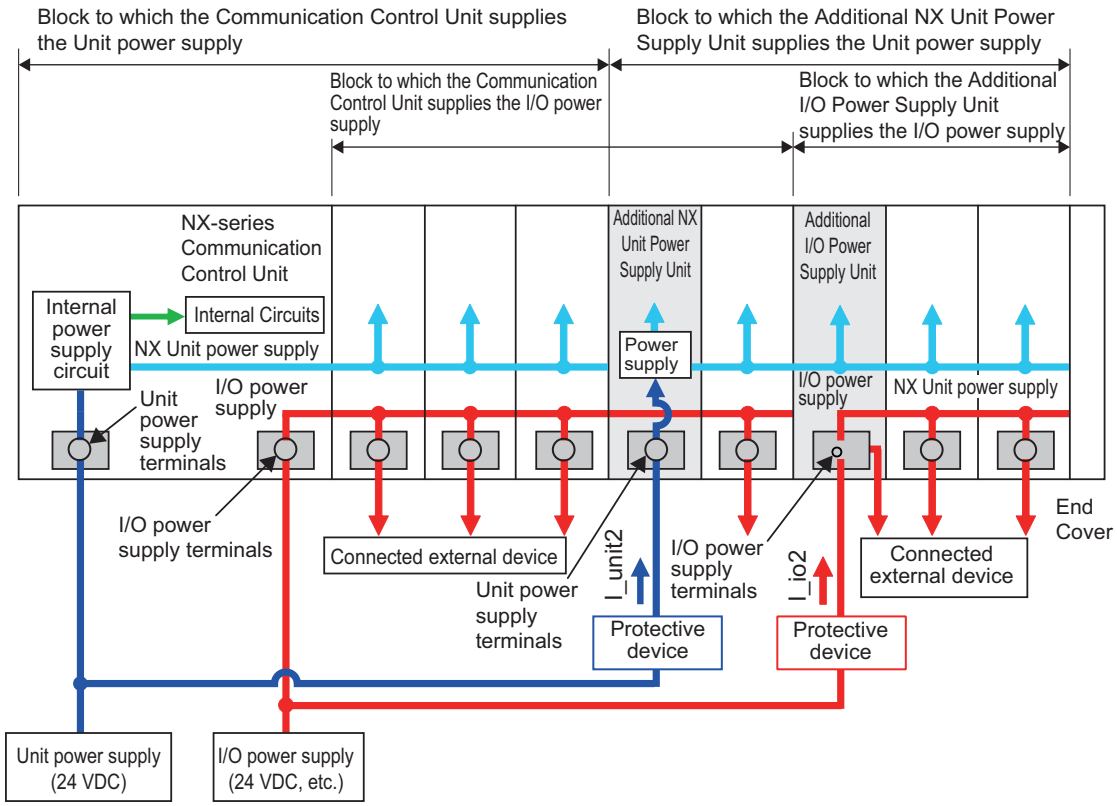
Current	Breaking/fusing time
56 A	1.5 s max.
70 A	0.8 s max.

The following values apply when the current capacity of power supply terminal is 4 A.

Current	Breaking/fusing time
6 A	1 min max.
12 A	15 s max.
21 A	5 s max.
30 A	2.5 s max.

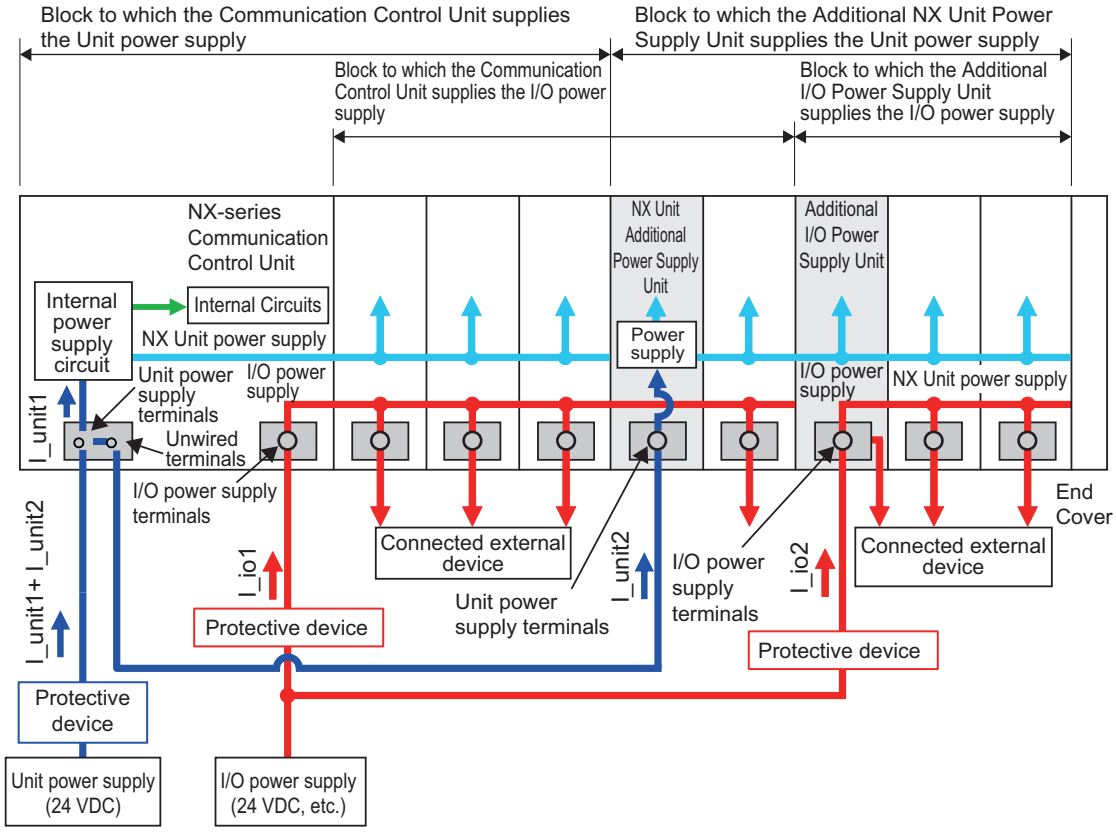
Installation Locations for Protective Devices

Install protective devices for the Unit power supply and I/O power supply in the locations that are shown in the following figure.



However, fewer protective devices may be required when the current consumption of each block does not exceed the rated current.
An example of this is provided below.

- Using Unwired Unit Power Supply Terminals
  In this example, the current consumption from each power supply is as follows:
  Current consumption from Unit power supply: I_unit1 + I_unit2 ≤ Lowest rated current
  Current consumption from I/O power supply for NX Units: I_io1 + I_io2 ≥ Lowest rated current[*1]



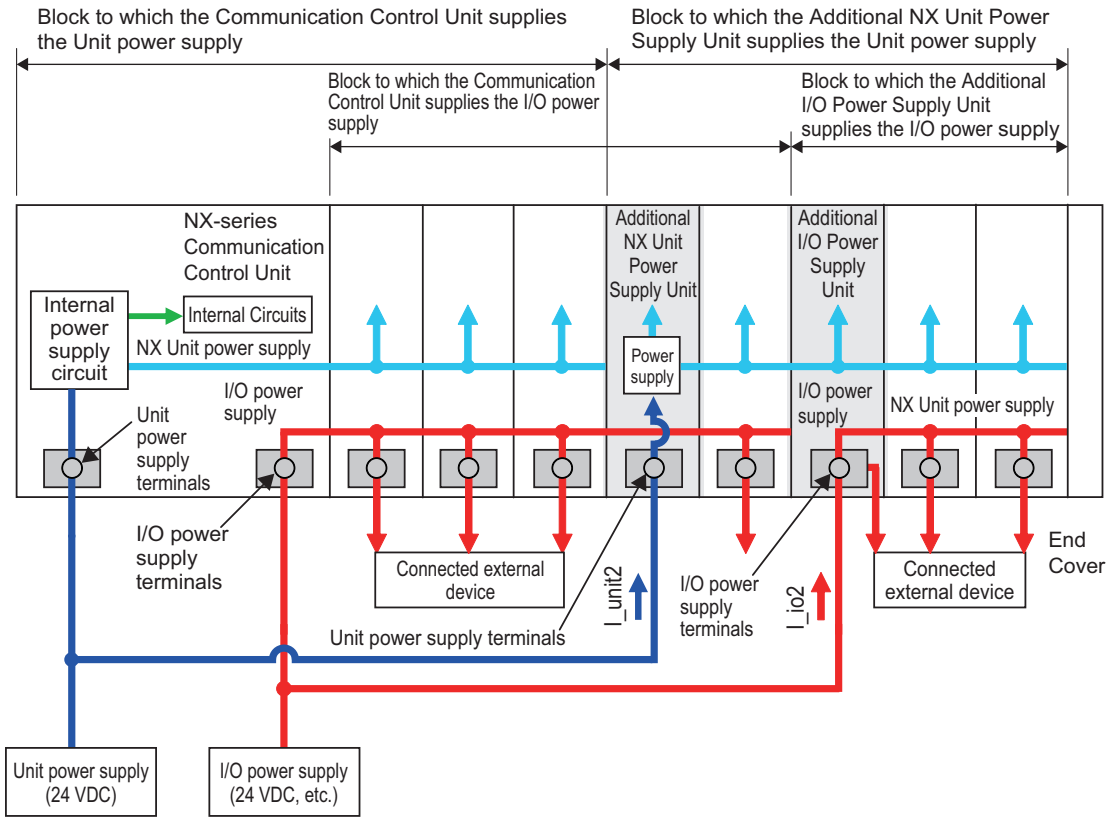
*1. The minimum value is selected among the rated currents of the multiple I/O Power Supply Units connected to the protective device. If, for example, two rated currents of 10 A and 4 A are used, 4 A will be selected.

- When Total Current Consumption for All Blocks Does Not Exceed the Rated Current

  In this example, the current consumption from each power supply is as follows:

  Current consumption from Unit power supply: I_unit1 + I_unit2 ≤ Lowest rated current

  Current consumption from I/O power supply for NX Units: I_io1 + I_io2 ≤ Lowest rated current*1



*1. The minimum value is selected among the rated currents of the multiple I/O power supply units connected to the protective device. If, for example, two rated currents of 10 A and 4 A are used, 4 A will be selected.

5

Installation and Wiring

This section describes how to install and wire the NX-series NX-CSG320 Communication Control Unit as well as details on installation locations.

5-1 Processing at Power ON 5-2
5-1-1 Power ON Operation 5-2
5-1-2 Operation When Resetting the Controller from the Sysmac Studio 5-2

5-2 Mounting Units 5-4
5-2-1 Installation in a Control Panel 5-5
5-2-2 Preparations for Installation 5-9
5-2-3 Installing the Communication Control Unit 5-11
5-2-4 Installing and Connecting NX Units 5-13
5-2-5 Mounting the End Cover 5-17
5-2-6 Mounting the End Plates 5-18
5-2-7 Attaching Markers 5-20
5-2-8 Installing and Removing the SD Memory Card 5-21
5-2-9 Removal of the Communication Control Unit 5-26
5-2-10 Removing NX Units 5-27
5-2-11 Assembled Appearance and Dimensions 5-28

5-3 Wiring 5-32
5-3-1 Wiring the Power Supply 5-33
5-3-2 Wiring the Additional NX Unit Power Supply Unit 5-34
5-3-3 Wiring the Additional I/O Power Supply Unit 5-34
5-3-4 Wiring the Protective Devices 5-34
5-3-5 Grounding 5-35
5-3-6 Connecting the Built-in EtherNet/IP Port 5-39
5-3-7 Wiring to the Screwless Clamping Terminal Blocks 5-46

5-4 Control Panel Installation 5-60
5-4-1 Temperature 5-60
5-4-2 Humidity 5-62
5-4-3 Vibration and Shock 5-62
5-4-4 Atmosphere 5-62
5-4-5 Electrical Environment 5-63
5-4-6 Grounding 5-67

5-1 Processing at Power ON

⚠ WARNING

- Do not disassemble any of the Units. Particularly the Units contain parts with high voltages when power is ON or immediately after power is turned OFF. Electrical shock may occur. There are also sharp internal parts that may cause injury.

5-1-1 Power ON Operation

Precautions for Safe Use

It takes approximately 20 seconds to enter RUN mode after the power supply is turned ON. During that time, digital outputs on the Communication Control Unit will be OFF.

Operation Until Operation Ready Status

Once the Unit power supply to the Unit power supply terminal starts, approximately 20 seconds elapses before the Communication Control Unit enters the operation-ready status. This period is called the *startup* status.
The *startup* time depends on the slave/NX Unit configuration, SD Memory Card usage, SD Memory Card self-diagnosis usage*, etc.
While the Communication Control Unit is in the startup status, the RUN indicator flashes at 0.5 second interval.
* This function performs self-diagnosis on the inserted SD Memory Card. This is executed if the self-diagnosis at startup is enabled in the **Operation Settings** under **Configurations and Setup** − **Controller Setup** in the Sysmac Studio.

The following processing is performed during the *startup* status of the Communication Control Unit.

Process	Description
Self diagnosis at startup	Operation is monitored for the following errors: Power Supply Error, CPU Unit Error, Hardware Initialization Error, and System Initialization Error. *1
Recording Power Turned ON and Power Interrupted events	The Power Turned ON and Power Interrupted events are recorded.

*1. Refer to *15-1-2 Fatal Errors* on page 15-4 for information on the Power Supply Error, CPU Unit Error, Hardware Initialization Error, and System Initialization Error.

5-1-2 Operation When Resetting the Controller from the Sysmac Studio

You can reset the Communication Control Unit from the Sysmac Studio.
A reset from the Sysmac Studio follows the same operation as cycling the power supply of the Unit power.
Confirm the following status before resetting the CPU Unit.

- Check the status of output loads.
- Make sure that SD Memory Card access is not in progress.

5-2 Mounting Units

This section describes how to mount Units to the NX-series Controller.



Precautions for Safe Use

Always turn OFF the power supply to the Controller before attempting any of the following.
- Mounting or removing NX Units or Communication Control Units
- Assembling the Units
- Setting DIP switches or rotary switches
- Connecting cables or wiring the system
- Connecting or disconnecting the terminal blocks or connectors

The built-in power supply of the Controller may continue to supply power after the power supply is turned OFF. The POWER indicator remains lit as long as power is supplied. Make sure that the POWER indicator is not lit before you perform any of the above operations.



Precautions for Correct Use

- Follow the instructions in this manual to correctly perform installation.
- Do not operate or store the Units in the following locations. Doing so may result in burning, in operation stopping, or in malfunction.
  a) Locations subject to direct sunlight
  b) Locations subject to temperatures or humidity outside the range specified in the specifications
  c) Locations subject to condensation as the result of severe changes in temperature
  d) Locations subject to corrosive or flammable gases
  e) Locations subject to dust (especially iron dust) or salts
  f) Locations subject to exposure to water, oil, or chemicals
  g) Locations subject to shock or vibration
- Take appropriate and sufficient countermeasures during installation in the following locations.
  a) Locations near devices that produce strong, high-frequency noise
  b) Locations subject to static electricity or other forms of noise
  c) Locations subject to strong electromagnetic fields
  d) Locations subject to possible exposure to radioactivity
  e) Locations close to power lines

5-2-1 Installation in a Control Panel

Installation in Cabinets or Control Panels

When the NX-series Controller is being installed in a cabinet or control panel, be sure to provide proper ambient conditions as well as access for operation and maintenance.

● Temperature Control

The ambient operating temperature of the NX-series Controller must be within the range of 0 to 55°C. When necessary, take the following steps to maintain the proper temperature.

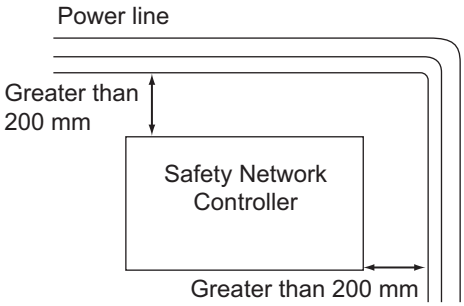
- Provide enough space for good air flow.
- Do not install the Controller above equipment that generates a large amount of heat such as heaters, transformers, or high-capacity resistors.
- If the ambient temperature exceeds 55°C, install a cooling fan or air conditioner.

● Accessibility for Operation and Maintenance

- To ensure safe access for operation and maintenance, separate the Controller as much as possible from high-voltage equipment and power machinery.
- It will be easy to operate the Controller if it is mounted at a height of 1.0 to 1.6 m above the floor.

● Improving Noise Resistance

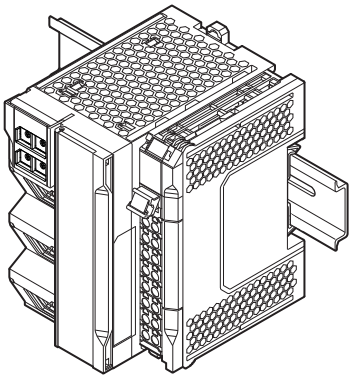
- Do not mount the Controller in a control panel containing high-voltage equipment.
- Install the Controller at least 200 mm away from power lines.



- Ground the mounting plate between the Controller and the mounting surface.

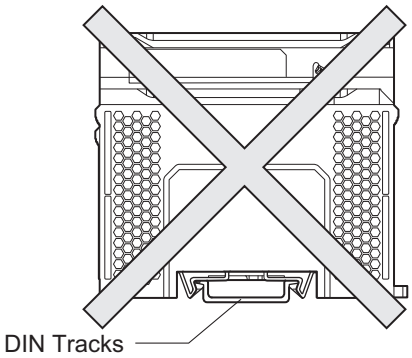
● Controller Orientation

- Each Rack must be mounted in the following position to provide proper cooling. This position is called an upright position.

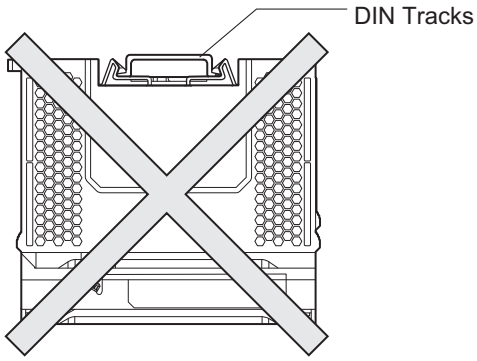


- Do not install a Rack in any of the following positions.

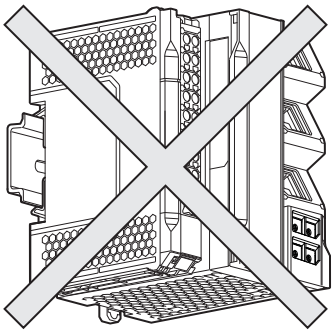
Place DIN Track downward



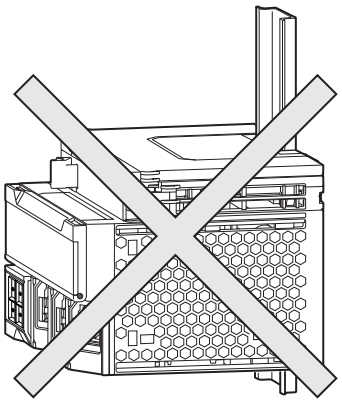
Place DIN Track upward



Place it upside down



Place DIN Track vertically



Installation Method in Control Panels

An NX-series Controller must be mounted inside a control panel on DIN Track.

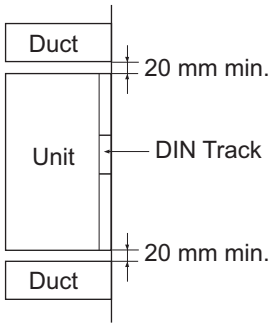
- Consider the width of wiring ducts, wiring, ventilation, and Unit replacement when determining the space between the CPU Rack and other devices.

Additional Information

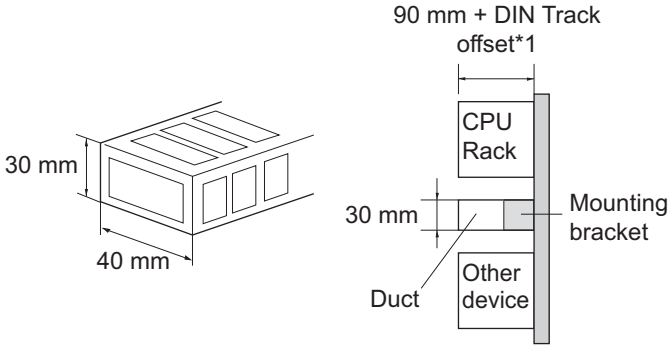
A Controller must be mounted on DIN Track.
It cannot be mounted with screws.

Wiring Ducts

Whenever possible, route I/O wiring through wiring ducts.
Install mounting bracket so that it is easy to fish wire through the duct. It is handy to have the duct at the same height as the CPU Rack.



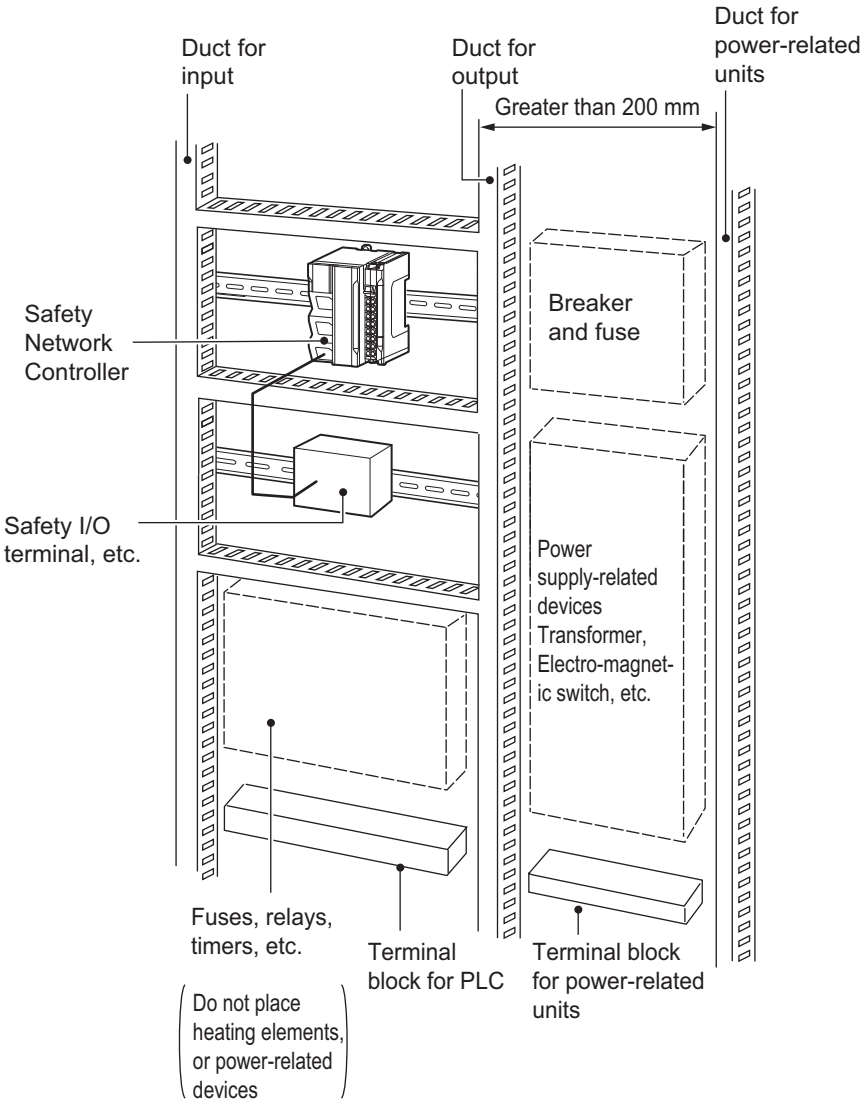
Wiring Duct Example



*1. It varies depending on the DIN Track to be used. Refer to *Installation Dimensions* on page 5-28 under *5-2-11 Assembled Appearance and Dimensions* on page 5-28 for details. It corresponds to the dimension (B).

● Routing Wiring Ducts

Install the wiring ducts at least 20 mm away from the tops of the Rack and any other objects (e.g., ceiling, wiring ducts, structural supports, devices, etc.) to provide enough space for air circulation and replacement of Units.



5-2-2 Preparations for Installation

We recommend using the following products to install the Unit on a DIN Track.

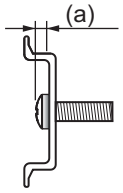
Name	Model	Manufacturer	Remarks
35-mm DIN Track	PFP-50N	OMRON Corporation	• Length: 50 cm • Material: Aluminum • Surface treatment: Insulated
	PFP-100N	OMRON Corporation	• Length: 100 cm • Material: Aluminum • Surface treatment: Insulated
	NS 35/ 7,5 PERF	Phoenix Contact	• Length: 75.5, 95.5, 115.5, or 200 cm • Material: Steel • Surface treatment: Conductive
	NS 35/ 15 PERF	Phoenix Contact	• Length: 75.5, 95.5, 115.5, or 200 cm • Material: Steel • Surface treatment: Conductive
End Plate	PFP-M	OMRON Corporation	Two End Plates are required for each CPU Rack.
	CLIPFIX 35	Phoenix Contact	Two End Plates are required for each CPU Rack.

Not all of the combinations of the DIN Tracks and End Plates listed above are possible.
Confirm applicability of the combinations in the following table.

DIN Track model	PFP-M (OMRON)	CLIPFIX 35 (Phoenix Contact)
PFP-50N	Possible	Possible
PFP-100N	Possible	Possible
NS 35/ 7,5 PERF	Possible	Possible
NS 35/ 15 PERF	Not possible	Possible

Also, use screws and washers of the following sizes to fix the DIN Tracks.

(a): Dimensions from the screw head to the fastening surface

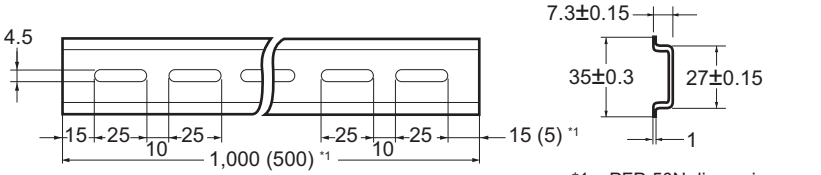


DIN Track model	Applicable screw size	(a)
PFP-50N	M4	4.1 mm max.
NS 35/ 7,5 PERF	M6	4.6 mm max.
NS 35/ 15 PERF	M6	10 mm max.

If you use any DIN Track other than those listed in the table above, refer to the dimensions shown in *5-2-11 Assembled Appearance and Dimensions* on page 5-28 and use proper screws and washers.

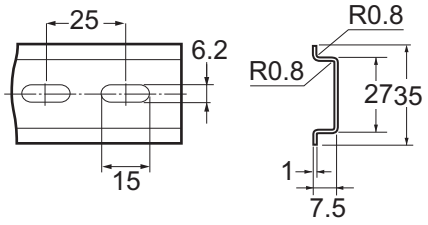
● DIN Tracks

PFP-100N/50N DIN Track

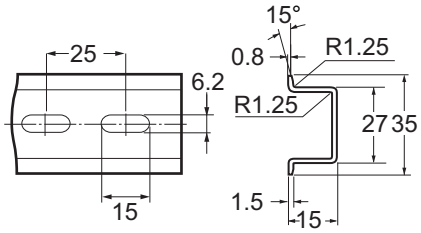


*1. PFP-50N dimensions are given in parentheses.

NS 35/ 7,5 PERF

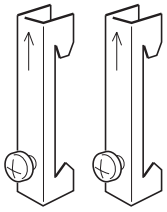


NS 35/ 15 PERF

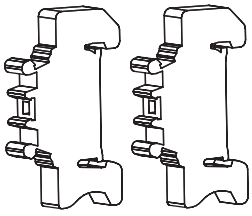


● End Plate

PFP-M (Two)



CLIPFIX 35 (Two)

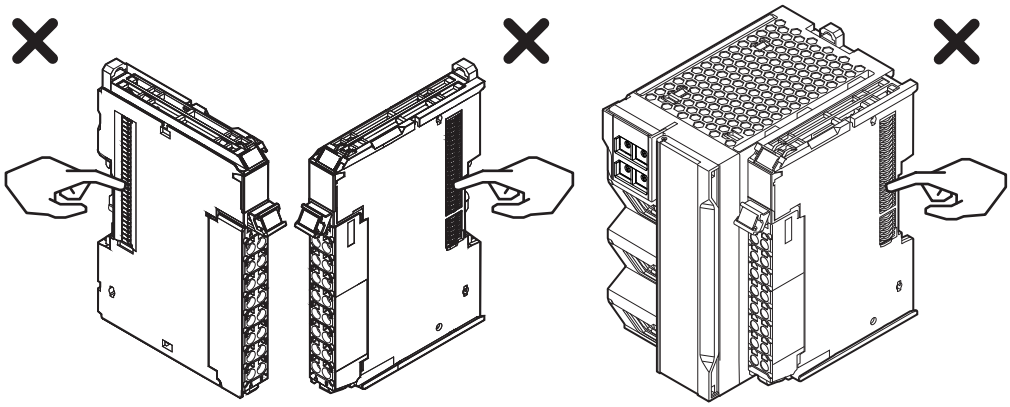


5-2-3 Installing the Communication Control Unit

This section describes how to install the Communication Control Unit.

Precautions for Safe Use

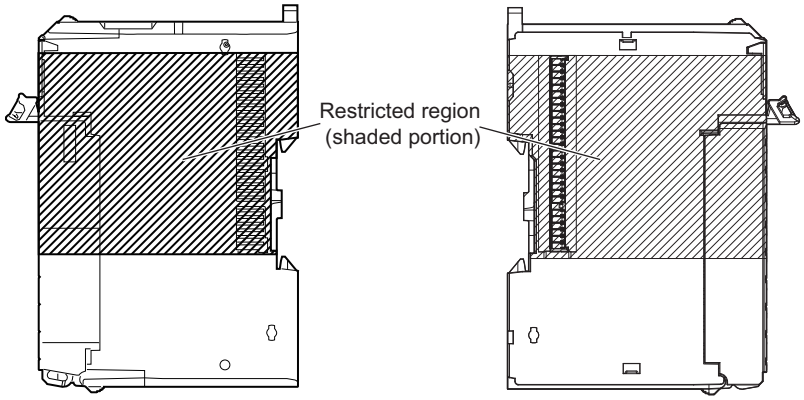
- Do not apply labels or tape to the Unit. When the Units are installed or removed, adhesive or scraps may adhere to the pins in the NX bus connector, which may result in malfunctions.
- Do not touch the pins in the NX bus connector on the Unit. Dirt may adhere to the pins in the NX bus connector, which may result in malfunctions.



Example: NX Units (12 mm wide)

Communication Control Unit

- Do not write on the Communication Control Unit or an NX Unit with ink within the restricted region that is shown in the following figure. Also do not get this area dirty. When the Unit is installed or removed, ink or dirt may adhere to the pins in the NX bus connector, which may result in malfunctions in the Controller.



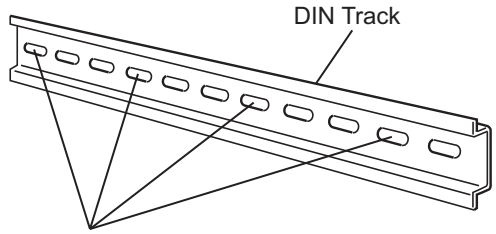
Precautions for Correct Use

- When you install the Unit, be careful not to touch or bump the pins in the NX bus connector.
- When you handle the Unit, be careful not to apply stress to the pins in the NX bus connector. If the Unit is installed and the power supply is turned ON when the pins in the connector are deformed, contact failure may cause malfunctions.

1 Install the DIN Track.

• Using a PFP-50N/100N DIN Track

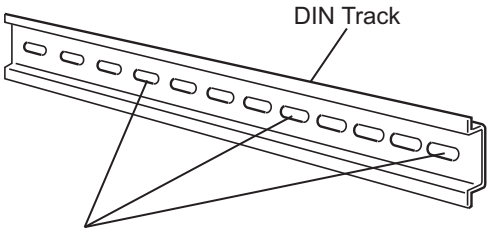
Use one M4 screw for each three holes in the DIN Track. There must be a screw for each interval of 105 mm or less. The screw tightening torque is 1.2 N·m.



Use one screw for each three holes.

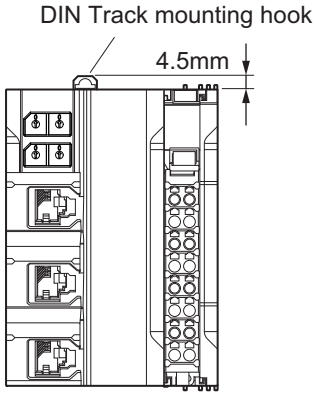
• Using an NS 35/7,5 PERF or NS 35/15 PERF DIN Track

Use one M6 screw for each four holes in the DIN Track. There must be a screw for each interval of 100 mm or less. The screw tightening torque is 5.2 N·m.

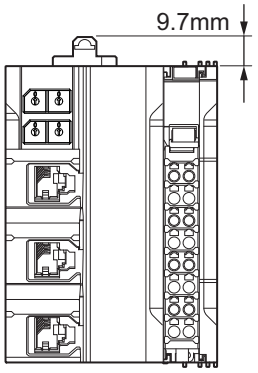


Use one screw for each four holes.

2 Make sure that the DIN Track mounting hook on the Communication Control Unit is in the locked position.



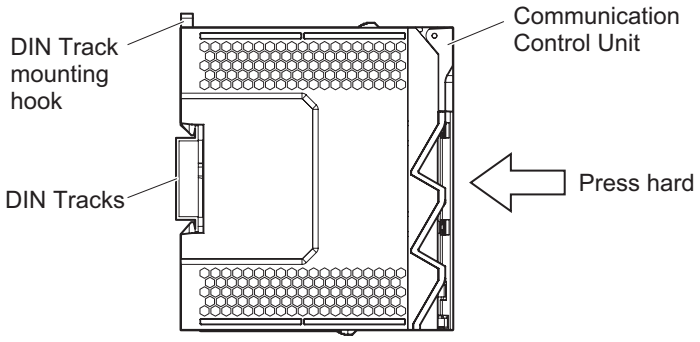
Locked position of DIN Track mounting hook



Unlocked position of DIN Track mounting hook

If the DIN Track mounting hook is pressed down, it is in the locked position.
If the DIN Track mounting hook is pulled up, it is in the unlocked position.
If it is in the unlocked position, press down the DIN Track mounting hook to place it to the locked position.

3 Press the Communication Control Unit with a certain amount of force against the DIN Track until you hear the DIN Track mounting hook lock into place.
After you mount the Communication Control Unit, make sure that it is securely mounted on the DIN Track.



Additional Information

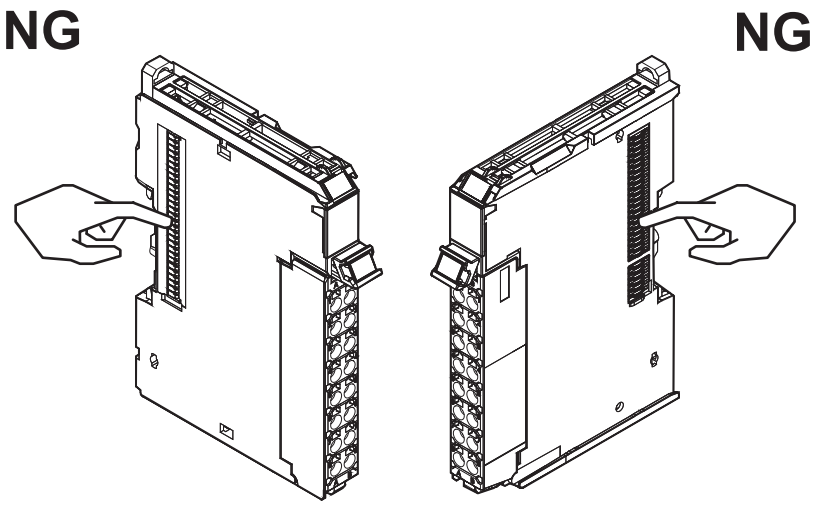
It is not normally necessary to unlock the DIN Track mounting hook when you mount the unit. However, if you mount the unit on a DIN Track that is not one of the recommended DIN Tracks, the DIN Track mounting hook may not lock properly. If that happens, first unlock the DIN track mounting hook, mount the unit to the DIN Track, then lock the DIN track mounting hook.

5-2-4 Installing and Connecting NX Units

This section describes how to mount NX Units to the Communication Control Unit and how to connect NX Units to each other.

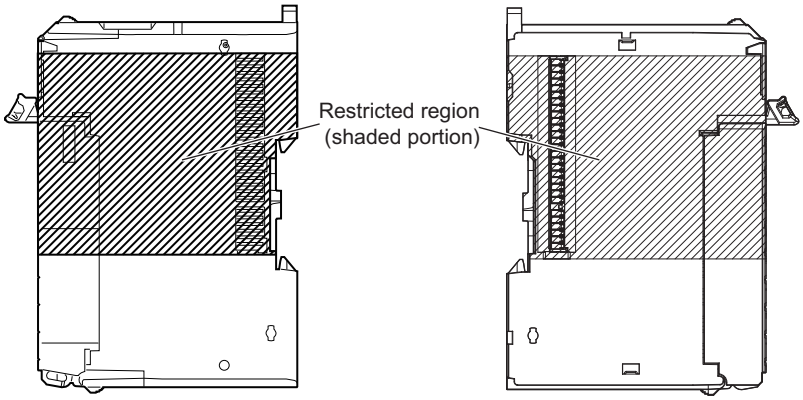
Precautions for Safe Use

- Always turn OFF the power supply before mounting the Units. If the power supply is not OFF, the Unit may result in malfunction or may be damaged.
- Do not apply labels or tape to the Unit. When the Unit is installed or removed, adhesive or scraps may adhere to the pins in the NX bus connector, which may result in malfunctions.
- Do not touch the pins in the NX bus connector on the Unit. Dirt may adhere to the pins in the NX bus connector, which may result in malfunctions.



Example: NX Unit (12 mm width)

- Do not write on an NX Unit with ink within the restricted region that is shown in the following figure. Also do not get this area dirty. When the Unit is installed or removed, ink or dirt may adhere to the pins in the NX bus connector, which may result in malfunctions in the CPU Rack.



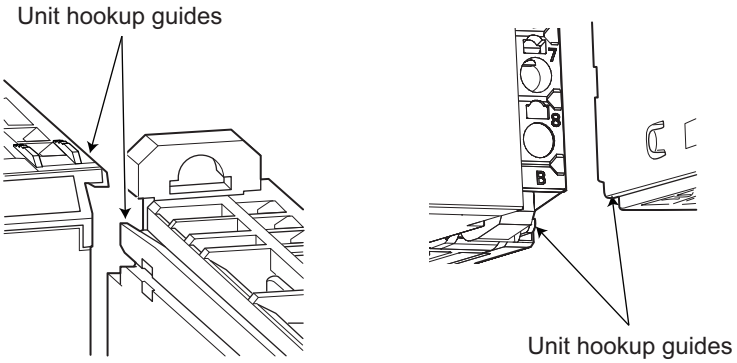
Precautions for Correct Use

- When you mount an NX Unit to the Communication Control Unit or when you connect NX Units to each other, always mount the Units one at a time on the DIN Track.
  If you connect NX Units to each other and attempt to mount them together to the DIN Track at the same time, the Units may separate from each other and fall.
- When you handle a Unit, be careful not to apply stress to the pins in the NX bus connector.
  If the Unit is installed and the power supply is turned ON when the pins in the NX bus connector are deformed, contact failure may cause malfunctions.
- When you handle a Unit, be careful not to touch or bump the pins in the NX bus connector.

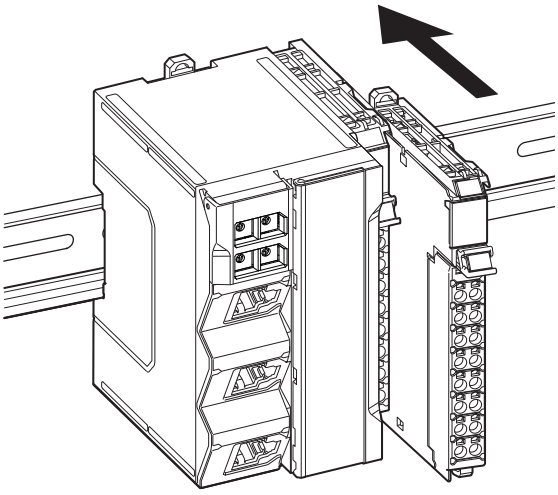
● Mounting an NX Unit to the Communication Control Unit

Mount the NX Unit to the Communication Control Unit after removing the End Cover.

1 From the front of the Communication Control Unit, engage the Unit hookup guides on the NX Unit with the Unit hookup guides on the Communication Control Unit.



2 Slide the NX Unit on the hookup guides.



3 Press the NX Unit with a certain amount of force against the DIN Track until you hear the DIN Track mounting hook lock into place.

When you mount the NX Unit, it is not necessary to release the DIN Track mounting hook on the NX Unit. After you mount the NX Unit, make sure that it is locked to the DIN Track.

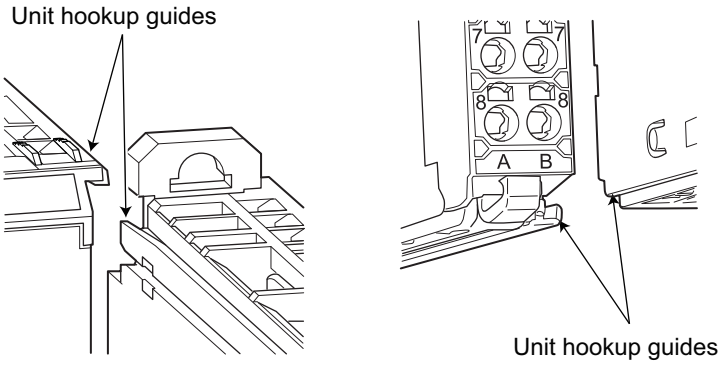
Additional Information

It is not normally necessary to unlock the DIN Track mounting hook when you mount the NX Unit. However, if you mount the NX Unit on a DIN Track that is not one of the recommended DIN Tracks, the DIN Track mounting hook may not lock properly. If that happens, unlock the DIN Track mounting hook at the start of the procedure, mount the NX Unit to the DIN Track, and then lock the DIN Track mounting hook.

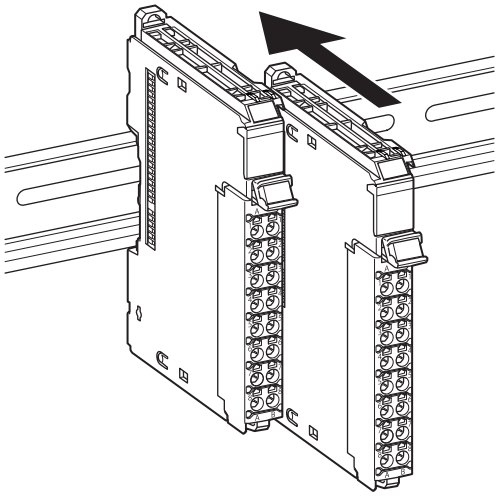
● Mounting NX Units to Each Other

Use the following procedure to mount NX Units to each other.

1 From the front of the previously mounted NX Unit, engage the Unit hookup guides on a new Unit with the Unit hookup guides on the previously mounted NX Unit.



2 Slide the NX Unit on the hookup guides.



3 Press the NX Unit with a certain amount of force against the DIN Track until you hear the DIN Track mounting hook lock into place.

When you mount the NX Unit, it is not necessary to release the DIN Track mounting hook on the NX Unit.

After you mount the NX Unit, make sure that it is locked to the DIN Track.

Additional Information

It is not normally necessary to unlock the DIN Track mounting hook when you mount the NX Unit. However, if you mount the NX Unit on a DIN Track that is not one of the recommended DIN Tracks, the DIN Track mounting hook may not lock properly. If that happens, unlock the DIN Track mounting hook at the start of the procedure, mount the NX Unit to the DIN Track, and then lock the DIN Track mounting hook.

5-2-5 Mounting the End Cover

Always mount the End Cover (NX-END02) provided with the product to the end of the CPU Rack.

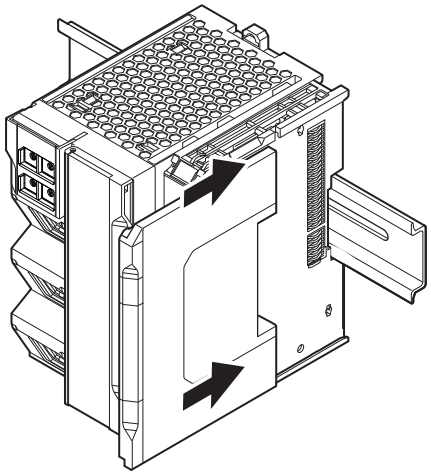
Precautions for Safe Use

The End Cover has a metal portion and is heavier than it looks. Be careful not to drop it when handling.

Precautions for Correct Use

Always mount an End Cover to the end of the CPU Rack to protect the last Unit on the CPU Rack. Not mounting the End Cover may result in malfunction or failure of the Units.

1 From the front of the rightmost Unit, slide the End Cover along the Unit hookup guides on the rightmost Unit on the CPU Rack.



2 Press the End Cover firmly against the DIN Track until you hear it lock into place on the DIN Track.

After you mount the End Cover, make sure that it is securely mounted on the DIN Track.

5-2-6 Mounting the End Plates

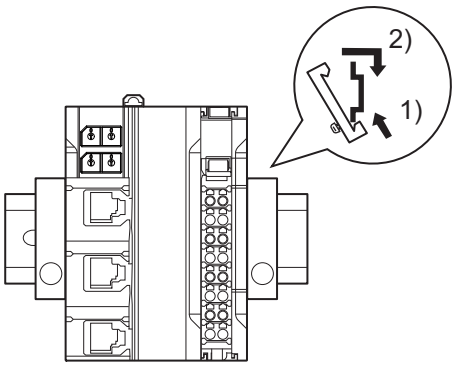
After you mount the End Cover, always secure the Unit with End Plates at both sides.

Precautions for Correct Use

After you mount the Unit on the DIN Track, always secure it with End Plates at both sides. If you do not secure it, the Unit may be damaged or malfunction.

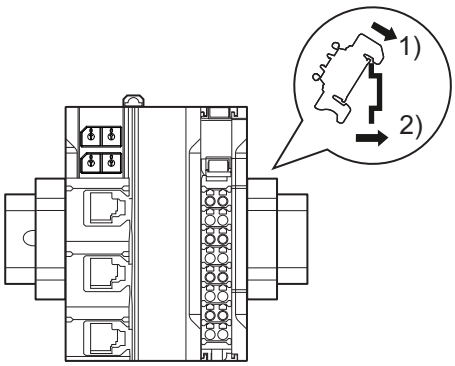
● Using PFP-M (OMRON)

To mount an End Plate, 1) hook the bottom of it on the bottom of the DIN Track and 2) rotate the End Plate to hook the top of it on the top of the DIN Track.
Then tighten the screw to lock the End Plate in place.

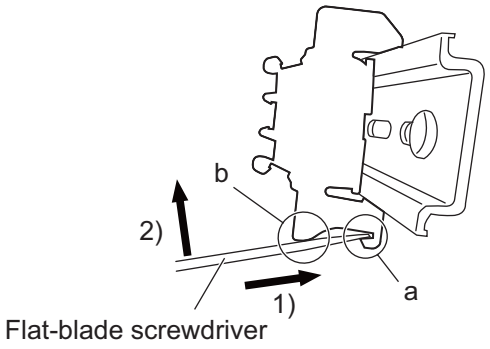


● Using CLIPFIX 35 (Phoenix Contact)

To mount an End Plate, 1) hook the top of it on the top of the DIN Track and 2) rotate the Plate to hook the bottom of it on the bottom of the DIN Track. Press in until you hear the End Plate lock into place.

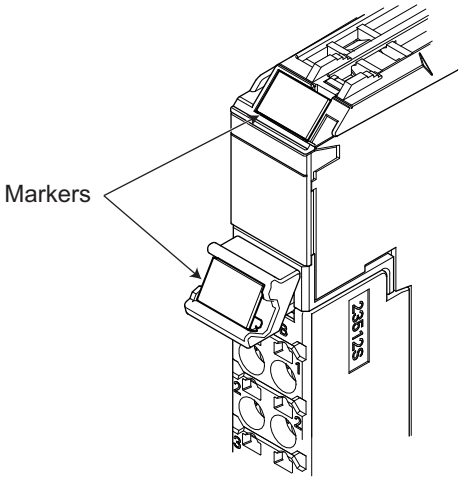


To remove an End Plate 1) insert the tip of a flat-blade screwdriver into groove “a” and 2) use “b” as a fulcrum and lift the end of the screwdriver, as shown in the following diagram.


b
2)
a
1)
Flat-blade screwdriver

5-2-7 Attaching Markers

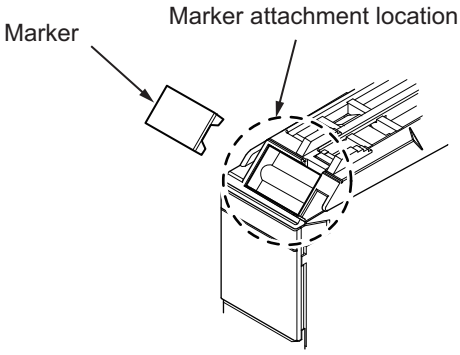
Markers can be attached to NX Units and their terminal blocks to identify them.
The plastic markers made by OMRON are installed for the factory setting. The ID information can be written on them.
Commercially available markers can also be installed.
Replace the markers made by OMRON if you use commercially available markers now.



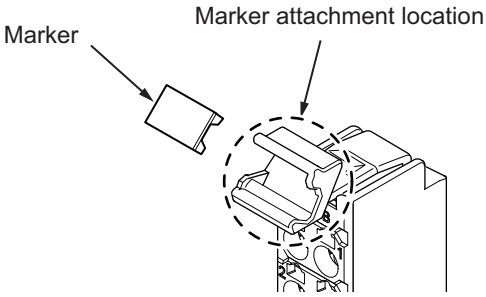
The marker attachment locations on the NX Units depend on the type of external connection terminals. Refer to the user's manual for the NX Units that you will use for the marker attachment locations.

● Installation Method

Insert the protrusions on the markers into the marker attachment locations on the NX Units and terminal blocks on NX Units.



<Unit>



<Terminal block>

● Commercially Available Markers

Commercially available markers are made of plastic and can be printed on with a special printer.
To use commercially available markers, purchase the following products.

Product name	Model number	
	Manufactured by Phoenix Contact	Manufactured by Weidmuller
Markers	UC1-TMF8	DEK 5/8
Special marker printer	UM EN BLUEMARK X1	PrintJet PRO

The markers made by OMRON cannot be printed on with commercially available special printers.

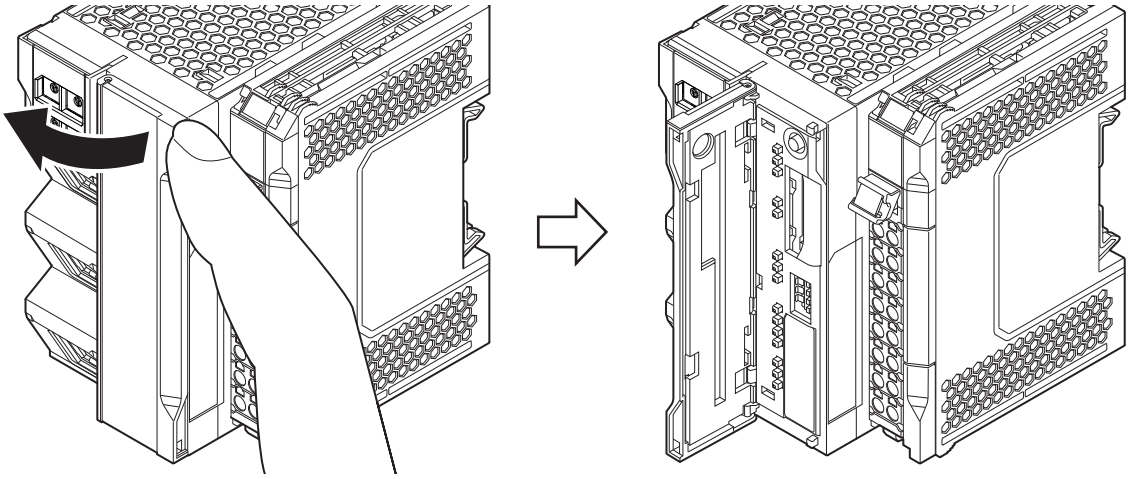
5-2-8 Installing and Removing the SD Memory Card

Before Using an SD Memory Card

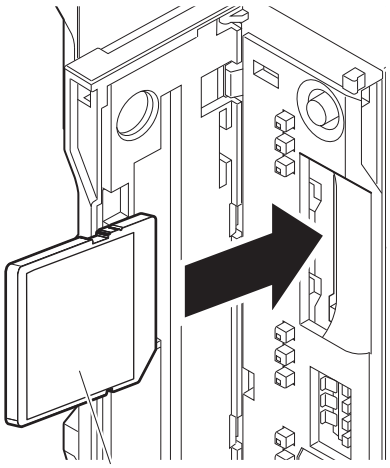
- Keep the following precautions because an SD Memory Card may become unusable.
  a) Do not turn OFF the power supply to the Controller while the SD BUSY indicator is lit (i.e., while SD Memory Card access is in progress).
     The SD BUSY indicator is lit when the SD Memory Card is accessed from the user program or from a computer through FTP.
  b) Do not remove the SD Memory Card while the SD BUSY indicator is lit or the SD PWR indicator is lit (i.e., while SD Memory Card power is supplied).
     Press the SD Memory Card power supply switch and confirm that the SD BUSY indicator or SD PWR indicator is not lit before you remove the SD Memory Card.
- Never insert the SD Memory Card facing the wrong way.
  If the SD Memory Card is inserted forcibly, it may become unusable.
- To format the SD Memory Card (e.g., to delete all of the data), insert the SD Memory Card in the Communication Control Unit and perform the operation from the Sysmac Studio.
- The SD Memory Card uses flash memory, and so its service life is limited. When the end of the SD Memory Card's service life approaches, the ability to write data is lost, and data is sometimes not retained after writing. The service life depends on the size of the data that is written and on the ambient temperature. For the unlikely event that data is lost, it is recommended to periodically back up data.
- The service life may be extremely short if a non-OMRON SD Memory Card is used. Also, operation may be affected due to deterioration in writing performance.
- If you use an OMRON SD Memory Card, the end of the life of the SD Memory Card can be detected in the following ways.
  a) *_Card1Deteriorated* (SD Memory Card Life Warning Flag) system-defined variable
  b) *SD Memory Card Life Exceeded* event in the event log
- You can use the SD memory card life expiration detection function on some specific SD Memory Cards. Refer to *Specifications of Supported SD Memory Cards, Folders, and Files* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for details.

Installing the SD Memory Card

1 Place your finger on the upper side panel of the memory card cover located in the middle of the Communication Control Unit and open it to the left.

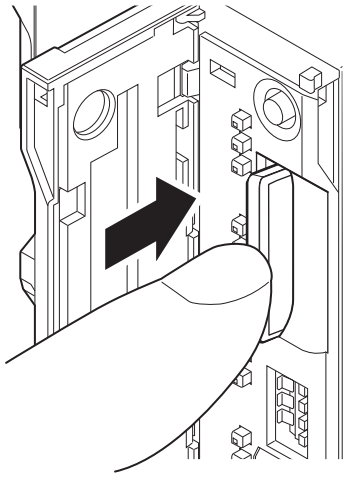


2 Insert the SD Memory Card with the label facing to the right.
Insert the SD Memory Card with the label facing the right side of the Communication Control Unit.



Label

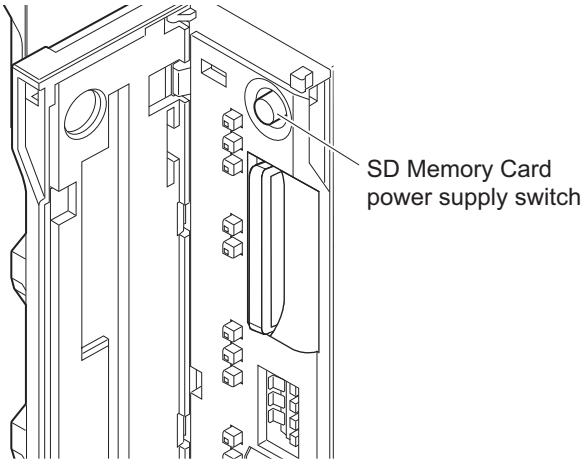
3 Push the SD Memory Card securely into the compartment.



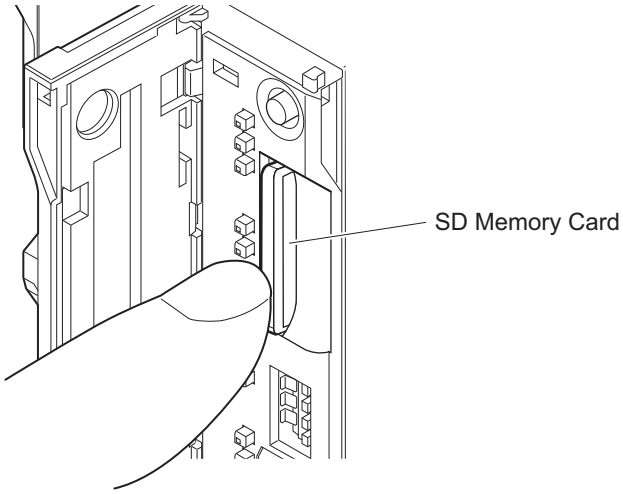
4 Close the Memory Card cover.

Removing the SD Memory Card

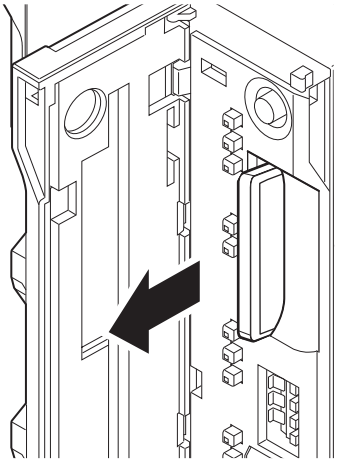
1 Press the SD Memory Card power supply switch.



2 Press the SD Memory Card after you confirm that the SD BUSY indicator (lit while SD Memory Card access is in progress) and SD PWR indicator (lit while SD Memory Card power is supplied) are no longer lit.



The SD Memory Card will be ejected from the compartment.



3 Pull out the SD Memory Card.

4 Close the Memory Card cover.

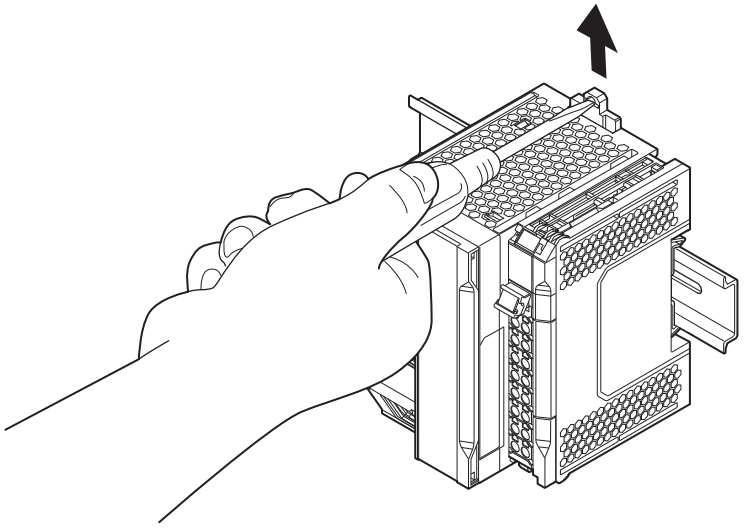
5-2-9 Removal of the Communication Control Unit

This section describes how to remove the Communication Control Unit.
If an NX Unit is mounted, remove the CPU Unit after removing the NX Unit next to the CPU Unit. Refer to *5-2-10 Removing NX Units* on page 5-27 for details on how to remove the NX Units.

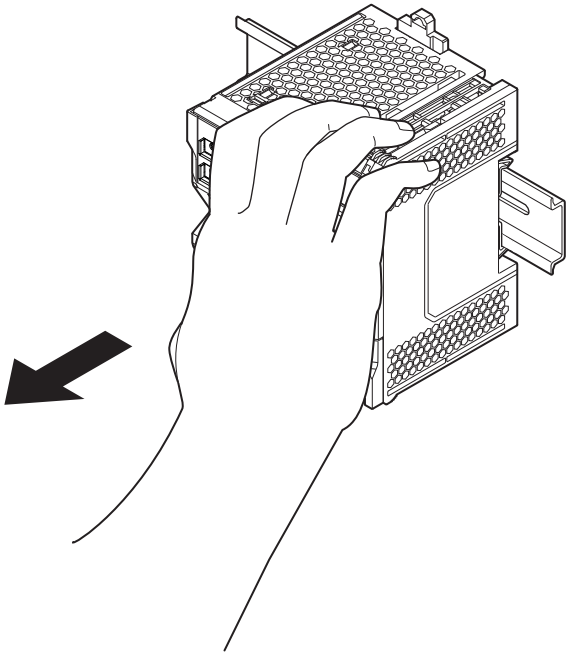
Precautions for Correct Use

When you remove a Unit, be careful not to touch or bump the pins in the NX bus connector.

1 Unlock the DIN Track mounting hook.
Use a flat-blade screwdriver to pull up the DIN Track mounting hook to unlocked position.
At this point, be sure not to drop the Communication Control Unit.



2 Remove the Communication Control Unit from the DIN Track.
Pull the Unit straight forward to remove. Be careful not to drop it.

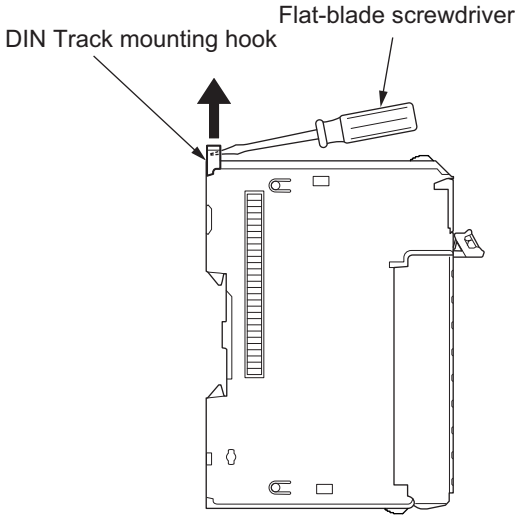


5-2-10 Removing NX Units

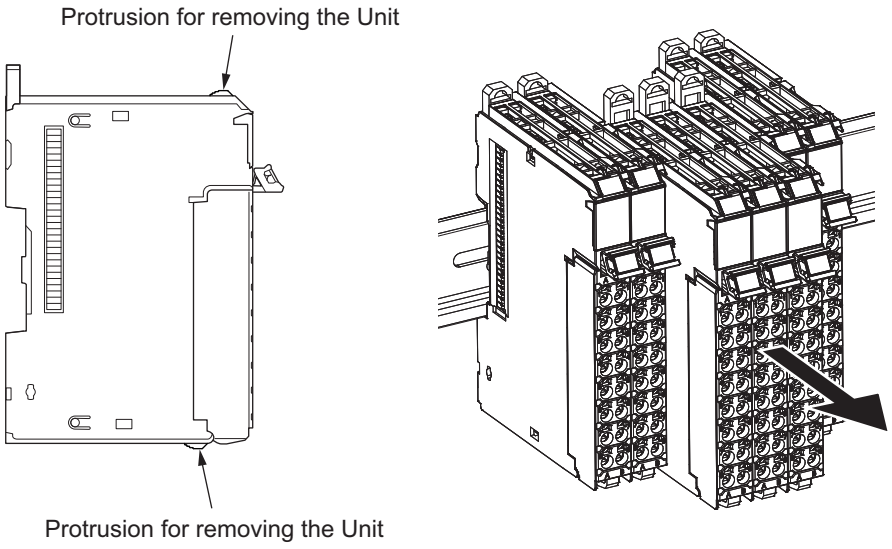
Precautions for Safe Use

Always turn OFF the Unit power supply and I/O power supply before you remove the NX Unit.

1 Use a flat-blade screwdriver to pull up the DIN Track mounting hook on the Unit to remove.



2 Put your fingers on the protrusions for removing multiple NX Units including the Unit to be removed, then pull out straight forward to remove.

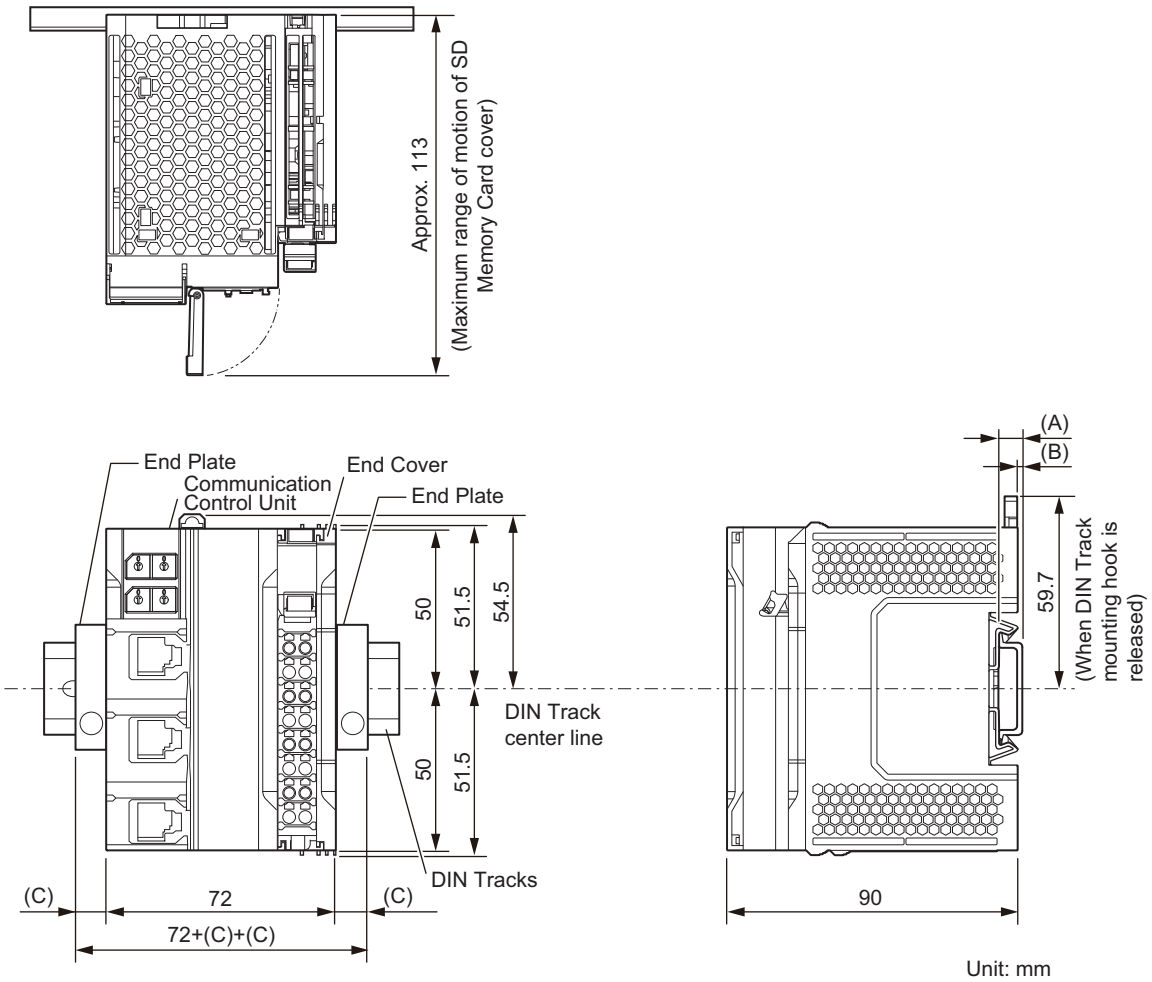


Precautions for Correct Use

- When removing an NX Unit, remove multiple Units together which include the one you want to remove. If you attempt to remove only one Unit, it is stuck and hard to pull out.
- Do not unlock the DIN Track mounting hooks on all of the NX Units at the same time. If you unlock the DIN Track mounting hooks on all of the NX Units at the same time, all of the Units may come off.
- When you remove a Unit, be careful not to touch or bump the pins in the NX bus connector.

5-2-11 Assembled Appearance and Dimensions

Installation Dimensions



- Unit width

Model	Unit width [mm]
NX-CSG□□□	72

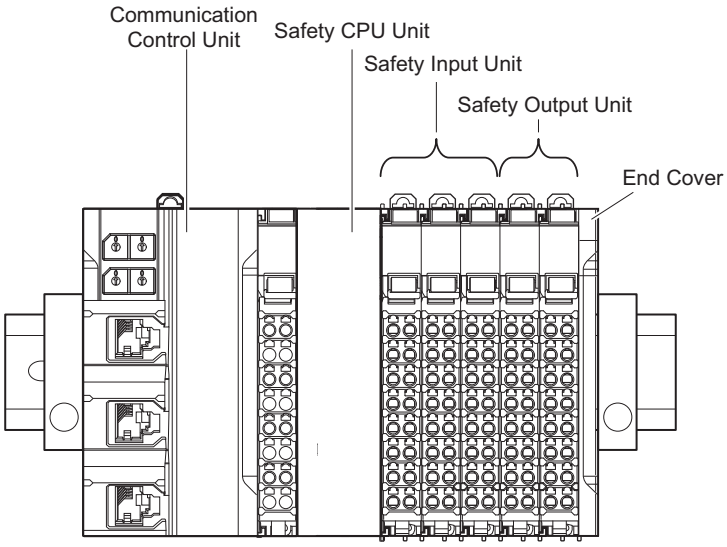
- DIN Track dimension

DIN Track model	(A) DIN Track dimension	(B) Dimension from the back of the Unit to the back of the DIN Track
PFP-100N	7.3 mm	1.5 mm
PFP-50N	7.3 mm	1.5 mm
NS 35/7,5 PERF	7.5 mm	1.7 mm
NS 35/15 PERF	15 mm	9.2 mm

- End Plate dimension

End Plate model	(C) End Plate dimension
PFP-M	10 mm
CLIPFIX 35	9.5 mm

● Calculation Example of CPU Rack Configuration Width

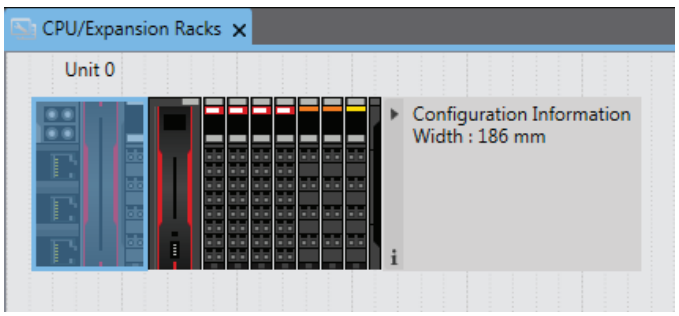


The widths of the Units in the example CPU Rack configuration and the total configuration width are given below.

Unit name	Model	Unit width	Qty	Subtotal unit width
Communication Control Unit	NX-CSG□□□	72 mm	1	72 mm
Safety CPU Unit	NX-SL5700	30 mm	1	30 mm
Safety Input Unit	NX-SID800	12 mm	3	36 mm
Safety Output Unit	NX-SOD400	12 mm	2	24 mm
Total (W =)				162 mm

Additional Information

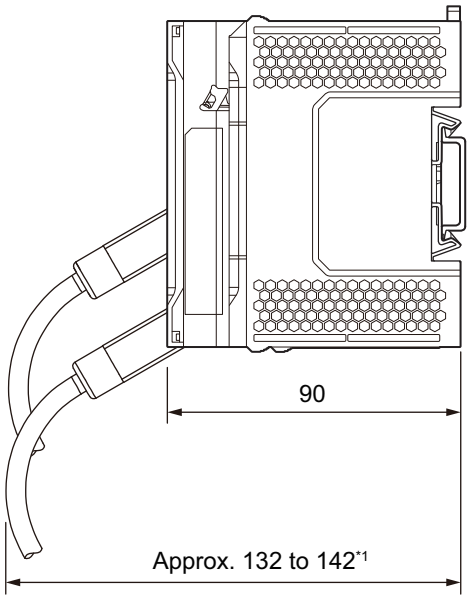
You can check the width of the CPU Rack when you create the Unit configuration on the **CPU and Expansion Racks** Tab Page on the Sysmac Studio. On the **CPU and Expansion Racks** Tab Page on the Sysmac Studio, click on the right end of the CPU Rack to display the width.



Installation Height

The installation height of the CPU Rack depends on the model of DIN Track and on the models of NX Units that are mounted.
Also, additional space is required for the cables that are connected to the Unit. Allow sufficient depth in the control panel and allow extra space when you mount the CPU Rack.

The following figure shows the dimensions from the cables connected to the CPU Rack to the back of the Unit. The unit of dimension is millimeter.
The height from the mounting surface of the DIN Track varies depending on the DIN Track to be used. Refer to *Installation Dimensions* on page 5-28 for the height of individual DIN Track type.



Unit: mm

*1. This is the dimension from the back of the Unit to the communications cables.
Approx. 132 mm: When MPS588-C connector is used
Approx. 142 mm: When XS6G-T421-1 connector is used

Precautions for Safe Use

Do not pull on the cables or bend the cables beyond their natural limit.
Doing so may break the cables.

5-3 Wiring

⚠ WARNING

- Make sure that the voltages and currents that are input to the slaves and Units are within the specified ranges.
  Inputting voltages or currents that are outside of the specified ranges may cause accidents or fire.



⚠ CAUTION

- Be sure that all terminal screws and cable connector screws are tightened to the torque specified in the relevant manuals. Loose screws may result in fire or malfunction.
- Do not touch any Unit when power is being supplied or immediately after the power supply is turned OFF. Doing so may result in burn injury.





Precautions for Safe Use

Use the methods that are specified in this manual for wiring the terminal blocks.

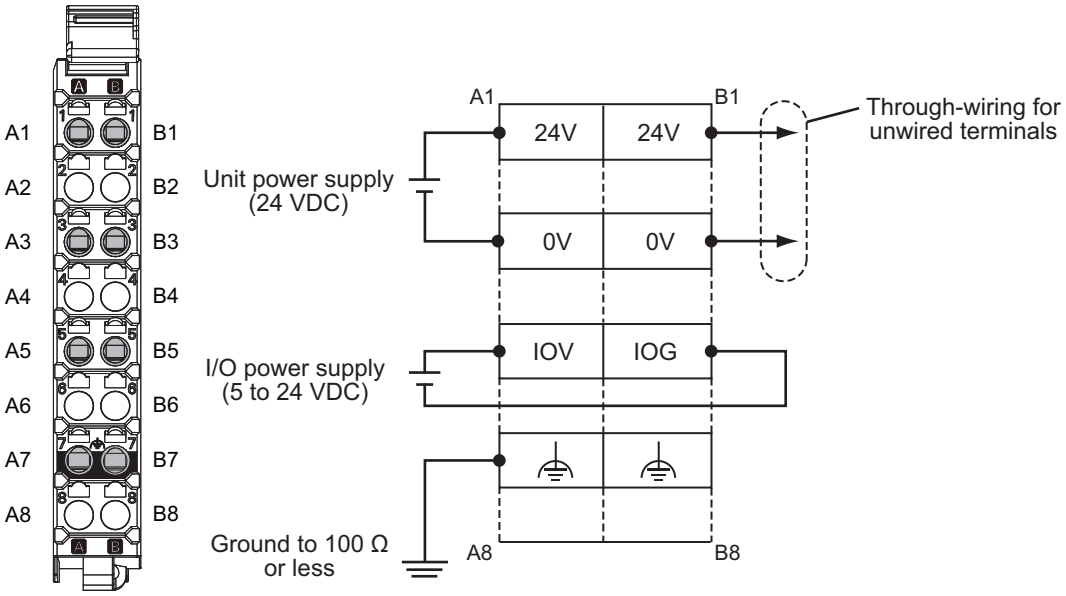


Precautions for Correct Use

Do not allow wire clippings, shavings, or other foreign material to enter any Unit. Otherwise, Unit burning, failure, or malfunction may occur. Cover the Units or take other suitable countermeasures, especially during wiring work.

5-3-1 Wiring the Power Supply

This section describes the wiring of the power supply to the power supply terminals on the Communication Control Unit.



● Unit Power Supply Terminals

These terminals are connected to the Unit power supply. The details are given in the following table.

Terminal number	Terminal name	Description
A1 or B1	UV	Connect the 24 VDC wire (positive side) from the Unit power supply to either the A1 or B1 terminal.
A3 or B3	UG	Connect the 0 VDC wire (negative side) from the Unit power supply to either the A3 or B3 terminal.

You can use the unwired terminals for through-wiring to the Unit power supply terminals on an Additional NX Unit Power Supply Unit. Make the current supplied from the unwired terminals meet the following condition.

Current supplied from unwired terminals ≤ Current capacity of power supply terminals − Current consumption from other blocks

Refer to *4-4-1 Selecting the Unit Power Supply* on page 4-20 for details on blocks.

Connect the DC power supply to the Unit power supply terminals.

Terminal number	Terminal name	Description
A1 or B1	24 V	Connect the 24 VDC wire (positive side) from the Unit power supply to either the A1 or B1 terminal.
A3 or B3	0 V	Connect the 0 VDC wire (negative side) from the Unit power supply to either the A3 or B3 terminal.

The 24 V terminals and the 0 V terminals are internally connected to each other.

You can use the unwired terminals for through-wiring to an Additional NX Unit Power Supply Unit or to the Unit power supply terminals on another Communication Control Unit.
When you supply the Unit power through the unwired terminals, be careful not to exceed 4 A, the current capacity of power supply terminals.

● I/O Power Supply Terminals

These terminals are connected to the I/O power supply. The details are given in the following table.

Terminal number indications	Terminal name	Description
A5	IOV	Connect the 5 to 24 VDC wire (positive side) from the I/O power supply.
B5	IOG	Connect the 0 VDC wire (negative side) from the I/O power supply.

Provide an I/O power supply voltage that is within the voltage specifications of the NX Unit I/O circuits and the connected external devices.

5-3-2 Wiring the Additional NX Unit Power Supply Unit

For information on wiring the Additional NX Unit Power Supply Unit, refer to the *NX-series System Units User's Manual* (Cat. No. W523-E1-05 or later).

5-3-3 Wiring the Additional I/O Power Supply Unit

For information on wiring the Additional I/O Power Supply Unit, refer to the *NX-series System Units User's Manual* (Cat. No. W523-E1-05 or later).

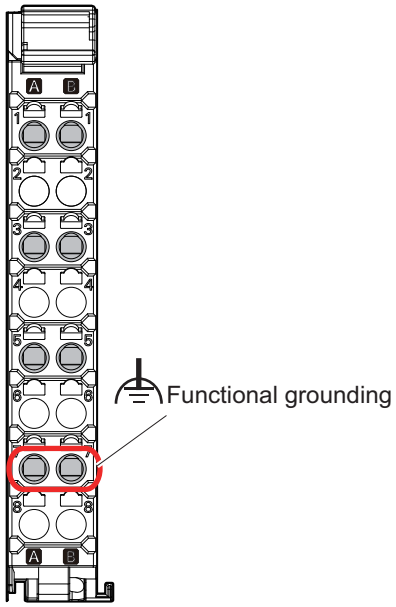
5-3-4 Wiring the Protective Devices

For information on wiring the protective devices to protect against short circuits and overcurrents of external circuits, refer to *4-4-3 Selecting Protective Devices* on page 4-23.

5-3-5 Grounding

This section describes how to ground the CPU Rack.

Units with Ground Terminals and Type of Ground Terminals



Communication Control Unit,
NX Unit

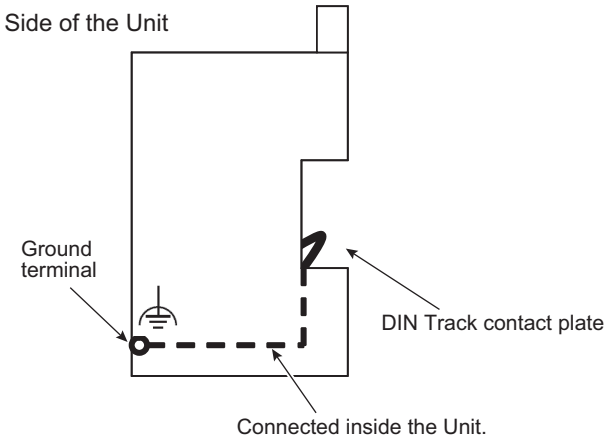
● Units with Ground Terminals

- Communication Control Unit
- Additional NX Unit Power Supply Unit
- Shield Connection Unit

Grounding type	Symbol	Function
A7, B7		Functional grounding is done to protect device and system functions, including prevention of noise from external sources, or prevention of noise from devices or equipment that could have harmful effects on other devices or equipment.

DIN Track Contact Plates

A Unit that has a ground terminal also has a DIN Track contact plate on the back of the Unit.
The DIN Track contact plate is connected internally to the ground terminal on the Unit.
This means that the ground terminal will be electrically connected to the DIN Track.


Side of the Unit
Ground terminal
DIN Track contact plate
Connected inside the Unit.

Grounding the CPU Rack

This section describes how to ground the ground terminals on the CPU Rack.
The functional ground terminals that are provided on some Units and the DIN Track are grounded.

- Using a dedicated ground wire, ground the ground terminals and DIN Track with a ground resistance of 100 Ω or less.
- The ground wire should not be more than 20 m long.
- Use a ground wire that is 2.0 mm^2 or larger. Refer to *5-3-7 Wiring to the Screwless Clamping Terminal Blocks* on page 5-46 for information on ground wires that are applicable to the functional ground terminal on the Communication Control Unit.
  For information on ground wires that are applicable to the functional ground terminals on the Additional NX Unit Power Supply Unit or Shield Connection Unit, refer to the *NX-series System Units User's Manual (Cat. No. W523)*.

If the DIN Track is made of steel and the surface is not treated to produce an insulating material, you can omit grounding the functional ground terminal on any Unit that has one, as shown in the following figures.

If the surface of the DIN Track is treated to produce an insulating material (e.g., anodized aluminum), the DIN Track contact plate will not be electrically connected to the DIN Track even if they are in physical contact.

Grounding the DIN Track

Attach a crimped terminal to the ground wire and then connect it to mounting hole on the DIN Track with a screw to ground the DIN Track.

Grounding the CPU Rack with Peripheral Devices and in Control Panels

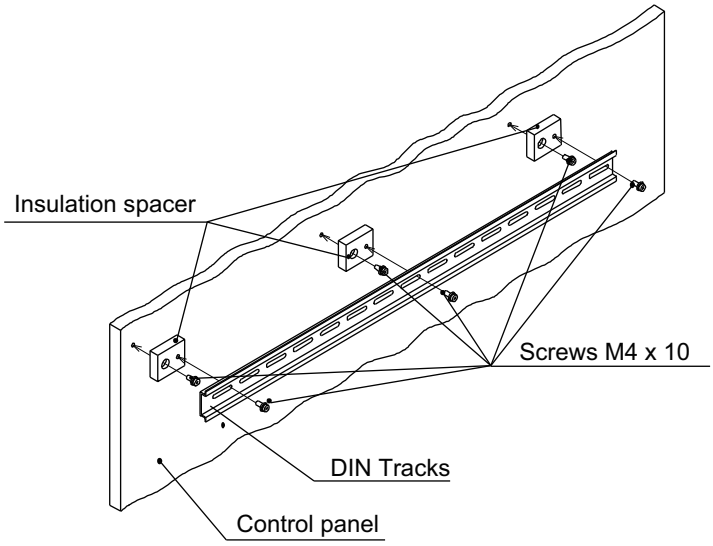
Refer to *5-4-6 Grounding* on page 5-67 for the grounding procedures for the CPU Rack with peripheral devices and in control panels.

Isolating the CPU Rack from the Control Panel

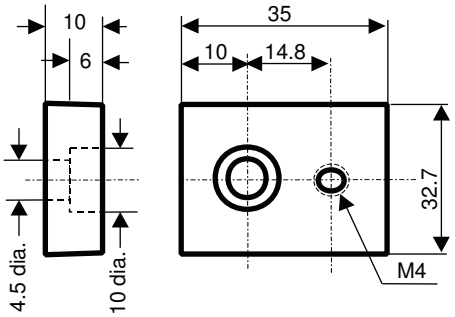
If the ground wire for a Unit with a ground terminal is shared with power equipment, noise will adversely affect the Units.
You can use OMRON NX-AUX01 DIN Track Insulation Spacers with PFP-50N or PFP-100N DIN Tracks to isolate the CPU Rack from the control panel.

● Installing DIN Track Insulation Spacers and DIN Track

Secure the DIN Track Insulation Spacers to the control panel with screws, and then secure the DIN Track to the DIN Track Insulation Spacers. The recommended tightening torque for M4 screws is 1.2 N·m.



- DIN Track Insulation Spacers
  NX-AUX01 (OMRON Corporation)
  Three Spacers are included in one model.



Precautions for Correct Use

If you use DIN Track Insulation Spacers to install a CPU Rack, the height will be increased by approximately 10 mm. Make sure that the CPU Rack and connecting cables do not come into contact with other devices.

5-3-6 Connecting the Built-in EtherNet/IP Port

Selecting the Network Devices

● Recommended Ethernet Switches

We recommend products that have passed the ODVA's conformance tests for Managed Ethernet Switch Device Profile.
For more information, contact ODVA.
ODVA website: https://www.odva.org

● Recommended Twisted-pair Cables and Connectors

Applicable EtherNet/IP communications cables and connectors vary depending on the used baud rate.
For 100Base-TX and 10Base-T, use an STP (shielded twisted-pair) cable of category 5 or higher. You can use either a straight or cross cable.
Cabling materials used for EtherNet/IP communication cables are shown in the table below. 100Base-TX in the Product name column of the table below indicates that either 100Base-TX or 10Base-T can be used.

Product name			Manufacturer	Model
For 1000Base-T and 100Base-Tx	Size and conductor pairs: AWG24×4 pairs *1	Cables	Hitachi Metals, Ltd.	NETSTAR-C5E SAB 0.5×4P CP
			Kuramo Electric Co., Ltd.	KETH-SB
			JMACS Japan Co., Ltd.	IETP-SB
		RJ45 Connectors	Panduit Corporation	MPS588-C
For 100Base-TX	Size and conductor pairs: AWG22×2 pairs*1	Cable	Kuramo Electric Co., Ltd.	KETH-PSB-OMR
			JMACS Japan Co., Ltd.	PNET/B
		RJ45 Assembly Connectors 	OMRON	XS6G-T421-1

*1. We recommend that you use cables and connectors in above combinations.

● Ethernet Switch Functions

This section describes the Ethernet switch functions that are important for an EtherNet/IP network. For a built-in EtherNet/IP port, consider whether the Ethernet switch supports these functions when you select the Ethernet switch.

- Multicast Filtering
  Multicast filtering transfers multicast packets to the specific nodes only. This function is implemented in the Ethernet switch as IGMP snooping or GMRP.
  Specific nodes are nodes equipped with an IGMP client, and have made transfer requests to the Ethernet switch. (OMRON built-in EtherNet/IP ports are equipped with an IGMP client.) Without

this function, multicast packets are transferred to all nodes in the network, just like broadcast packets, which increases the traffic in the network.
Settings must be made in the Ethernet switch to enable this function. There must be enough multicast filters for the network.

- QoS (Quality of Service) Function for TCP/UDP port numbers (L4)
  This function controls the priority of packet transmissions so that packets can be sent with higher priority to a particular IP address or TCP (UDP) port. The TCP and UDP protocols are called transport layer protocols, leading to the name L4 (layer 4) QoS function.
  When tag data links and message communications are executed on the same network, tag data links can be sent at higher priority to prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow.
  Settings must be made in the Ethernet switch to enable this function and give higher priority to tag data link packets.



Additional Information

If the Sysmac Studio or Network Configurator is used to set the connection type to **Multi-cast connection** in the connection settings, multicast packets are used. If the connection type is set to **Point to Point connection**, multicast packets are not used.

● Precautions for Ethernet Switch Selection

The functions supported by the Ethernet switch may affect tag data link transmission delays and the settings in the Controller configurations and setup.
In addition, if the Ethernet switch supports advanced functions, special settings are required for the functions.
When you select an Ethernet switch, it is necessary to consider what kind of data transmission and how much traffic you use over the the network.
Refer to the following precautions when you select an Ethernet switch.
Refer to *11-1 Adjusting the Communications Load* on page 11-2 to estimate the communications load for tag data links.

- Executing CIP Safety I/O communications and Tag Data Links Only
  We recommend that you use an L2 Ethernet switch without multicast filtering or an L2 Ethernet switch with multicast filtering.
  An L2 Ethernet switch with multicast filtering prevents increased traffic due to unnecessary multicast packets, therefore it allows CIP Safety I/O communications and the tag data links to operate at a higher speed.
  If either of the following conditions exists, there is no difference in the traffic whether multicast filtering is supported or not.
  a) CIP Safety I/O communications or the tag data links are set to share the same data with all nodes in the network. (The multicast packets are transferred to all nodes in the network, just like a broadcast.)
  b) CIP Safety I/O communications and the tag data link settings are all one-to-one (unicast) and multicast packets are not used.

  If multicast filtering is used, settings must be made accordingly on the Ethernet switch. There must be enough multicast filters for the network.

- Executing CIP Safety I/O communications or Tag Data Links, and Message Communications
  We recommend an L2 Ethernet switch with multicast filtering and L4 QoS.
  If you set CIP Safety I/O communications or the tag data links to higher-priority transmission, it is possible to prevent problems such as transmission delays due to message communications traffic and packet losses resulting from buffer overflow.
  You must make special settings in the Ethernet switch when using the multicast filtering function and L4 QoS function.

Precautions for Correct Use

- Ask the Ethernet switch manufacturer for setting procedures for the Ethernet switch.
- Install the Ethernet switch so that its environmental resistance specifications are not exceeded. Ask the Ethernet switch manufacturer for information on the environmental resistance of the Ethernet switch.

Network Installation

Refer to *Selecting the Network Devices* on page 5-39 for devices recommended for use with the built-in EtherNet/IP port.

Precautions for Correct Use

Basic installation precautions are given below.

- Take the greatest care when you install the Ethernet System. Be sure to follow ISO 8802-3 specifications. Be sure you understand them before attempting to install an Ethernet System.
- Unless you are already experienced in installation of communications systems, we strongly recommend that you employ a professional to install your system.
- Do not install Ethernet equipment near sources of noise.
  If a noisy environment is unavoidable, take adequate measures against noise interference, such as installation of network components in metal cases or the use of optical cable in the system.
- When using a shielded cable with the shields on both ends of the cable connected to connector hoods, ground loops induced by improper grounding methods may decrease noise immunity and cause device damage. To prevent ground loops caused by differences in potential between device grounding points, the reference potential between the devices must be stabilized. Design grounding appropriately so that noise current does not flow to ground lines between the devices. Refer to *Section 5 Installation and Wiring* on page 5-1 for grounding methods.
- To obtain information on installing EtherNet/IP cable, contact ODVA.
  ODVA website: https://www.odva.org
- When you install an EtherNet/IP network that combines an information network with the control system, and the communications load may be heavy due to tag data links, we recommend that you set up a network where the load does not affect communications. For example, install the tag data links in a segment that is separate from the information network.

● Precautions When Laying Twisted-pair Cable

- Firmly insert the connector until it locks into place when you connect the cable to the Ethernet switch and the built-in EtherNet/IP port.
- Do not lay the twisted-pair cable together with high-voltage lines.
- Do not lay the twisted-pair cable near devices that generate noise.
- Do not lay the twisted-pair cable in locations subject to high temperatures or high humidity.

- Do not lay the twisted-pair cable in locations subject to excessive dirt, dust, oil mist or other contaminants.

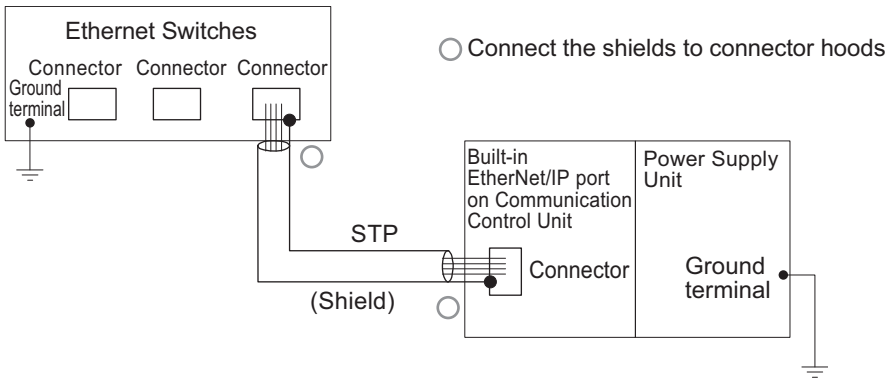
Connecting the Shield to Connector Hoods: Between an EtherNet/IP Port and an Ethernet Switch

Connect the shield to connector hoods as described below.

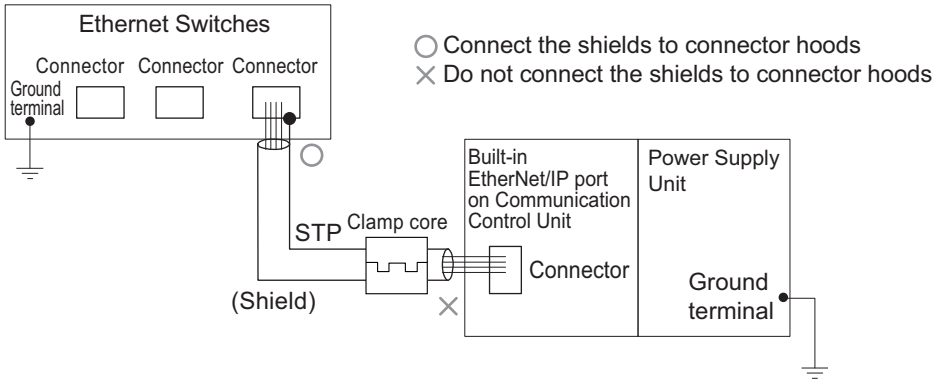
- Connect both ends
  or
- Connect the Ethernet Switch side only. A clamp core must be attached to the EtherNet/IP port side of the cable.

Connect the cable shields to the connector hoods as described in either (1) or (2) below.

1. Connecting the shields at both ends of the cable
   Connect the shields at both ends of the cables to connector hoods.



2. Connecting the shields on the Ethernet switch side only
   A clamp core must be attached to the end of the cable on the EtherNet/IP port side. For a recommended clamp core and attachment methods, refer to *Recommended Clamp Core and Attachment Method (page 5-43)* described later.
   To comply with EMC standards, it is mandatory that a clamp core be attached when connecting the shield to the connector hood only at the Ethernet switch side.
   Connect the shields to the connector hoods only at the Ethernet switch side.



Additional Information

Noise immunity may be reduced and device damage may occur due to ground loops, which can occur due to improper shield connections and grounding methods.
When using a baud rate of 100 Mbps or less, it may be possible to alleviate this problem by connecting only the Ethernet switch side as described in (2), rather than connecting both ends as described in (1).

Connecting the Shield to Connector Hoods: Between Two Ethernet Switches

Regardless of which baud rate is used, check with the Ethernet switch manufacturers for information about installing the network between Ethernet switches, and in particular whether or not it is necessary to connect the cable shields to the connector hoods.

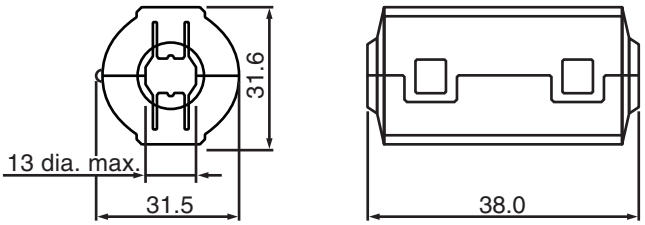
Recommended Clamp Core and Attachment Method

If you connect a shielded cable with only the Ethernet switch side connected to connector hoods, you must attach a clamp core to the EtherNet/IP port side of the Communication Control Unit.
The recommended clamp core and attachment method are given below.

Recommended Clamp Core:

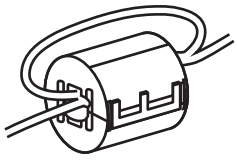
Manufacturer	Product	Model
NEC TOKIN	Clamp core	ESD-SR-250

ESD-SR-250 dimensions



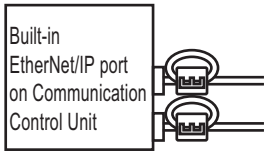
Recommended Attachment Method:

- Attaching a clamp core to the communication cable.



Make two loops with the cable as shown.

- Attaching a communication cable.



Attach to the base of the communications cable, as illustrated in the figure.

● Precautions When Installing Ethernet Switches

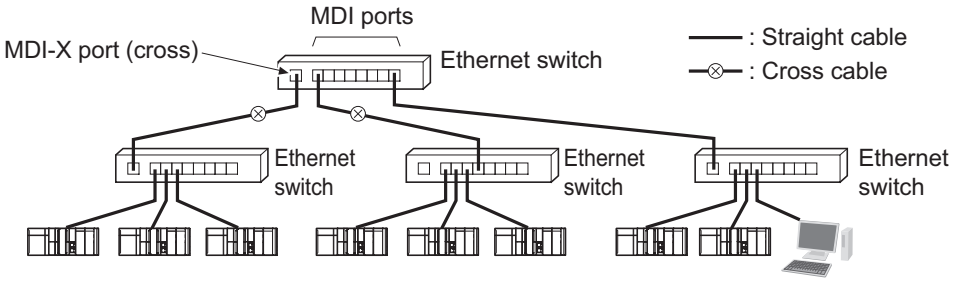
- Do not ground the Ethernet switch in the same location as a drive-system component, such as an inverter.

- Always use a dedicated power supply for the Ethernet switch. Do not use the same power supply for other equipment, such as an I/O power supply, motor power supply, or control power supply.
- Before installation, check the Ethernet switch's environmental resistance specifications, and use an Ethernet switch that is appropriate for the ambient conditions. Contact the Ethernet switch manufacturer for details on Ethernet switch's environmental resistance specifications.

● Ethernet Switch Connection Methods

- To connect Ethernet switches with twisted-pair cables, connect an MDI port to an MDI-X port with a straight cable.

  Note It is very difficult to distinguish cross cables and straight cables by appearance. Incorrect cables will cause communications to fail. We recommend cascade connections with straight cables wherever possible.



- Some Ethernet switches can automatically distinguish between MDI and MDI-X. When this kind of Ethernet switch is used, straight cable can be used between Ethernet switches.

Precautions for Correct Use

Adjust the built-in EtherNet/IP port's link settings to match the communications mode settings of the connected Ethernet switch. If the settings do not match, the link will be unstable and prevent normal communications. The following table shows the allowed settings for each Ethernet switch communications mode.

Ethernet Switches		Built-in EtherNet/IP Port				
		AUTO-Nego*1	10 Mbps (fixed)		100 Mbps (fixed)	
			full*1	half*1	full	half
Auto-Nego		Best	--	OK	--	OK
10 Mbps (fixed)	full	--	OK	--	--	--
	half	OK	--	OK	--	--
100 Mbps (fixed)	full	--	--	--	OK	--
	half	OK	--	--	--	OK
1,000 Mbps (fixed)	full	--	--	--	--	--

*1. AUTO-Nego: Auto-negotiation, full: Full-duplex, half: Half-duplex.

(Best = Recommended; OK = Allowed; --- = Not allowed.)

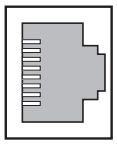
Connecting to the Network

● Ethernet Connectors

The following standards and specifications apply to the connectors for the Ethernet twisted-pair cable.

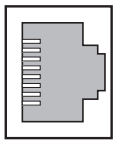
- Electrical specifications: Conforming to IEEE 802.3 standards.
- Connector structure: RJ45 8-pin Modular Connector (conforming to ISO 8877)
- For information on connecting shield wire to connector hoods, refer to *Precautions When Laying Twisted-pair Cable* on page 5-41.

10BASE-T and 100BASE-TX:



Connector pin	Signal name	Abbreviation	Signal direction
1	Transmission data +	TD+	Output
2	Transmission data −	TD−	Output
3	Reception data +	RD+	Input
4	Not used.	---	---
5	Not used.	---	---
6	Reception data −	RD−	Input
7	Not used.	---	---
8	Not used.	---	---

1000BASE-T:



Connector pin	Signal name	Abbreviation	Signal direction
1	Communication data DA+	BI_DA+	Input/output
2	Communication data DA−	BI_DA-	Input/output
3	Communication data DB+	BI_DB+	Input/output
4	Communication data DC+	BI_DC+	Input/output
5	Communication data DC−	BI_DC−	Input/output
6	Communication data DB−	BI_DB−	Input/output
7	Communication data DD+	BI_DD+	Input/output
8	Communication data DD−	BI_DD−	Input/output

● Connecting the Cable

Precautions for Correct Use

- Turn OFF the Controller's power supply before connecting or disconnecting Ethernet communications cable.
- Allow extra space for the bending radius of the communications cable.
  For the dimensions when the communications cable is connected to the Communication Control Unit, refer to *Section 5 Installation and Wiring* on page 5-1. The required space depends on the communications cable and connector that are used. Consult the manufacturer or sales agent.

1 Lay the twisted-pair cable.

2 Connect the cable to the Ethernet switch.

3 Connect the twisted-pair cable to the connector on the built-in EtherNet/IP port.
Be sure to press the connectors (both the Ethernet switch side and Ethernet side) until they lock into place.

5-3-7 Wiring to the Screwless Clamping Terminal Blocks

This section describes how to connect wires to the screwless clamping terminal blocks, the installation and removing methods, and functions for preventing incorrect attachment.

You can connect ferrules that are attached to the twisted wires to the screwless clamping terminal block. You can also connect the twisted wires or the solid wires to the screwless clamping terminal block. If you connect the ferrules, all you need to do to connect the wires is to insert the ferrules into the terminal holes.

⚠ WARNING

Make sure that the voltages and currents that are input to the Units and slaves are within the specified ranges.
Inputting voltages or currents that are outside of the specified ranges may cause accidents or fire.

Wiring Terminals

The terminals to be wired are as follows.

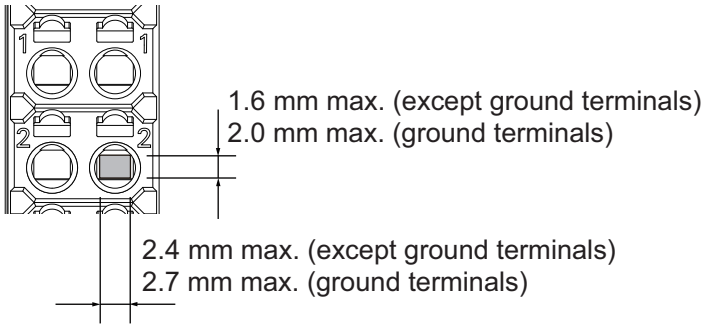
- I/O power supply terminals
- I/O terminals

Applicable Wires

You can connect twisted wires, solid wires, or ferrules attached to twisted wires to the screwless clamping terminal block. The applicable wire dimensions and preparation methods are given below.

● Dimensions of Wires Connected to the Terminal Block

The dimensions of wires that you can connect into the terminal holes of the screwless clamping terminal block are as in the figure below.
Process the applicable wires that are specified in the following description to apply the dimensions.



● Using Ferrules

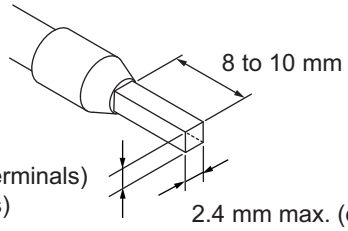
If you use ferrules, attach the twisted wires to them.
Observe the application instructions for your ferrules for the wire stripping length when attaching ferrules.
Always use plated one-pin ferrules. Do not use unplated ferrules or two-pin ferrules.

The applicable ferrules, wires, and crimping tools are given in the following table.

Terminal type	Manufacturer	Ferrule model	Applicable wire (mm^2 (AWG))	Crimping tool
All terminals except ground terminals	Phoenix Contact	AI0,34-8	0.34 (#22)	Phoenix Contact (Applicable wire sizes are given in parentheses.) CRIMPFOX 6 (0.25 to 6 mm^2, AWG24 to 10)
		AI0,5-8	0.5 (#20)	
		AI0,5-10		
		AI0,75-8	0.75 (#18)	
		AI0,75-10		
		AI1,0-8	1.0 (#18)	
		AI1,0-10		
		AI1,5-8	1.5 (#16)	
		AI1,5-10		
Ground terminals		AI2,5-10	2.0*1	
All terminals except ground terminals	Weidmuller	H0.14/12	0.14 (#26)	Weidmuller (Applicable wire sizes are given in parentheses.) PZ6 Roto (0.14 to 6 mm^2, AWG26 to 10)
		H0.25/12	0.25 (#24)	
		H0.34/12	0.34 (#22)	
		H0.5/14	0.5 (#20)	
		H0.5/16		
		H0.75/14	0.75 (#18)	
		H0.75/16		
		H1.0/14	1.0 (#18)	
		H1.0/16		
		H1.5/14	1.5 (#16)	
		H1.5/16		

*1. For the ferrule type AI2,5-10, use wires with a diameter of 2.0 to 2.1 mm^2. Wires with a diameter exceeding 2.1 mm^2 cannot be used with the screwless clamping terminal block.

When you use any ferrules other than those in the above table, crimp them to the twisted wires so that the following processed dimensions are achieved.



1.6 mm max. (except ground terminals)
2.0 mm max. (ground terminals)

2.4 mm max. (except ground terminals)
2.7 mm max. (ground terminals)

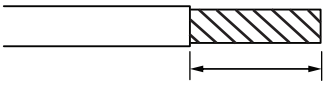
● Using Twisted or Solid Wires

If you use twisted wires or solid wires, use the following table to determine the correct wire specifications.

Terminals		Wire type				Wire size	Conductor length (stripping length)
		Twisted wires		Solid wire			
Classification	Current capacity	Plated	Unplated	Plated	Unplated		
All terminals except ground terminals	2 A max.	Possible	Possible	Possible	Possible	0.08 to 1.5 mm^2 (AWG28 to 16)	8 to 10 mm
	Greater than 2 A and 4 A or less		Not possible	Possible*1	Not possible		
Ground terminals	---	Possible	Possible	Possible*2	Possible*2	2.0 mm^2	9 to 10 mm

*1. Secure wires to the screwless clamping terminal block. Refer to *Securing Wires* on page 5-48 for how to secure wires.

*2. With the NX-TB□□□1 Terminal Block, use twisted wires to connect the ground terminal. Do not use a solid wire.

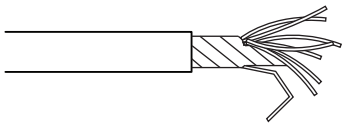


Conductor length (stripping length)

Precautions for Correct Use

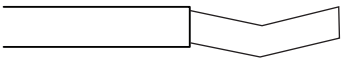
- Use cables with suitable wire sizes for the carrying current. There are also restrictions on the current due to the ambient temperature. Refer to the manuals for the cables and use the cables correctly for the operating environment.
- For twisted wires, strip the sheath and twist the conductor portion. Do not unravel or bend the conductor portion of twisted wires or solid wires.

NG



Unravel wires

NG



Bend wires

Additional Information

If more than 2 A will flow on the wires, use plated wires or use ferrules.

Securing Wires

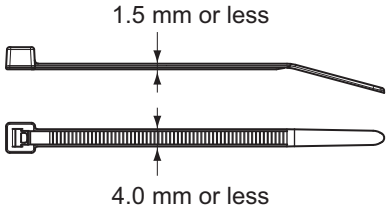
It is necessary to secure wires to the screwless clamping terminal block depending on the wire types that are used or the current flows on the wires.

The following table gives the necessity for securing wires.

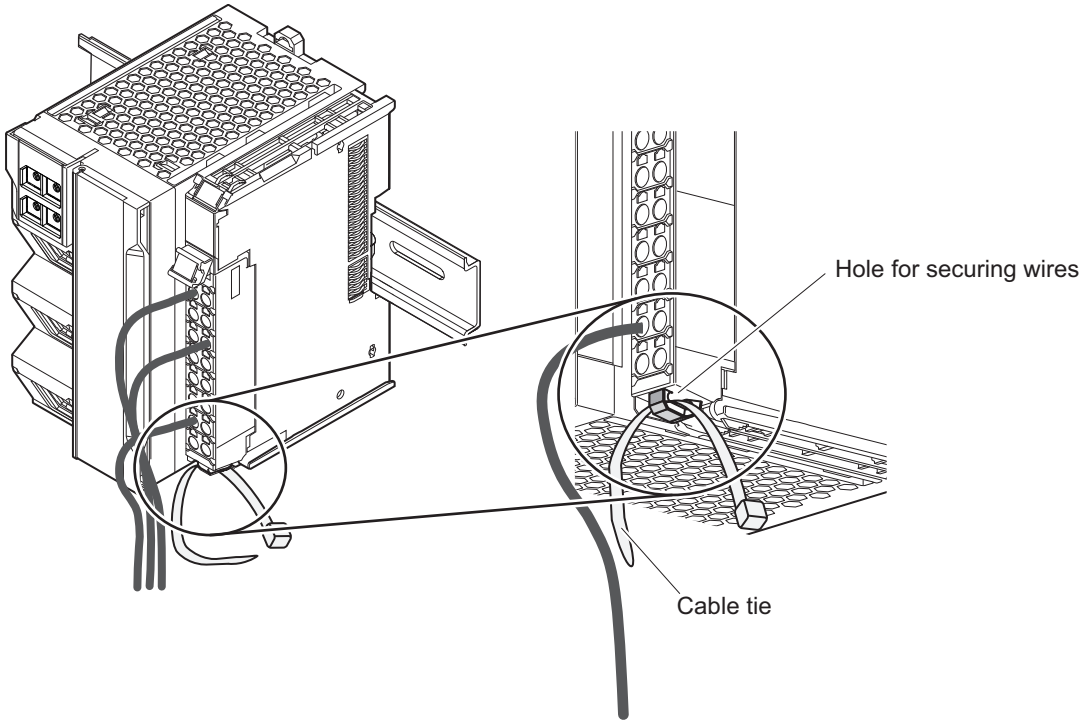
Terminals		Wire type				
		Ferrule	Twisted wires		Solid wire	
Classification	Current capacity		Plated	Unplated	Plated	Unplated
All terminals except ground terminals	2 A max.	No	No	No	No	No
	Greater than 2 A and 4 A or less			Not possible	Yes	Not possible
Ground terminals	---		No	No	No	No

Use the following procedure to secure the wires.

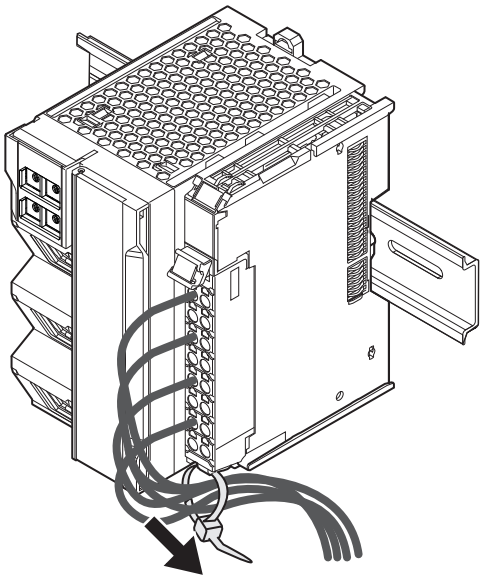
1 Prepare a cable tie.
A cable tie can be used with a width of 4 mm or less and a thickness of 1.5 mm or less. Select a cable tie correctly for the operating environment.



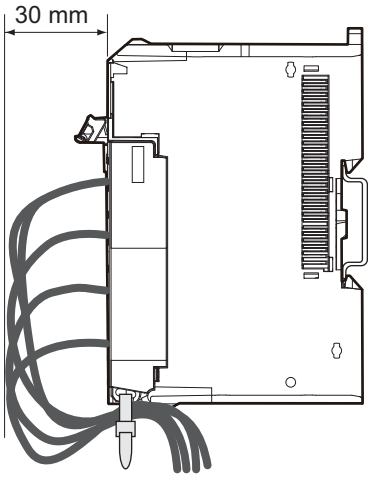
2 Pass a cable tie through the hole for securing wires on the bottom of the screwless clamping terminal block.



3 Bundle the wires with a cable tie and secure them to the screwless clamping terminal block.



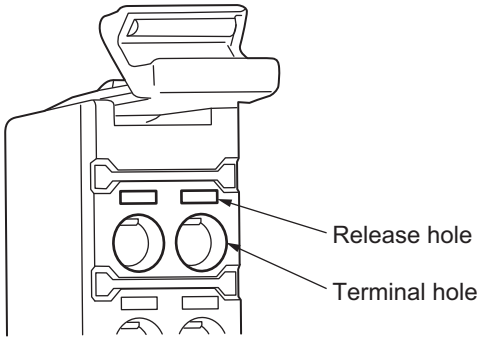
Secure wires within the range of 30 mm from the screwless clamping terminal block.



Connecting and Removing Wires

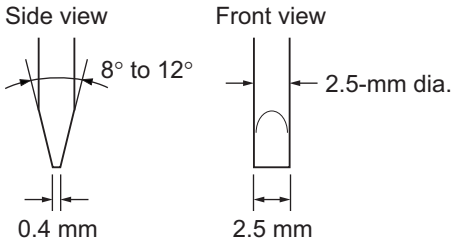
This section describes how to connect and remove wires.

● Terminal Block Parts and Names



● Required Tools

Use a flat-blade screwdriver to connect and remove wires.
Use the following flat-blade screwdriver.

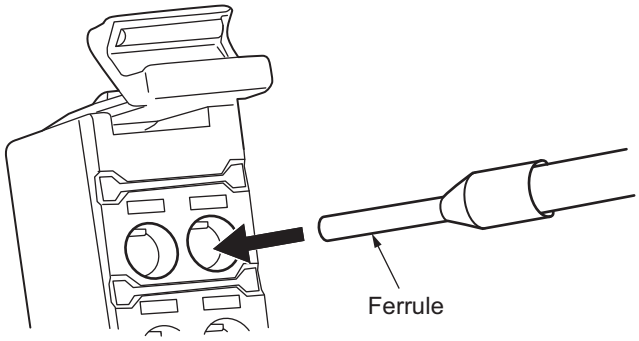


Recommended screwdriver

Model	Manufacturer
SZF 0-0,4X2,5	Phoenix Contact

● Connecting Ferrules

Insert the ferrule straight into the terminal hole.
You do not need to insert a flat-blade screwdriver into the release hole.

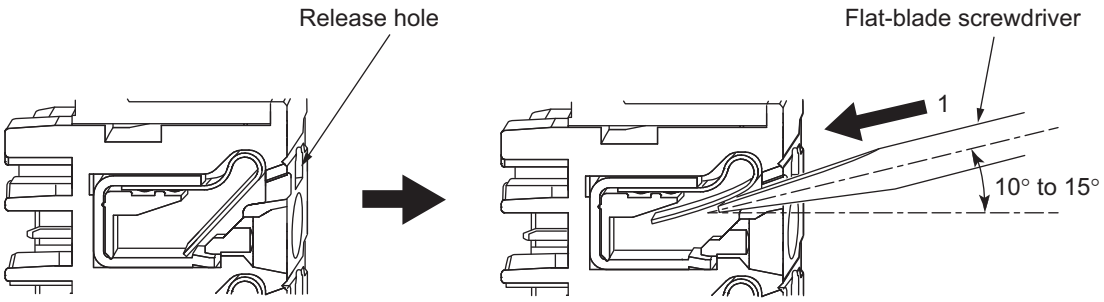


After you make a connection, make sure that the ferrule is securely connected to the terminal block.

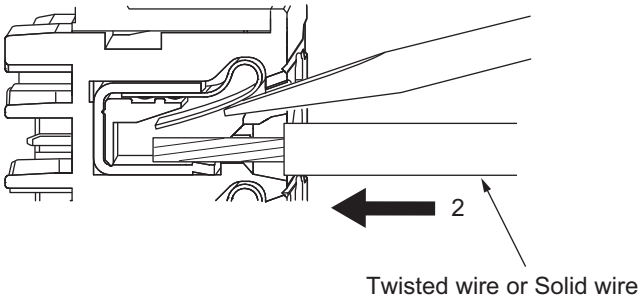
● Connecting Twisted Wires or Solid Wires

Use the following procedure to connect the twisted wires or solid wires to the terminal block.

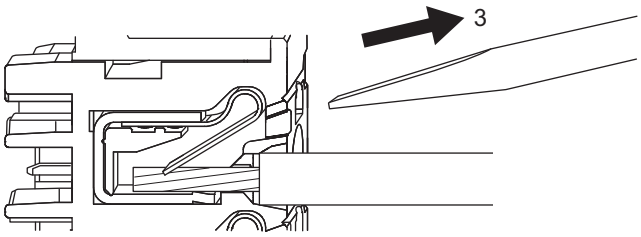
1 Press a flat-blade screwdriver diagonally into the release hole.
The optimal angle for insertion is between 10° to 15°. If the screwdriver is inserted correctly, you should feel resistance from the spring inside the release hole.



2 Leave the flat-blade screwdriver pressed into the release hole and insert the twisted wire or the solid wire into the terminal hole.
Insert the stripped portion of the wire all the way into the terminal hole to prevent shorting.



3 Remove the flat-blade screwdriver from the release hole.

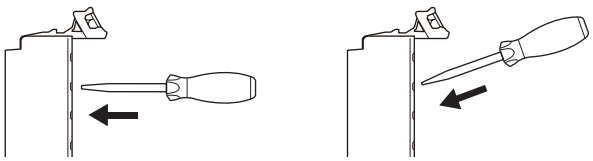


After you make a connection, lightly pull the twisted wire or the solid wire to make sure that the wire is securely connected to the terminal block.

Precautions for Safe Use

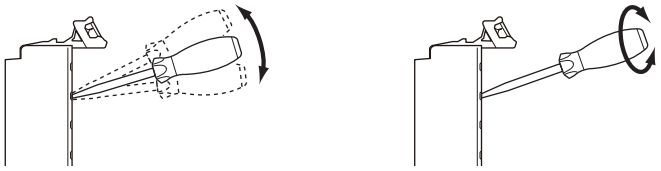
- Do not press the flat-blade screwdriver straight into the release holes on a screwless clamping terminal block. Doing so may damage the terminal block.

NG **OK**



- When you insert a flat-blade screwdriver into a release hole on a screwless clamping terminal block, press it down with a force of 30N or less. Applying excessive force may damage the terminal block.
- Do not incline or twist the flat-blade screwdriver while it is in a release hole on a screwless clamping terminal block. Doing so may damage the terminal block.

NG **NG**



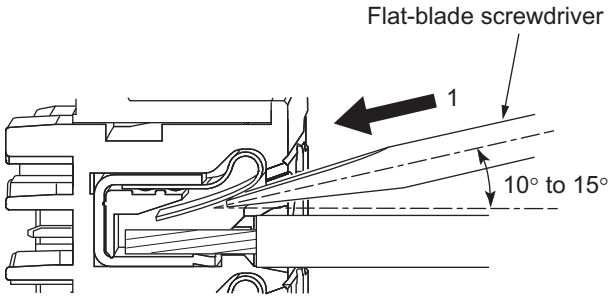
- Make sure that all wiring is correct.
- Do not bend the cable forcibly. Doing so may break the cables.

● Removing Wires

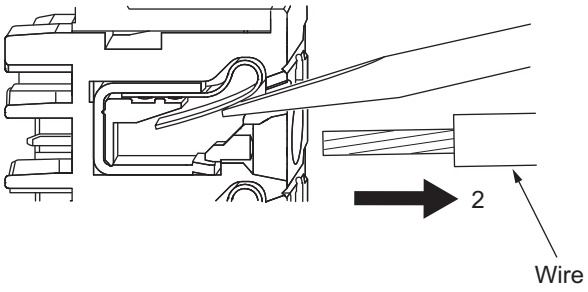
Use the following procedure to remove the wires from the terminal block.
The removal method is the same for ferrules, twisted wires, and solid wires.

If wires are secured firmly to the terminal block, release them first.

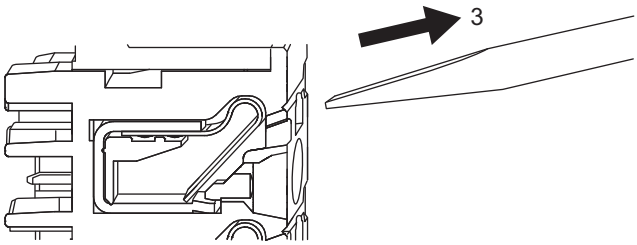
1 Press the flat-blade screwdriver diagonally into the release hole.
The optimal angle for insertion is between 10° to 15°. If the screwdriver is inserted correctly, you should feel resistance from the spring inside the release hole.



2 Insert the flat-blade screwdriver into the release hole and remove the wire from the terminal hole.



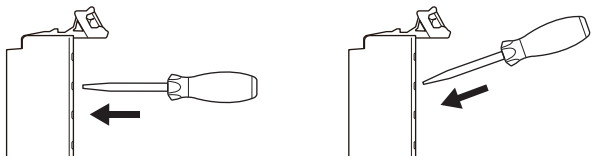
3 Remove the flat-blade screwdriver from the release hole.



Precautions for Safe Use

- Do not press the flat-blade screwdriver straight into the release holes on a screwless clamping terminal block. Doing so may damage the terminal block.

NG **OK**



- When you insert a flat-blade screwdriver into a release hole on a screwless clamping terminal block, press it down with a force of 30N or less. Applying excessive force may damage the terminal block.
- Do not incline or twist the flat-blade screwdriver while it is in a release hole on a screwless clamping terminal block. Doing so may damage the terminal block.

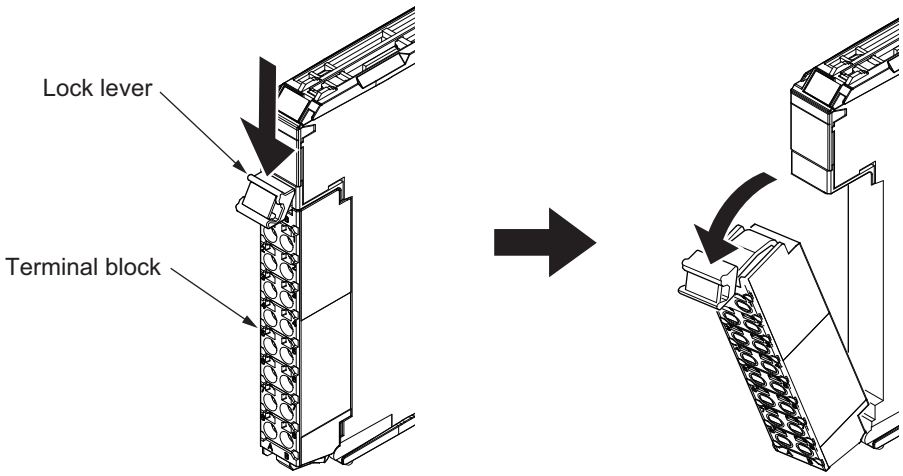
NG **NG**



- Make sure that all wiring is correct.
- Do not bend the cable forcibly. Doing so may break the cables.

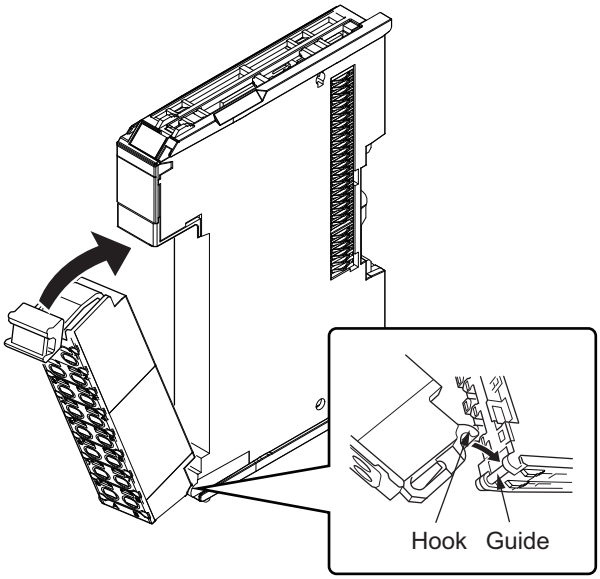
Removing a Terminal Block

1 Press the lock lever on the terminal block and pull out the top of the terminal block to remove it.



Attaching a Terminal Block

1 Mount the terminal block hook that is applicable to each Unit model on the guide at the bottom of the NX Unit, lift up the terminal block, and press in on the top of the terminal block until you hear it engage.
The terminal block will click into place on the Unit. After you mount the terminal block, make sure that it is locked to the Unit.

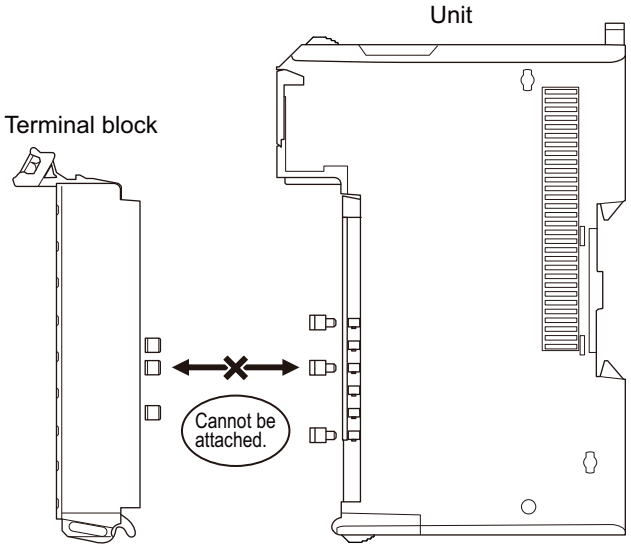


Refer to the user's manuals of the NX Units for the applicable terminal blocks.

Preventing Incorrect Attachment of Terminal Blocks

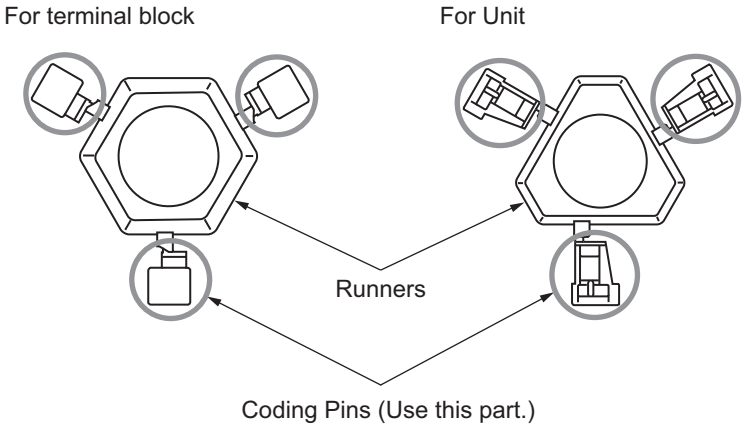
In order to prevent unintentionally installing the wrong terminal block, you can limit the combination of a Unit and a terminal block.

Insert three Coding Pins (NX-AUX02) into three of the six incorrect attachment prevention holes on the Unit and on the terminal block. Insert these pins into positions so that they do not interfere with each other when the Unit and terminal block are connected to each other.
You can use these pins to create a combination in which the wrong terminal block cannot be attached because the pin patterns do not match.



● Types of Coding Pins

There are two types of Coding Pins, both with their own unique shape: one for terminal blocks and one for Units.
Three pins come with each runner.



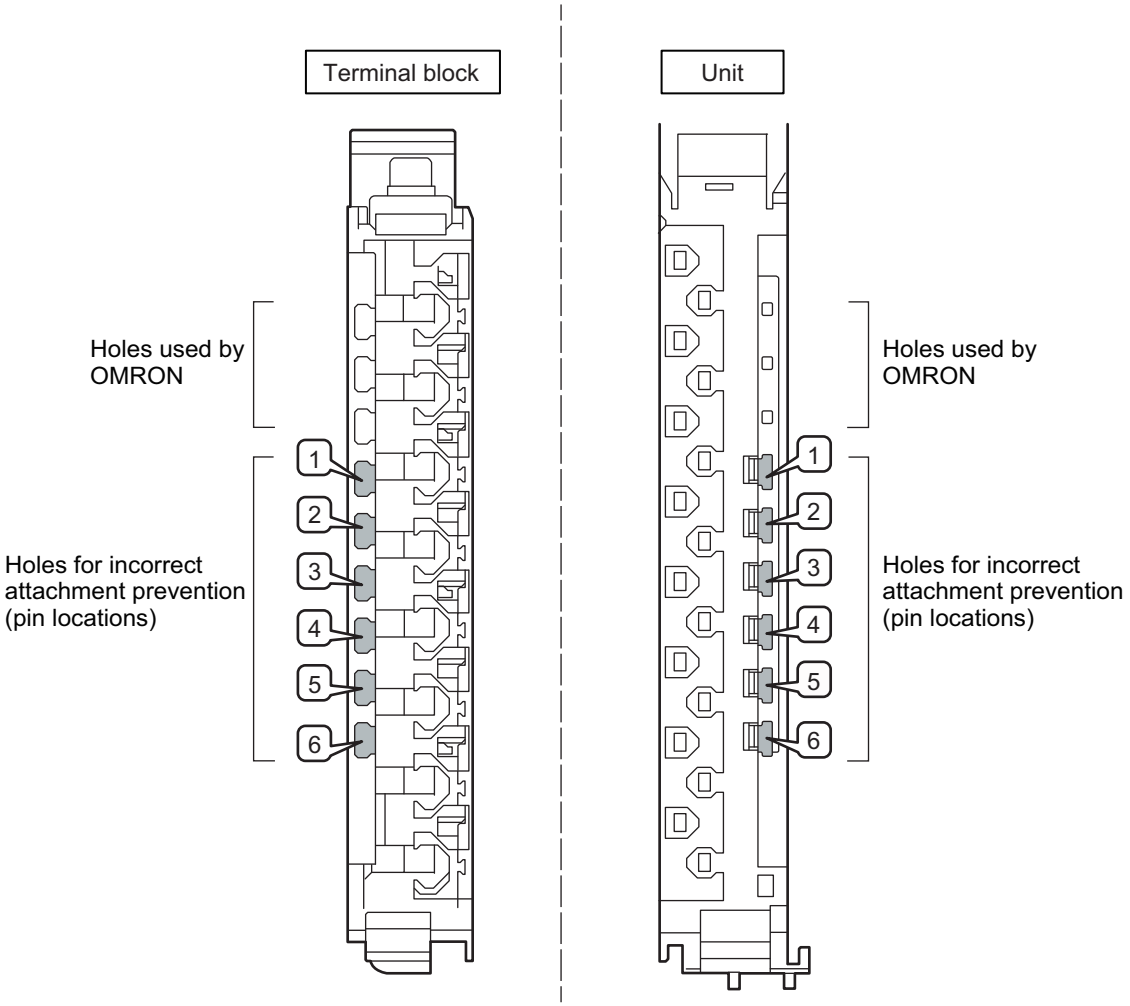
Use the following Coding Pins.

Name	Model	Specification
Coding Pin	NX-AUX02	For 10 Units (Terminal block: 30 pins, Unit: 30 pins)

● Insertion Locations and Patterns of Coding Pins

Insert three Coding Pins each on the terminal block and on the Unit at the positions designated by the numbers 1 through 6 in the figure below.

As shown in the following table, there are 20 unique pin patterns that you can use.



○: Pin inserted

Pattern	Pin locations for terminal block						Pin locations for Unit					
	1	2	3	4	5	6	1	2	3	4	5	6
No.1	○	○	○							○	○	○
No.2	○	○		○					○		○	○
No.3	○	○			○				○	○		○
No.4	○	○				○			○	○	○	
No.5	○		○	○				○			○	○
No.6	○		○		○			○		○		○
No.7	○		○			○		○		○	○	
No.8	○			○	○			○	○			○
No.9	○			○		○		○	○		○	
No.10	○				○	○		○	○	○		
No.11		○	○	○			○				○	○
No.12		○	○		○		○			○		○
No.13		○	○			○	○			○	○	
No.14		○		○	○		○		○			○
No.15		○		○		○	○		○		○	
No.16		○			○	○	○		○	○		
No.17			○	○	○		○	○				○
No.18			○	○		○	○	○			○	
No.19			○		○	○	○	○		○		
No.20				○	○	○	○	○	○			

Two sets of NX-AUX02 Pins are required to make the maximum of 20 pin patterns. (One set for 10 Units.)

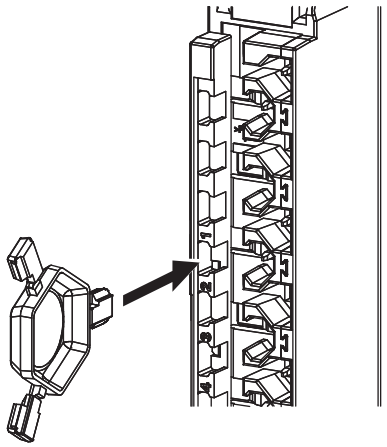
Precautions for Correct Use

- The holes not designated by the numbers 1 through 6 in the above figure are used by OMRON. If you insert any Coding Pins into the holes reserved for use by OMRON, you will not be able to mount the terminal block to the Unit.
- Do not use Coding Pins that have been attached and removed.

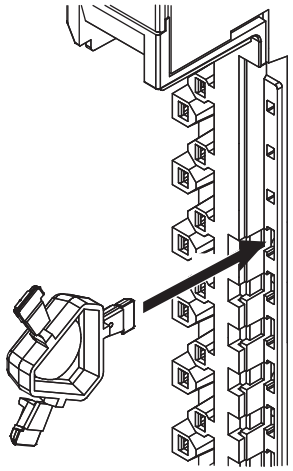
● Inserting the Coding Pins

1 Hold the pins by the runner and insert a pin into one of the incorrect attachment prevention holes on the terminal block or on the Unit.

Terminal block

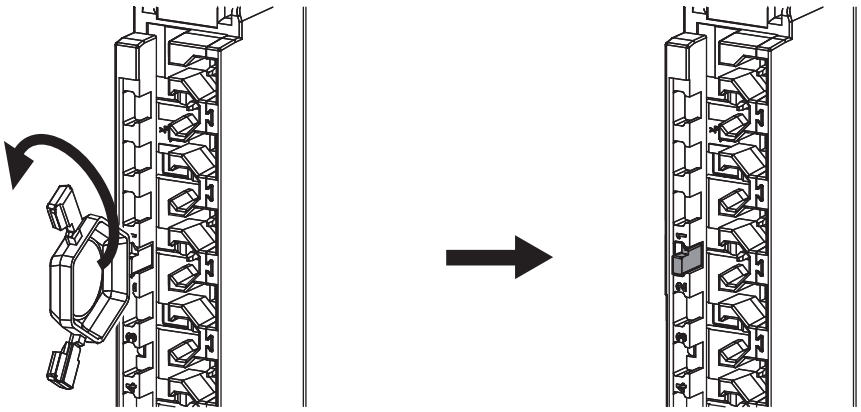


Unit

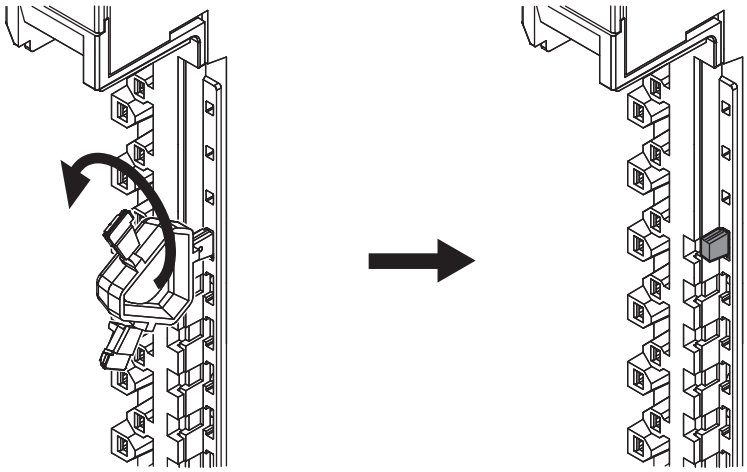


2 Rotate the runner to break off the Coding Pin.

Terminal block



Unit



Checking Wiring

You can check the wiring from the Watch Tab Page on the Sysmac Studio.
For Input Units, you can turn ON and OFF an input from the external device that is connected to the Unit you need to check and monitor the results.
For Output Units, you can use forced refreshing to control the I/O outputs to the Unit you need to check to confirm the operation of the connected external device.
Refer to *Section 9 Checking Operation and Actual Operation* on page 9-1 for the monitoring and forced refreshing operations.

5-4 Control Panel Installation

To ensure system reliability and safety, the system must be designed and configured according to the installation environment (temperature, humidity, vibration, shock, corrosive gases, overcurrent, noise, etc.).

5-4-1 Temperature

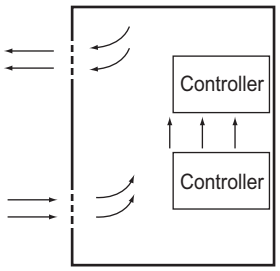
Panels have been reduced in size due to space-saving and miniaturization in devices and systems, and the temperature inside the panel may be at least 10 to 15°C higher than outside the panel. Implement the following measures against overheating at the installation site and in the panel, and allow a sufficient margin for the temperature before use.

High Temperatures

Use the following cooling methods as required, taking into account the ambient temperature and the amount of heating inside the panel.

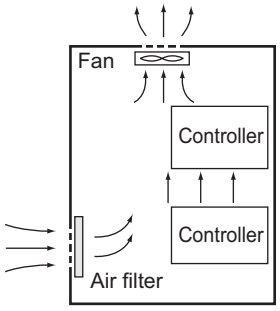
● Natural Cooling

- Natural cooling relies on natural ventilation through slits in the panel, rather than using cooling devices such as fans or coolers. When using this method, observe the following points.
- Do not install the Controller at the top of the panel, where hot air tends to stagnate.
- To provide ventilation space above and below the Controller, leave sufficient distance from other devices, wiring ducts, etc.
- Do not mount the Units in the wrong direction (e.g., vertically or upside down). Doing so may cause abnormal heating in the Controller.
- Do not install the Controller directly above any heat-generating equipment, such as heaters, transformers, and devices with high resistance.
- Do not install the Controller in a location exposed to direct sunlight.



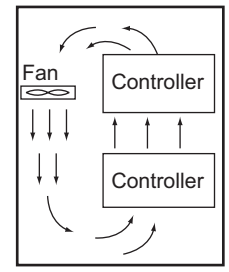
Natural Cooling

● Forced Ventilation (by Fan at Top of Panel)



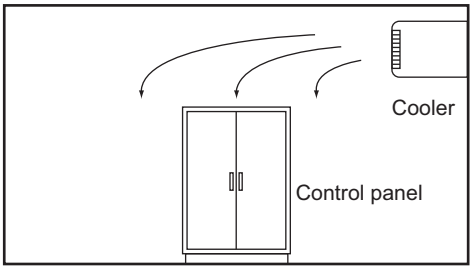
Forced Ventilation Method

● Forced Air Circulation (by Fan in Closed Panel)



Forced Air Circulation

● Room Cooling (Cooling the Entire Room Where the Control Panel Is Located)



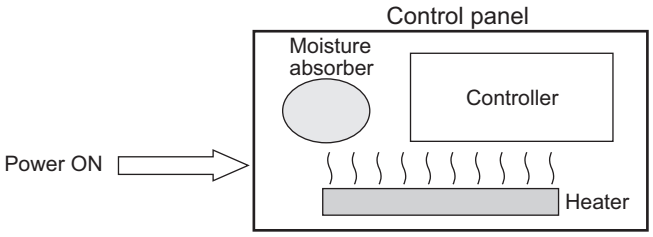
Room Cooling

Low Temperatures

The Controller may not start normally if the temperature is below 0°C when the power is turned ON. Maintain an air temperature of at least approximately 5°C inside the panel, by implementing measures such as installing a low-capacity space heater in the panel.
Alternatively, leave the Controller power ON to keep the Controller warm.

5-4-2 Humidity

Rapid temperature changes can cause condensation to occur, resulting in malfunctioning due to short-circuiting.
When there is a possibility of this occurring, take measures against condensation, such as leaving the Controller power ON at night or installing a heater in the control panel to keep it warmer.



Examples of Measures against Condensation

5-4-3 Vibration and Shock

The Controller is tested for conformity with the sine wave vibration test method (IEC 60068-2-6) and the shock test method (IEC 60068-2-27) of the Environmental Testing for Electrotechnical Products. It is designed so that malfunctioning will not occur within the specifications for vibration and shock. If, however, the Controller is to be used in a location in which it will be directly subjected to regular vibration or shock, then implement the following countermeasures:

- Separate the control panel from the source of the vibration or shock.
  Or secure the Controller and the panel with rubber padding to prevent vibration.
- Make the building or the floor vibration-resistant.
- To prevent shock when other devices in the panel such as electromagnetic contactors operate, secure either the source of the shock or the Controller with rubber padding.

5-4-4 Atmosphere

Using the Controller in any of the following locations can cause defective contact with connectors and corrosion of components. Implement countermeasures such as purging the air as required.

- In locations exposed to dust, dirt, salt, metal powder, soot, or organic solvents, use a panel with an airtight structure. Be careful of temperature increases inside the panel.
- In locations exposed to corrosive gas, purge the air inside the panel to clear the gas and then pressurize the inside of the panel to prevent gas from entering from outside.
- In locations where flammable gas is present, either use an explosion-protected construction or do not use the Controller.

5-4-5 Electrical Environment

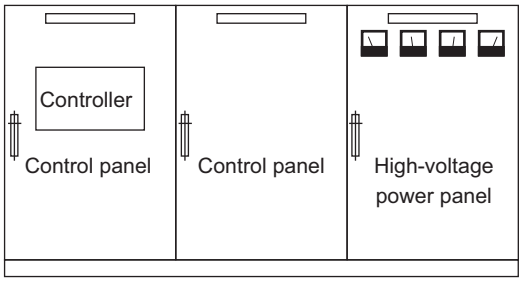
When installing or wiring devices, make sure that there will be no danger to people and that noise will not interfere with electrical signals.

Controller Installation Location

Install separately the Controller from high-voltage (600 V or higher) and power devices to ensure safe operation and maintenance. Install the Controller as far away as possible in case of unavoidable circumstances.

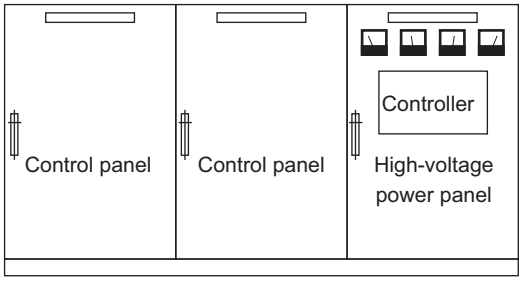
Example of Recommended Equipment Arrangement

OK



Example of Poor Equipment Arrangement

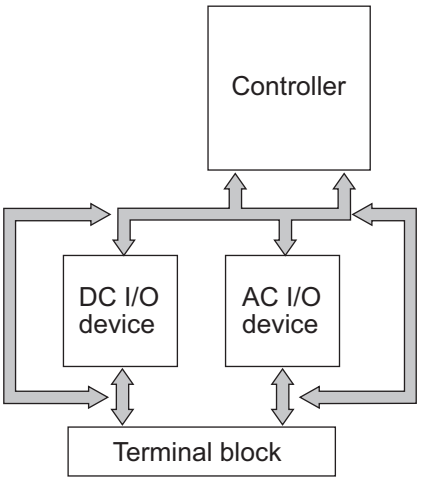
NG



Examples of Equipment Arrangement in Panel with High-voltage Devices

Arrangement of Controller and Units

The coils and contacts in electromagnetic contacts and relays in an external circuit are sources of noise. Do not install them close to the Controller. Locate them at least 100 mm away from the Controller.

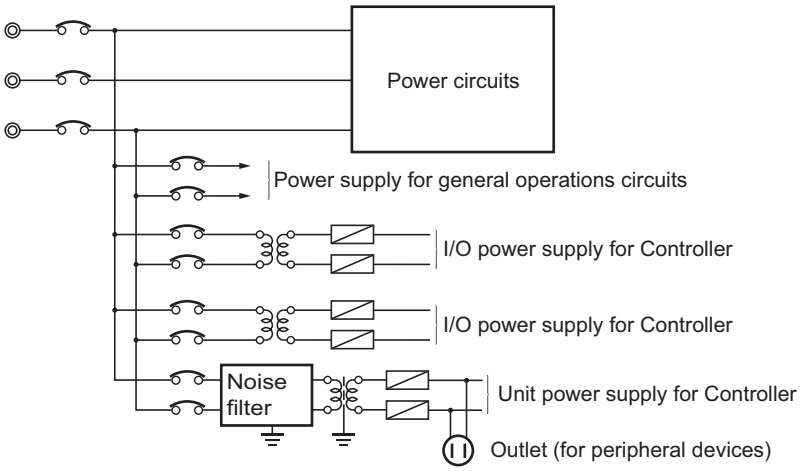


Example of Arrangement in Panel

Wire Layout for the Power Supply System

Observe the following points when wiring the power supply system.

- Separate the Controller power supply from the I/O device power supply and install a noise filter near the Controller power supply feed section.
- Use an isolating transformer to significantly reduce noise between the Controller and the ground. Install the isolating transformer between the Controller power supply and the noise filter, and do not ground the secondary coil of the transformer.
- Keep the wiring between the transformer and the Controller as short as possible, twist the wires well, and keep the wiring separate from high-voltage and power lines.

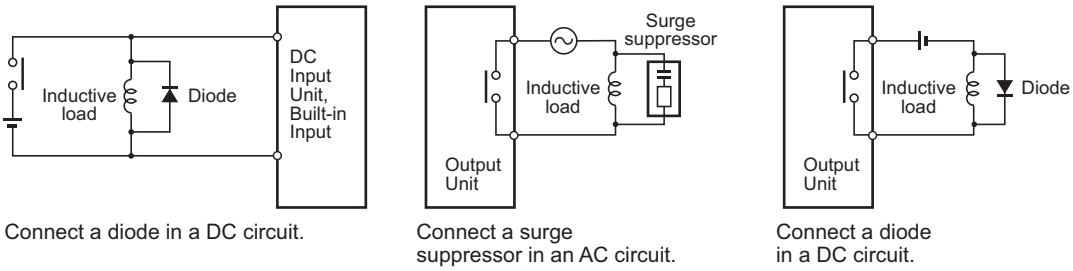


Power Supply System Diagram

Wiring External I/O Signal Lines

Observe the following points when wiring external I/O signal lines.

- To absorb reverse electromotive force when an inductive load is connected to an output signal, connect a surge suppressor near the inductive load in an AC circuit, or connect a diode near the inductive load in a DC circuit.



Connect a diode in a DC circuit.

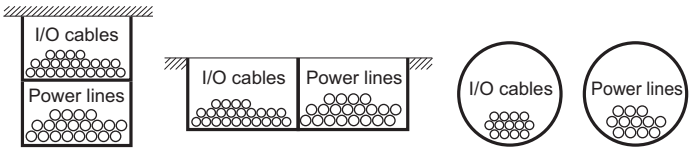
Connect a surge suppressor in an AC circuit.

Connect a diode in a DC circuit.

Input Signal Noise Countermeasures

Output Signal Noise Countermeasures

- Never bundle output signal lines with high-voltage or power lines, and do not route them in close proximity or parallel to such lines.
  If output signal lines must be routed in close proximity to such lines, place them in separate ducts or conduits. Be sure to ground the ducts or conduits.



Suspended ducts

Floor ducts

Conduits

I/O Cable Arrangement

- If the signal lines and power lines cannot be routed in separate ducts, use shielded cable. Connect the shield to the ground terminal at the Controller, and leave it unconnected at the input device.
- Wire the lines so that common impedance does not occur.
  Such wiring will increase the number of wires, so use common return circuits.
  Use thick wires with sufficient allowance for the return circuits, and bundle them with lines of the same signal level.
- For long I/O lines, wire the input and output signal lines separately.
- Use twisted-pair wires for pilot lamps (and particularly lamps with filaments).
- Use countermeasures, such as CR surge absorbers and diodes, for input device and output load device noise sources, as required.

External Wiring

Wiring, and noise countermeasures in particular, are based on experience, and it is necessary to closely manage wiring based on experience and information in the manuals.

● Wiring Routes

Each of the following combinations includes different signal types, properties, or levels. They will cause the signal-to-noise ratio to drop due to factors such as electrical induction. As a general rule when wiring, either use separate cables or separate wiring routes for these items. Future maintenance operations and changes to the system will also be made easier by carefully organizing the wiring from the start.

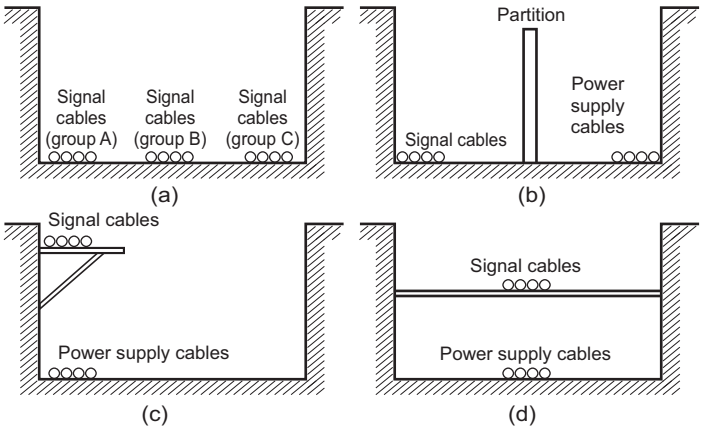
- Power lines and signal lines
- Input signals and output signals
- Analog signals and digital signals
- High-level signals and low-level signals

- Communications lines and power lines
- DC signals and AC signals
- High-frequency devices (such as Inverters) and signal lines (communications)

● Wiring

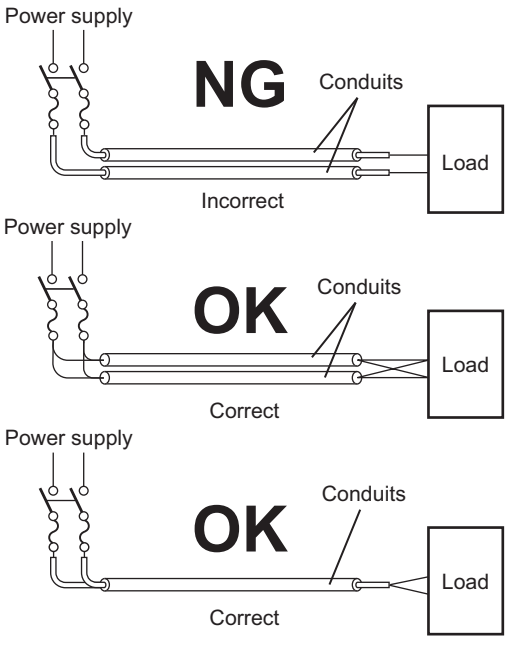
Observe the following points when wiring power supply and signal cables.

- When routing signal cables with differing characteristics through the same duct, always keep them separated.
- As much as possible, avoid routing multiple power supply lines through the same duct. If it cannot be avoided, then construct a partition between them in the duct and ground the partition.



Partitioning Methods for Signal and Power Supply Cables

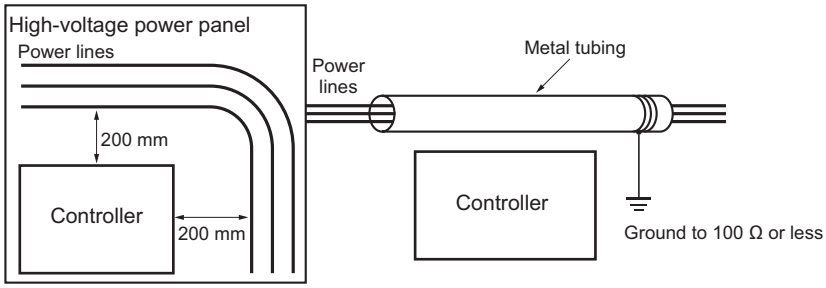
- To avoid overheating the conduits when using conduits for wiring, do not place wires for a single circuit in separate conduits.



Parallel Wiring (Single Phase)

- Power cables and signal cables adversely affect each other. Do not wire them in parallel.

- Noise induction may occur if the Controller is installed in a panel that includes high-voltage devices. Wire and install them as far apart as possible. (Refer to *Controller Installation Location* on page 5-63.)
- Either install the Controller a minimum of 200 mm away from high-voltage lines or power lines, or place the high-voltage lines or power lines in metal tubing and completely ground the metal tubing to 100 Ω or less.



Example: Separating Controller from Power Lines

● Other Precautions

- Digital I/O Units have both plus and minus commons, so pay attention to the polarity when wiring.

5-4-6 Grounding

This section describes the earthing methods and precautions.

Considerations for Earthing Methods

Local potential fluctuations due to lightning or noise from power devices will cause potential fluctuations between ground terminals of devices. This potential fluctuation may result in device malfunction or damage. To prevent this, it is necessary to suppress the occurrence of a difference in electrical potential between ground terminals of devices. You need to consider the earthing methods to achieve this objective

The recommended earthing methods for each usage condition are given in the following table.

Specifications of communications cables for EtherNet/IP	Earthing methods			
	Equipotential bonding system	Star earthing		Daisy Chain
		Connecting devices and noise sources to separate earth electrodes	Connecting devices and noise sources to a common earth electrode	
The cable shield connected to the connector hood at both ends of the communications cable	Recommended	Recommended	Not recommended	Not recommended
EtherNet/IP not used	Recommended	Recommended	Not recommended	Not recommended

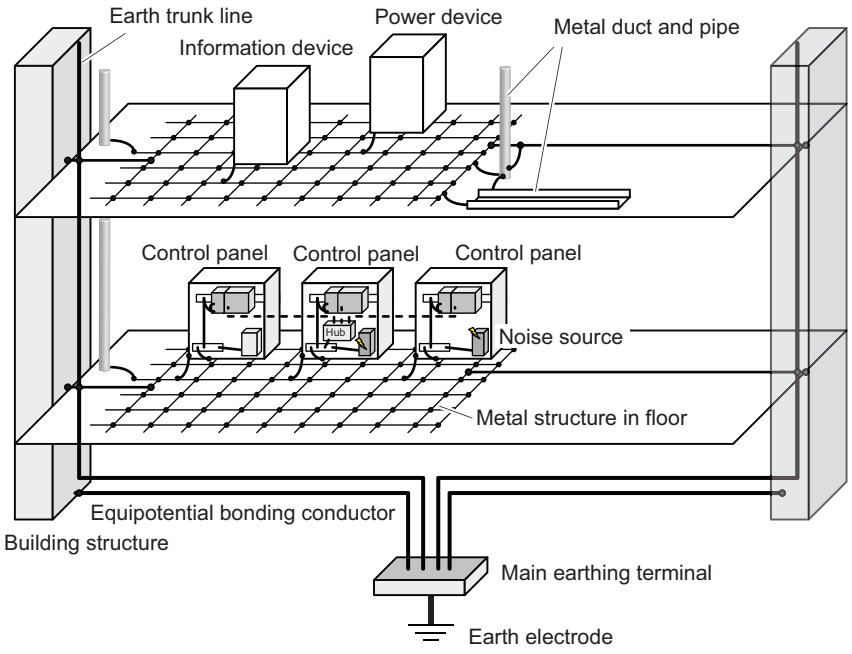
Additional Information

- In countries or regions where earthing methods are regulated, you must comply with the regulations. Refer to the applicable local and national ordinances of the place where you install the system, or other international laws and regulations.
- Ethernet switches are used with the EtherNet/IP. For information on the environmental resistance of the Ethernet switch to use, the grounding between Ethernet switches, or the specifications of cables, ask the Ethernet switch manufacturer.

Equipotential Bonding System

Equipotential bonding is an earthing method in which steel frames and building structures, metal ducts and pipes, and metal structures in floors are connected together and make connections to the earth trunk line to achieve a uniform potential everywhere across the entire building. We recommend this earthing method.

The following figure shows an example of an equipotential bonding system.
Connect the main earthing terminal and building structures together with equipotential bonding conductors and embed the mesh ground line in each floor.
Connect the ground line of each control panel to the equipotential bonding system.

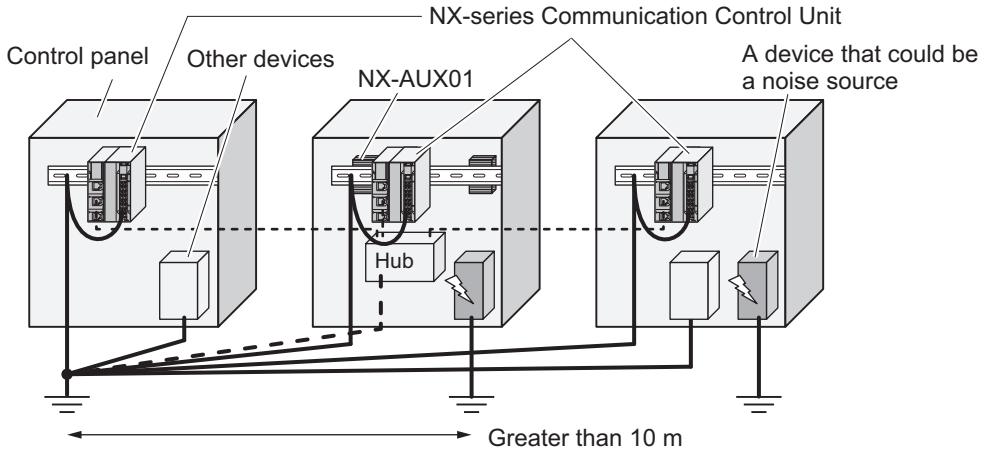


Star Earthing

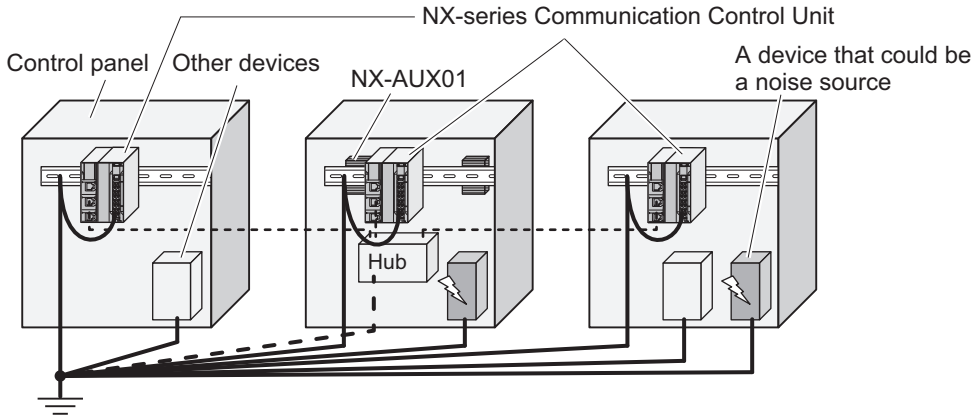
If the earthing method used for the building is not equipotential bonding or the earthing system is unknown, choose (a) from the earthing methods given below.

a. Installation method by connecting devices and noise sources to separate earth electrodes
This is an earthing method to separately ground an earth electrode of the device that is connected with a communications cable or other devices and an earth electrode of a high-power device that could be a noise source, such as a motor or inverter. Each earth electrode must be ground to 100 Ω or less.

Connect the ground lines of the device that is connected with a communications cable and other devices as a bundle to a single earth electrode. Be sure that the earth electrode is separated by a minimum of 10 m from any other earth electrode of a device that could be a noise source.

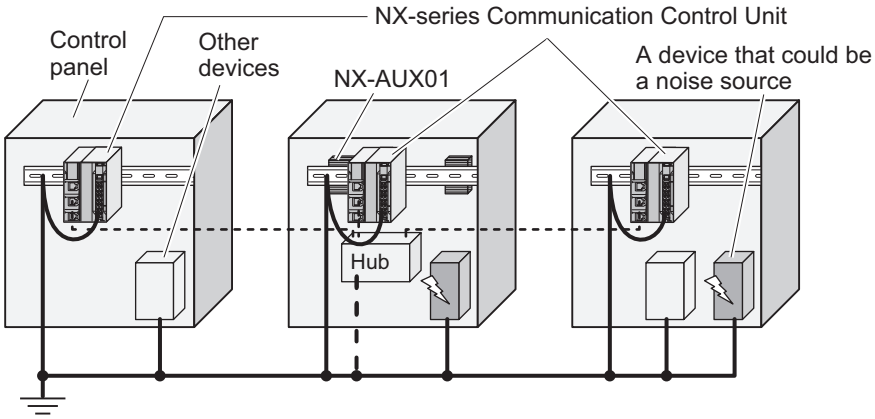


b. Installation method by connecting devices and noise sources to a common earth electrode
This is an earthing method to connect the device that is connected with a communications cable, other devices, and a device that could be a noise source, to a common earth electrode. This earthing method is not recommended, because the device that is a potential noise source may interfere electromagnetically with other devices.



● Daisy Chain

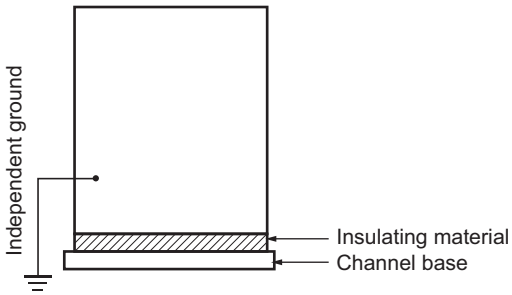
This is an earthing method to connect the device that is connected with a communications cable, other devices, and a device that could be a noise source using a daisy-chain topology to a common earth electrode.
This earthing method is not recommended because the device that could be a noise source may interfere electromagnetically with other devices.



Precautions for Grounding

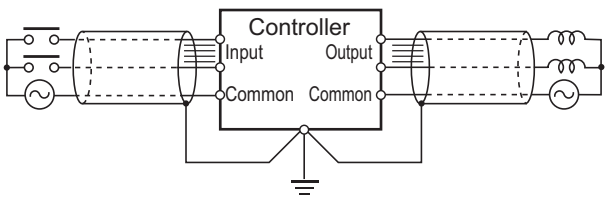
● General Precautions

- To prevent electrical shock, do not connect devices to ground poles (or steel frames) with non-equalized potential to which multiple devices are connected.
- Use a ground pole as close to the Controller as possible and keep the ground line as short as possible.
- If the same ground is used for both the signal lines and the enclosure, isolate the channel base (a metal plate inside a grounded control panel) with an insulating material.
  Refer to *Isolating the CPU Rack from the Control Panel* on page 5-38 for how to isolate the CPU Rack of a Communication Control Unit.



Example: Insulating and Grounding an Enclosure

- If high-frequency equipment is present, then ground not only the high-frequency equipment but also the panel itself in which the Controller is housed.
- As shown in the following diagram, when using shielded cable for I/O wiring, connect the shield near the Controller to the enclosure ground terminal.
  Follow the instructions in the Communications Unit manual for preparing shielded communications cables.



Shielded Cable Ground

Controller Ground Terminals

The Controller has the following ground terminal.

Grounding type	Symbol	Connection
Functional Grounding		Ground this terminal when power supply noise causes malfunctioning.

When the functional ground terminal is correctly grounded, it is generally effective in suppressing power supply common noise. Occasionally, however, grounding this terminal will result in picking up more noise, so be careful when using it.

6

Safety Network Controller Operation

This section provides information that is necessary to use the Safety Network Controller, including how the Safety Network Controller works.

6-1 Overview of the Safety Network Controller Operation 6-2
6-1-1 Introduction to FSoE Communications 6-2
6-1-2 Introduction to Communications between NX Units 6-3
6-1-3 Introduction to CIP Safety Communications 6-3
6-1-4 Introduction to Tag Data Links 6-4
6-1-5 Calculating the Number of Connections 6-9

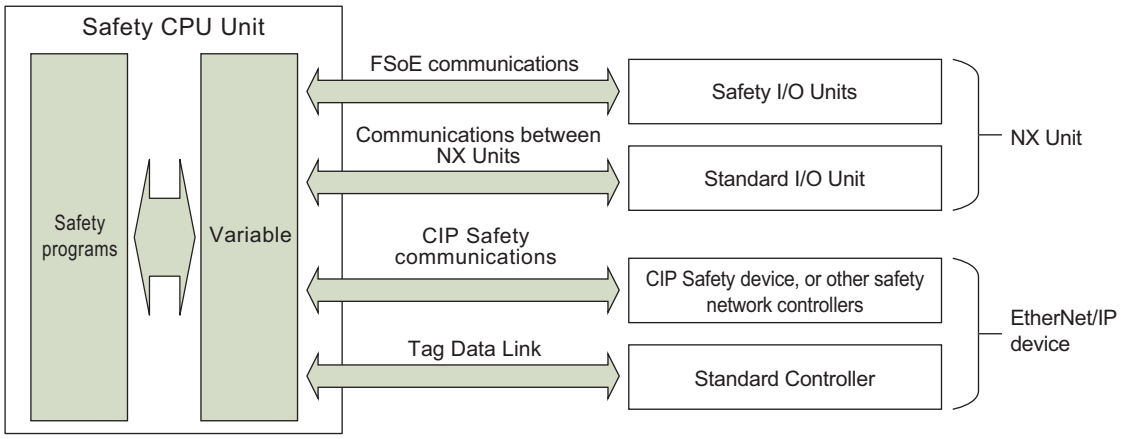
6-2 I/O System 6-14
6-2-1 Relationship between the Types of Signals and the Types of Communications 6-14
6-2-2 Safety Data Types and Standard Data Types 6-14
6-2-3 Specifying Safety Data Types and Standard Data Types 6-15

6-3 Safety I/O Function 6-16
6-3-1 Safety Input Function 6-16
6-3-2 Safety Output Function 6-38

6-1 Overview of the Safety Network Controller Operation

This section describes an overview of the Safety CPU Unit operation.

A Safety CPU Unit executes safety programs and performs I/O refreshing to achieve safety controls. The Safety CPU Unit accesses the data for I/O refreshing through variables and executes the safety programs. It also performs I/O refreshing with "safety process data communications" and "standard process data communications".

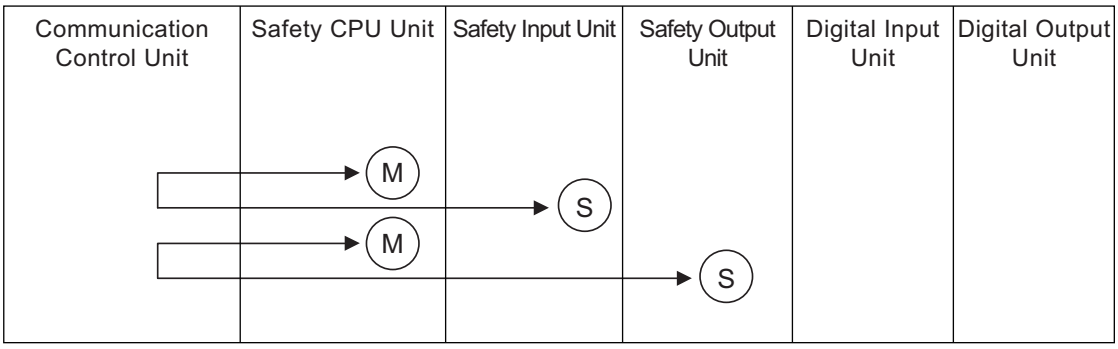


The following table shows the relationship between the connected devices and the communications types.

Communications type		Description
Safety process data communications	FSoE communications	Safety communications with NX Units on the CPU Rack. This is used for communications with the Safety I/O Units.
	CIP Safety communications *6-1 Overview of the Safety Network Controller Operation* on page 6-2	Safety communications with the CIP Safety devices on the EtherNet/IP network. This type is used for communications with the Safety I/O terminals or other Safety Network Controllers.
Standard process data communications	Communications between NX Units	Standard communications with the NX Unit on the CPU Rack. This is used for communications with the NX Unit including Digital I/O Units.
	Tag data links	Standard communications with the EtherNet/IP devices on the EtherNet/IP network. This is used for communications with standard controllers.

6-1-1 Introduction to FSoE Communications

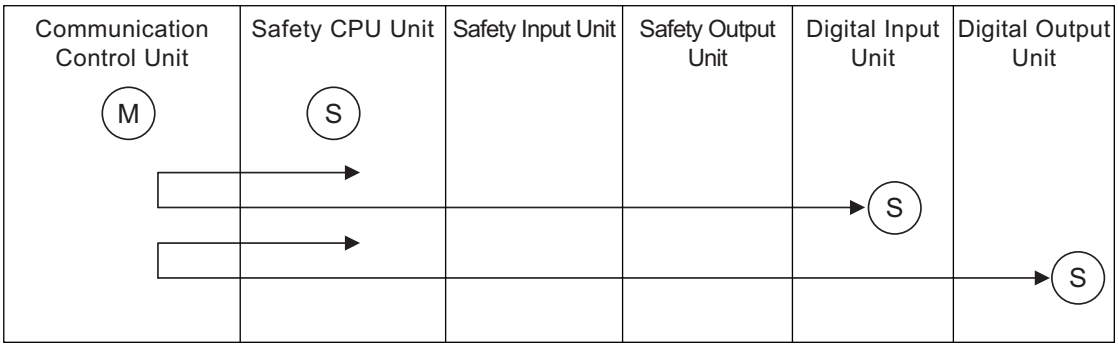
FSoE communications exchange data cyclically between the Safety CPU Unit and the Safety I/O Unit on the CPU Rack. The Safety CPU Unit works as an FSoE master and requests Safety I/O Units as the FSoE slaves, to open an FSoE connection. The Communication Control Unit relays the FSoE communications between the Safety CPU Unit and the Safety I/O Unit.



M: FSoE Master
S: FSoE Slave

6-1-2 Introduction to Communications between NX Units

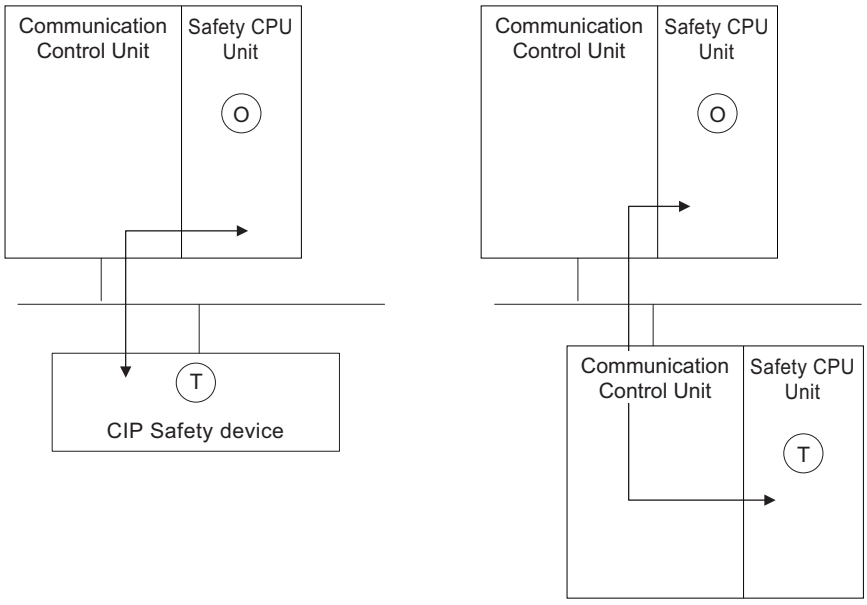
In communications between NX units, data is cyclically exchanged between the Safety CPU Unit and the standard I/O Unit. The Communication Control Unit works as an NX bus master and exchanges data between the Safety CPU Unit (as an NX bus slave) and the standard I/O Unit. Exposed variables of the Safety CPU Unit are used for the data exchange.



M: NX Bus Master
S: NX Bus Slave

6-1-3 Introduction to CIP Safety Communications

CIP Safety communications exchange data cyclically between the Safety CPU Unit and the Safety I/O Terminal, or between the Safety CPU Units. The Safety CPU Unit works as a CIP Safety originator and requests the Safety I/O Terminal as a CIP Safety target, to open a CIP Safety connection. In addition, the Safety CPU Unit can work as a CIP Safety target to publish its dataset to other Safety CPU Units. The Communication Control Unit relays the CIP Safety communications between the Safety CPU Unit and the Safety I/O Terminal, or between the Safety CPU Units.



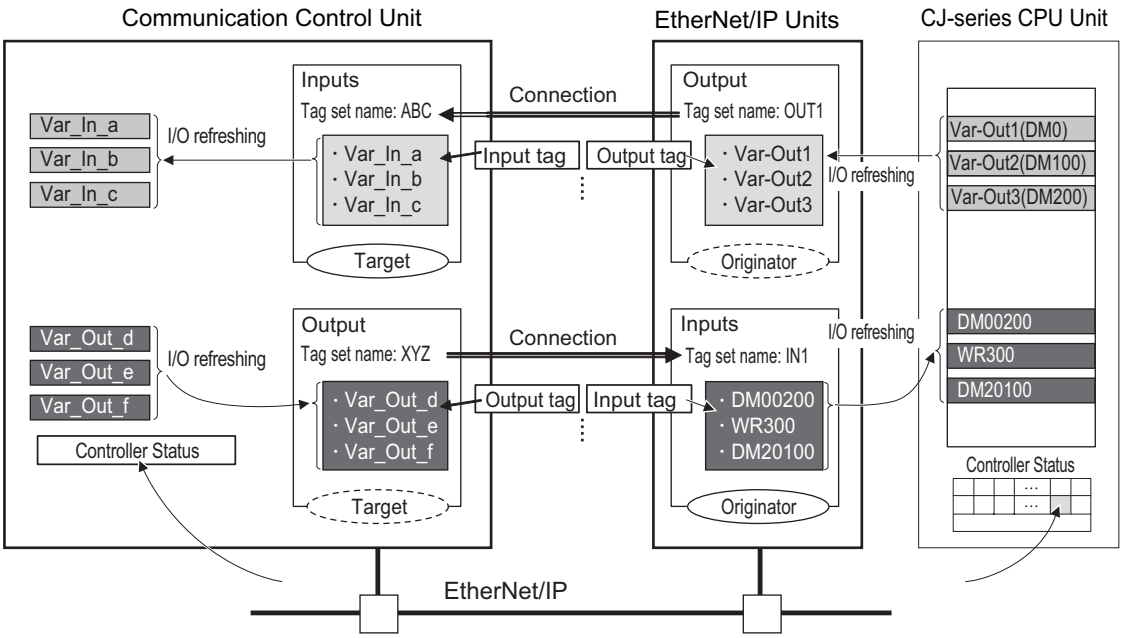
O: CIP Safety Originator
T: CIP Safety Target

6-1-4 Introduction to Tag Data Links

Tag Data Links

Tag data links enable cyclic tag data exchanges on an EtherNet/IP network between Controllers or between Controllers and other devices. Variables are assigned to tags.
The settings for tag data links are made with the Sysmac Studio. For the details on the settings, refer to *7-4-2 Setting Tag Data Links* on page 7-17.

With a tag data link, one node requests the connection of a communications line to exchange data with another node.
The node that requests the connection is called the originator, and the node that receives the request is called the target.



Connection information is set in the EtherNet/IP port of the Controller which is assigned as an Originator.

The output words and input words for each node for which data is exchanged must be set in the connection information. These words are called the output tag set and input tag set. A tag set must specify at least one tag.
The size of data for data exchange is the total size of tags included in the tag set. The size of the output tag set and the size of the input tag set must match.

Data Link Data Areas

● Tags

A tag is a unit that is used to exchange data with tag data links.
Data is exchanged between the local network variables and remote network variables as specified in the tags.

● Tag Sets

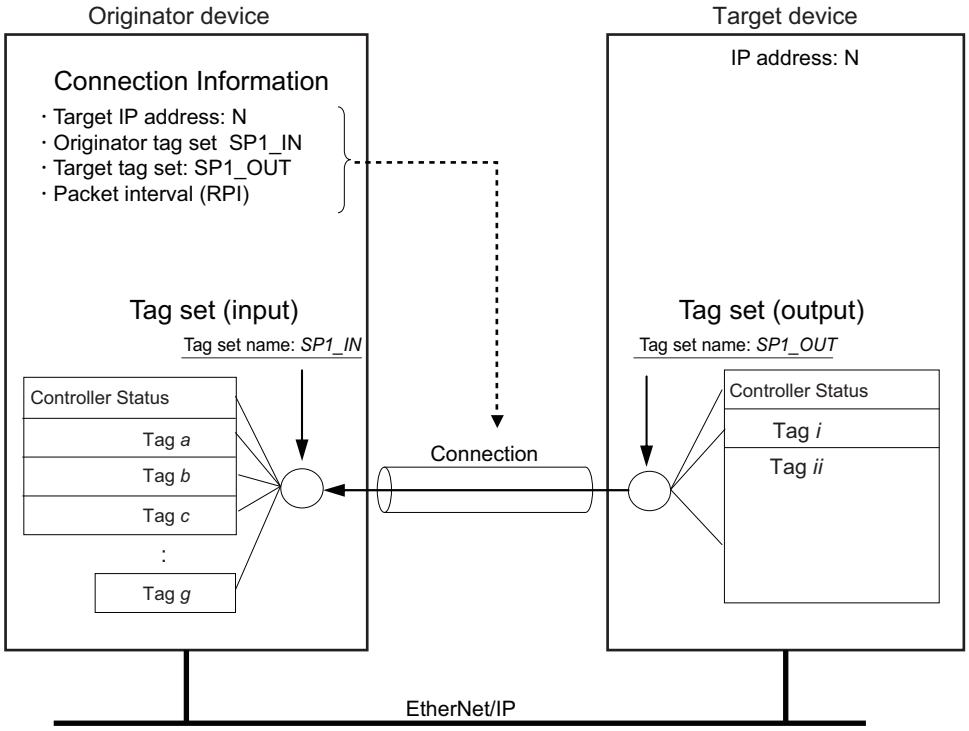
When a connection is established, 1 to 32 tags including Controller status are collected as a set of tags. This is called a tag set. Each tag set represents the data that is linked for a tag data link connection.
Tag data links are therefore created through a connection between one tag set and another tag set.
A tag set name must be set for each tag set.
Note A tag set is a unit of data exchange which allows to maintain the data concurrency.

Precautions for Correct Use

Data with tags is exchanged in the order that the tags are registered in the tag set. Register the tags in the same order of the input and output tag sets.

Example

In the following example, input tags "a" to "g" at the originator are a tag set named *SP1_IN* and output tags "I" and "ii" are a tag set named *SP1_OUT*. A connection is set between these two tag sets.



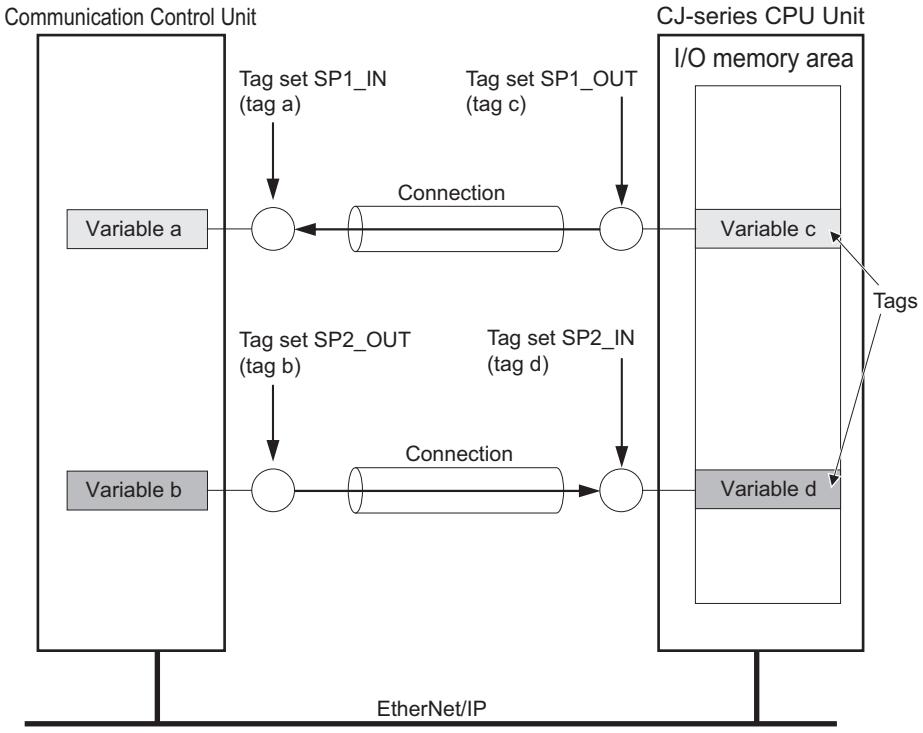
There are input (consume) and output (produce) tag sets. Each tag set can contain either input tags or output tags. The same input tag cannot be included in more than one input tag set.

Number of Tags in Tag Sets

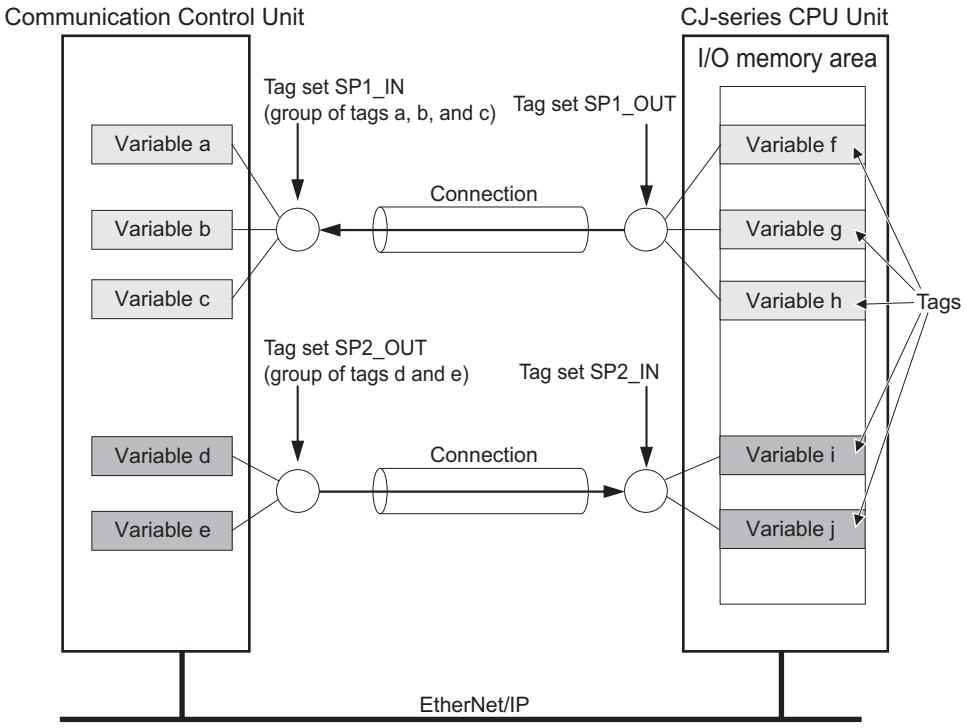
You can set any tag sets containing one or more tags for the input and output tag sets for one connection.

For example, you can set a tag set with one tag for the input tag set and set a tag set with more than one tag for the output tag set.

- Tag Set with Only One Tag Each
  Each tag set contains only one tag.



- Tag Sets Each with Multiple Tags
  As shown below, tags can be grouped. You can place up to 32 tags in one tag set.



Note To enable a connection, each tag set must include only input tags or only output tags. (Both input and output tags cannot be included in the same tag set.)

Connection Setting Parameters

The connection settings have the following setting parameters.

- Setting the Requested Packet Interval (RPI)
  The RPI (Requested Packet Interval) is the I/O data refresh cycle on the Ethernet line when tag data links are established. With EtherNet/IP, data is exchanged on the communications line at the RPI that is set for each connection, regardless of the number of nodes.
  With the built-in EtherNet/IP port, you can set RPI for each connection.

- Setting Multi-cast and Unicast Communications
  You can select a multi-cast connection or unicast (point-to-point) connection as the connection type in the tag data link connection settings.
  With a multi-cast connection, you can send an output tag set in one packet to multiple nodes and make allocations to the input tag sets.
  A unicast connection separately sends one output tag set to each node, and so it sends the same number of packets as the number of input tag sets.
  Therefore, multi-cast connections can decrease the communications load if one output tag set is sent to multiple nodes.
  To use a multi-cast connection and send an output tag set in one packet to multiple nodes, the following settings for the receiving node must be the same as the settings of the sending node: the connection type (multi-cast), the connection I/O type, requested packet interval (RPI), and timeout value.

Precautions for Correct Use

- The performance of communications devices is limited to some extent by the limitations of each product's specifications. Consequently, there are limits to the requested packet interval (RPI) settings.
  Refer to *Section 11 Communications Load* on page 11-1, and set an appropriate requested packet interval (RPI).
- If multi-cast connections are used, however, use an Ethernet switch that has multi-cast filtering, unless tag set is received by all nodes in the network.
  If an Ethernet switch without multi-cast filtering is used, multi-cast packets are broadcast to the entire network, and so the packets are sent to nodes that do not require them, which will cause the communications load on those nodes to increase.
- If you use tag data links with multi-cast traffic at a baud rate over 100 Mbps, use an Ethernet switch that supports a baud rate of 1000 Mbps.
  If there is an Ethernet device on the same network that communicates at 100 Mbps or less, the device may affect tag data link communications and cause tag data links to be broken, even if the device is not related to tag data link communications.

Additional Information

If the maximum number of connections is exceeded, you must review the number of connections for the built-in EtherNet/IP port, or the number of nodes.

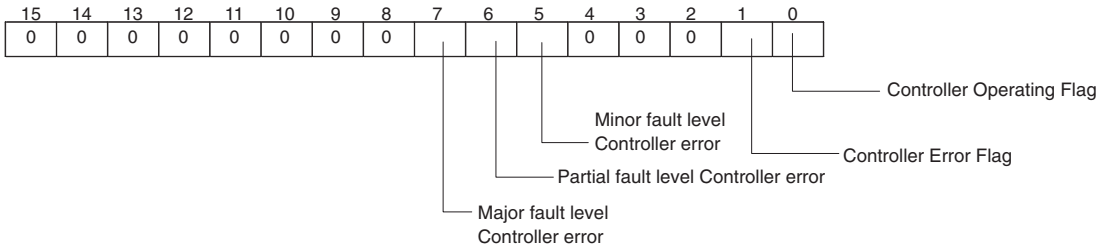
Starting and Stopping Tag Data Links

Tag data links are automatically started when the data link parameters are downloaded from the Network Configurator and the power supply to the Communication Control Unit is turned ON.

Thereafter, you can start and stop tag data links for the entire network or individual devices from the Network Configurator. Starting and stopping tag data links for individual devices must be performed for the originator.

Controller Status

You can include the Controller status as a member of a tag set in the data sent and received.
The Controller status is a set of flags that indicate the operating status of the Communication Control Unit such as operating information, error information, and Controller error level.
If the Controller status is specified as an output (send) tag, the Controller status is added to the start of the tag set in the following format.
(Select the **Include** Option for the **Controller Status** in the upper right of the **Edit Tag Set** Dialog Box.)



Note Of the flags in bits 5 to 7 that indicate the current error level, only the flag for the highest error level changes to TRUE.
For example, if a minor fault level Controller error and a major fault level Controller error occur at the same time, only the flag for the major fault level Controller error (bit 7) will change to TRUE and the flag for the minor fault level Controller error (bit 5) will remain as FALSE.

To receive the Controller status, specify the Controller status for the In - Consume Tab Page in the dialog box used to edit the receive tag set.
(Select the **Include** Option for the **Controller Status** in the upper right of the **Edit Tag Set** Dialog Box.)

6-1-5 Calculating the Number of Connections

● Calculating the Number of Safety I/O Connections for the Safety CPU Unit

You must specify the total number of CIP Safety originator connections, CIP Safety target connections, and FSoE master connections, which must be set within the number of safety I/O connections that you can set for the Safety CPU Unit. You cannot set the number that exceeds the number of safety I/O connections that you can set.

Precautions for Correct Use

There is a restriction on the data size that can be communicated between the Safety CPU Unit and the NX Bus Master, as well as the restrictions on the number of Safety I/O connections. This data size includes exposed variables. You can check the usage on the Memory Usage Tab Page of the Sysmac Studio.

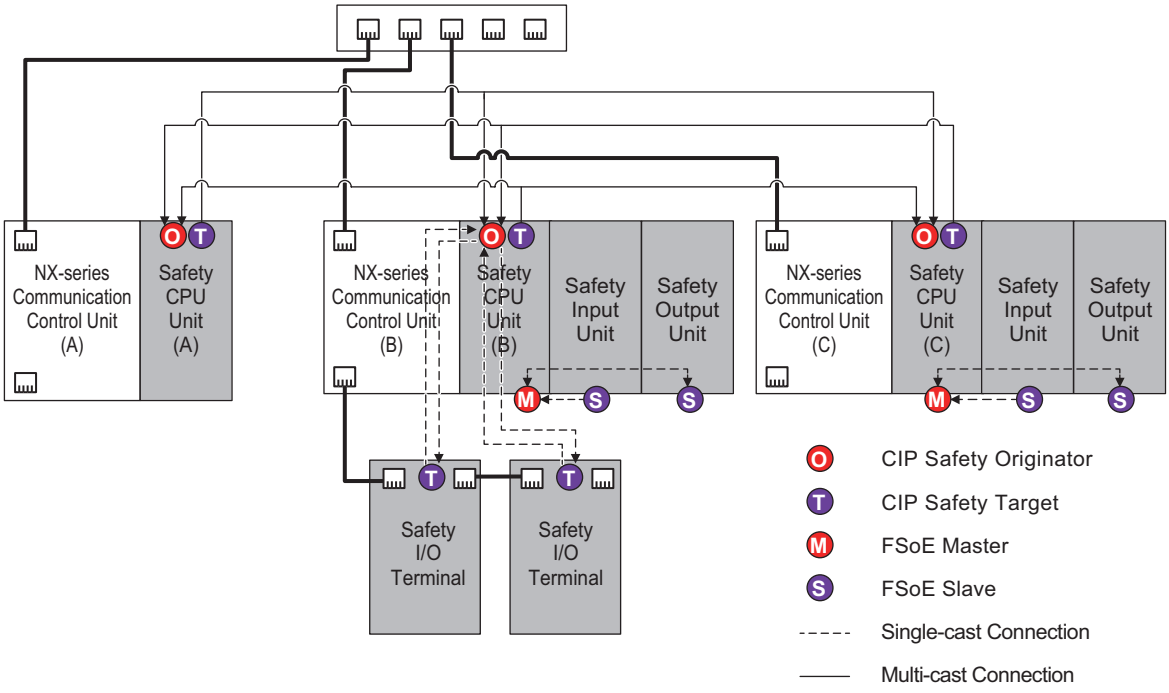
- Counting the Number of CIP Safety Originator Connections

For the CIP Safety originator connections, you can establish a unidirectional input or output communication with a CIP Safety target per connection. Two connections are used to establish bidirectional input and output communications.

- Counting the Number of CIP Safety Target Connections
  CIP Safety target connections have the single-cast connection and the multi-cast connection.
  For the single-cast connection, you can establish a unidirectional input or output communication with a CIP Safety originator per connection. Two connections are used to establish bidirectional input and output communications.
  For the multi-cast connection, you can establish a unidirectional input communication with multiple CIP Safety originators per connection.

- Counting the Number of FSoE Master Connections
  For the FSoE master connections, you can establish bidirectional input and output communications with a FSoE slave per connection.

- Example of Calculating the Number of Safety I/O Connections
  A calculation example of using the combination of the NX-series Communication Control Units and Safety CPU Units is given below.



	Number of CIP Safety originator connections (X)	Number of CIP Safety target connections (Y)	Number of FSoE master connections (Z)	Total (X+Y+Z)
Safety CPU Unit (A)	2	1	0	3
Safety CPU Unit (B)	6	1	2	9
Safety CPU Unit (C)	2	1	2	5

Calculating the Number of Routable CIP Safety Connections for the Communication Control Unit

You must specify the total number (m+n) of targets that establish connections as an originator (m) and originators that establish connections as a target (n), which must be set within the maximum number of routable CIP Safety connections for the Communication Control Unit. If you set the number that exceeds the maximum number of routable CIP Safety connections, the *CIP Safety Originator Connection Not Established Error* (80310000 hex) will occur. In addition, if the total number of CIP Safety originator connections and CIP Safety target connections exceeds the number of routable CIP Safety connections, you cannot perform the connection settings.

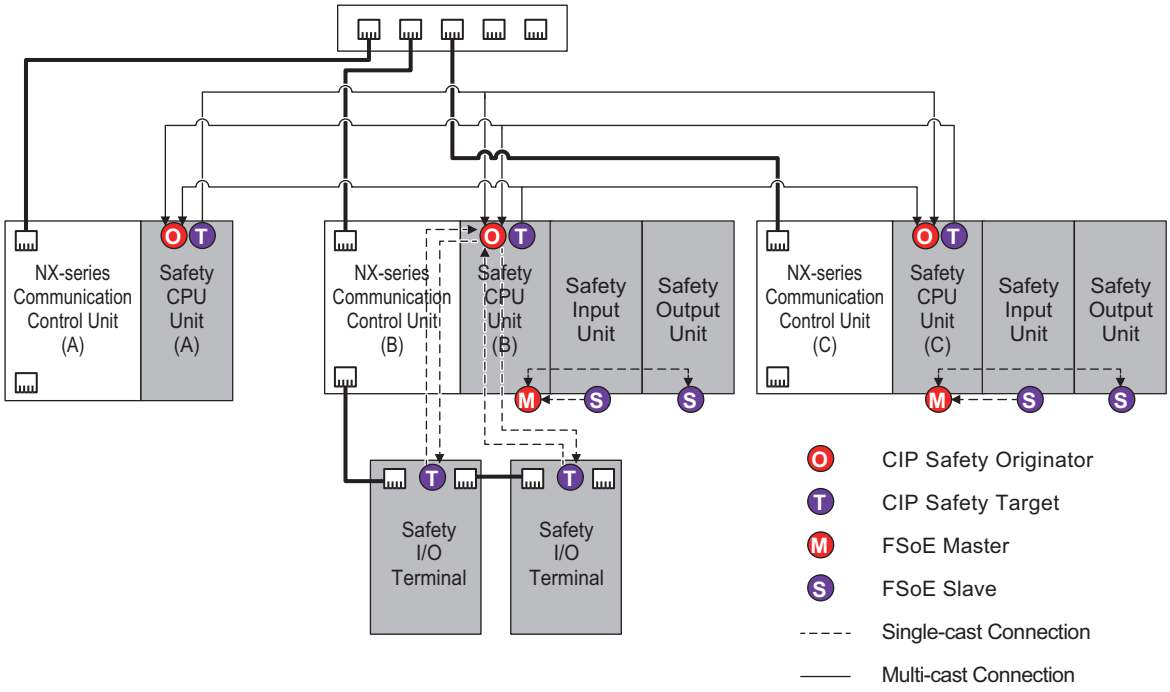
If a multi-cast connection is opened for multiple CIP Safety originators and connections, the number of originators that establish connections as a target becomes the number of CIP Safety originators.

If more than one single-cast connection is established for a CIP Safety target device, the number of targets that have established connections as an originator is equal to the number of single-cast connections.

Additional Information

The maximum number of total routable CIP Safety connections for a Communication Control Unit is 254. For multi-cast connections, the maximum number is 128.

- Example of Calculating the Maximum Number of Routable CIP Safety Connections
  A calculation example of using the combination of the NX-series Communication Control Units and Safety CPU Units is given below.



	Number of targets that establish connections as an originator (m)	Number of originators that establish connections as a target (n)	Total (m +n)
Communication Control Unit (A)	2*1	2*1	4*2
Communication Control Unit (B)	6*1	2*1	8*2
Communication Control Unit (C)	2*1	2*1	4*2

*1. Two multi-cast connections are included in this number.
*2. Four multi-cast connections are included in this number.

● Calculating the Number of Tag Data Link Connections for the Communication Control Unit

You need to specify the total number of connections consisting of the originator connections opened by the own node and the target connections opened by the originator, which needs to be within the maximum number of connections that can be configured.

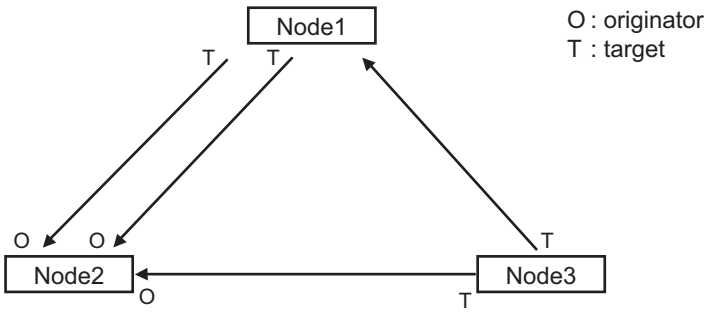
Example:

Node 1 has established two (target) connections with Node 2 and one (originator) connection with Node 3. Therefore, the total number of connections is 3.

Node 2 has established two (originator) connections with Node 1 and one (originator) connection with Node 3. Therefore, the total number of connections is 3.

Node 3 has established one (target) connection with Node 1 and one (target) connection with Node 2. Therefore, the total number of connections is 2.

In either case, you will be able to establish connections because the number of connections is within the maximum number of connections that can be configured for the built-in EtherNet/IP.

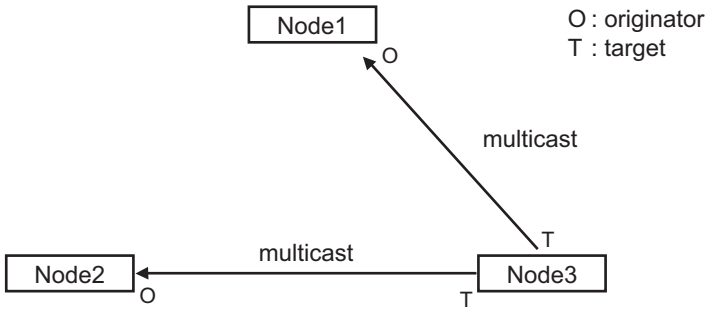


Note that multi-cast will consume the bandwidth corresponding to the number of connections even though only one packet is transmitted.

Example:

Node 3 is transmitting one multi-cast packet to Node 1 and Node 2, respectively. In this case, Node 3 has established two connections total: one (target) connection with Node 1 and one (target) connection with Node 2.

Note that the number of connections is same for multi-cast and unicast, whichever you specify.

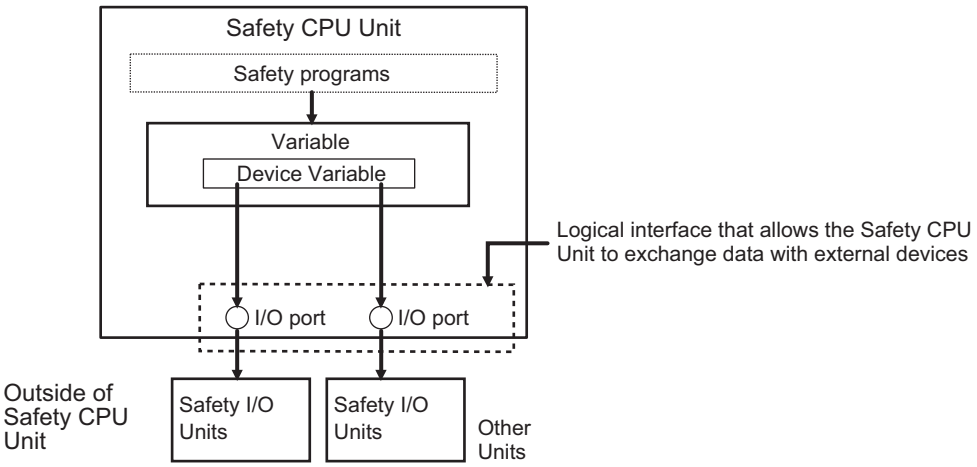

Node1
O : originator
T : target
O
multicast
T
multicast
Node2
Node3
O
T

6-2 I/O System

This section describes how the Safety CPU Unit processes I/O with external devices such as Safety I/O Units.

When the Safety CPU Unit exchanges signals with Safety I/O Units and other external devices, it does so through logical interfaces that are called "I/O ports".

I/O ports are created automatically when you create the control configuration for safety controls on the Sysmac Studio and set up the safety process data communications.
You assign device variables to I/O ports to gain access to the external devices from the safety programs.



You can check the **I/O ports** in the **I/O Map** of the Sysmac Studio.

6-2-1 Relationship between the Types of Signals and the Types of Communications

The safety control system uses the communications that are described below to process all I/O with safety inputs, safety outputs, standard inputs, standard outputs, and standard controls.

- The exchange of signals with safety inputs and safety outputs is done with safety process data communications.
- The exchange of standard signals with safety inputs, safety outputs, and standard controllers is done with standard process data communications.

6-2-2 Safety Data Types and Standard Data Types

In this safety control system, the data type of a variable determines whether a signal is related to the safety controls. Broadly speaking, there are the following two data types: safety data types and standard data types.

Safety Data Type Variables

A safety data type variable is a variable that specifies data that is related to safety controls.

The names of safety data type variables have the word *SAFE* appended to a *standard data type name* such as *SAFEBOOL*.
Refer to *8-2-5 Data Type* on page 8-14 for details on the safety data types.

Standard Data Type Variables

These variables represent data that is not related to safety controls.
Refer to *7-8 Exposing Variables to Standard Controllers* on page 7-53 for details on how to access standard data type variables from the standard controllers.

Each type of signal is defined with a standard data type or safety data type as shown below.

Type of signal	Data type of variable to use
Outputs from safety control to standard control	Standard data type
Inputs from standard control to safety control	
Safety inputs from external devices	Safety data type
Safety outputs to external devices	
Standard inputs from external devices	Standard data type
Standard outputs to external devices	
Internal safety-related signals with no I/O with any external devices	Safety data type
Internal standard-related signals with no I/O with any external devices	Standard data type

6-2-3 Specifying Safety Data Types and Standard Data Types

The safety data type variables and standard data type variables are used depending on the type of communications.

- Signals that are input and output through safety process data communications must be defined as safety data type variables.
- Signals that are input and output through standard process data communications must be defined as standard data type variables.

6-3 Safety I/O Function

The following sections describe the safety I/O functions of the Safety I/O Units.

6-3-1 Safety Input Function

Connectable Input Devices

The Safety Input Unit diagnoses the connected external devices and other things through the safety input terminals.
The safety input devices and standard input devices that can be connected to the safety input terminals of the Safety Input Unit are listed in the following table.

Input device name	Type of input device	Type of contacts
Emergency stop switch	Device with mechanical contacts	Single channel Dual-channel equivalent input
Safety door switch	Device with mechanical contacts	Single channel Dual-channel equivalent input Dual-channel complementary input
Safety limit switch	Device with mechanical contacts	Single channel Dual-channel equivalent input Dual-channel complementary input
Two-hand switches	Device with mechanical contacts	Dual-channel complementary input
Safety key selector switch	Device with mechanical contacts	Single channel Dual-channel equivalent input Dual-channel complementary input
Enabling switch	Device with mechanical contacts	Dual-channel equivalent input
EDM feedback	Device with mechanical contacts	Single channel
Reset switch	Device with mechanical contacts, standard input	Single Channel with Test Pulse Single Channel without Test Pulse
Safety light curtain	Device with semiconductor output	Dual-channel equivalent input
Safety laser scanner	Device with semiconductor output	Dual-channel equivalent input
High-coded door switch	Device with semiconductor output	Dual-channel equivalent input

You can set the above parameters for the following general-purpose input devices.

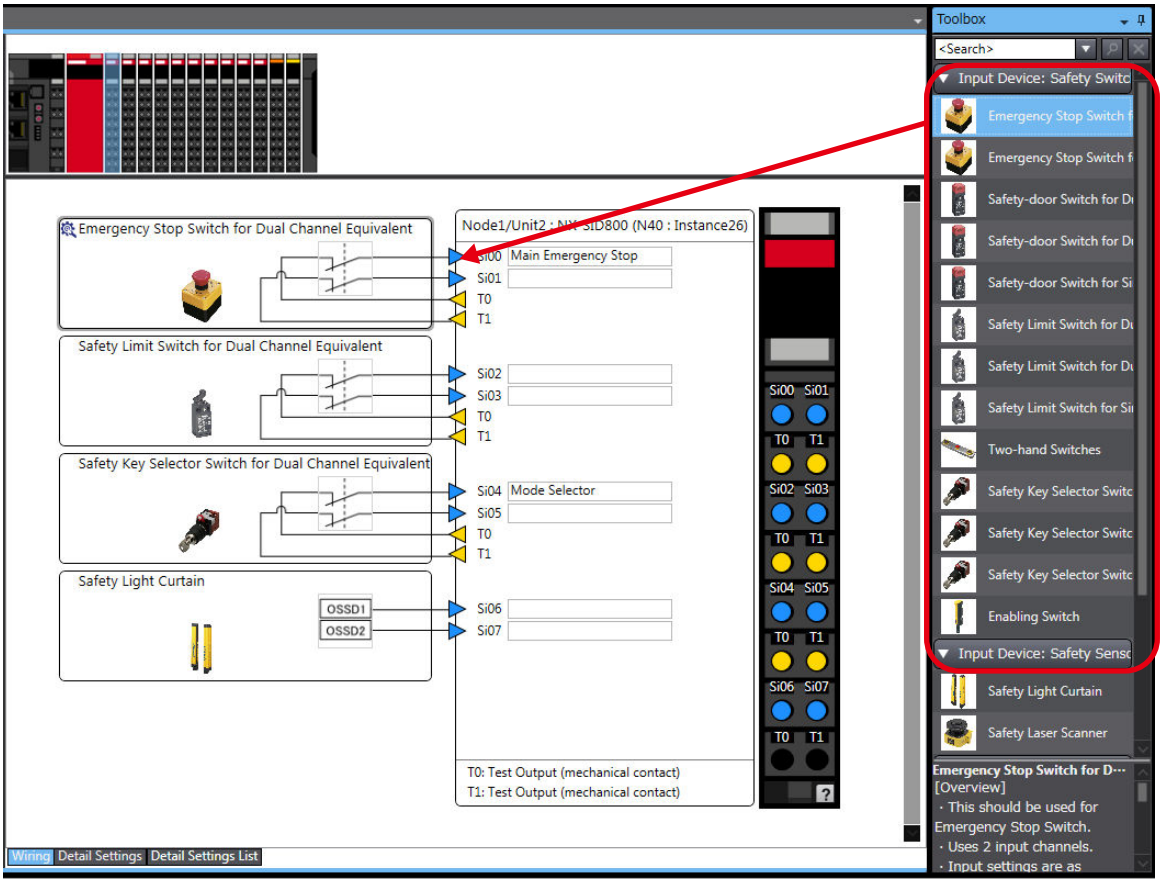
Type	Possible settings
Safety input devices with mechanical contacts • Mechanical Contact for Single Channel • Mechanical Contact for Dual Channel Equivalent • Mechanical Contact for Dual Channel Complementary	Emergency stop switch, safety door switch, safety limit switch, two-hand switches, safety key selector switch, Enabling switch, and EDM feedback
Safety input device with semiconductor output • Semiconductor Output for Single Channel • Semiconductor Output for Dual Channel Equivalent • Semiconductor Output for Dual Channel Complementary	Safety light curtain, safety laser scanner, and high-coded door switch

The following OMRON Special Safety Input Devices can be connected directly without a special controller. (This applies only to the NX-SIH400.)

Type	Examples	
OMRON Single-beam Safety Sensors	E3ZS and E3FS	* Conforms to Type 2 and PLc.
OMRON Non-contact Door Switches	D40A-2	* Conforms to PLe and Safety Category 4.
	D40Z	* Conforms to PLe and Safety Category 4.
	D40A	* Conforms to PLd and Safety Category 3.
OMRON Safety Mats	UM and UMA	* Conforms to PLd and Safety Category 3.
OMRON Safety Edges	SGE (4-wire connection)	* Conforms to PLd and Safety Category 3.

Setting Up Safety Functions

You can easily set the safety functions of the safety input terminals from the Sysmac Studio by selecting the types of external devices that are connected. Refer to the *6-3 Safety I/O Function* on page 6-16 for details.



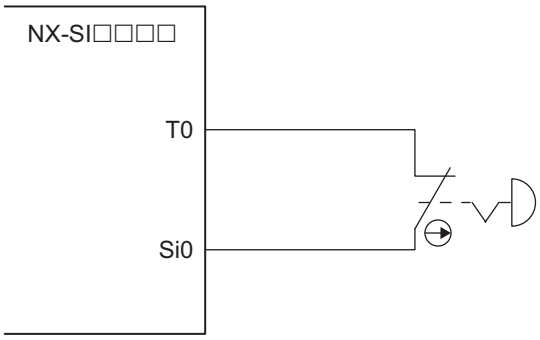
Connecting Input Devices

This section describes the connection methods for input devices.

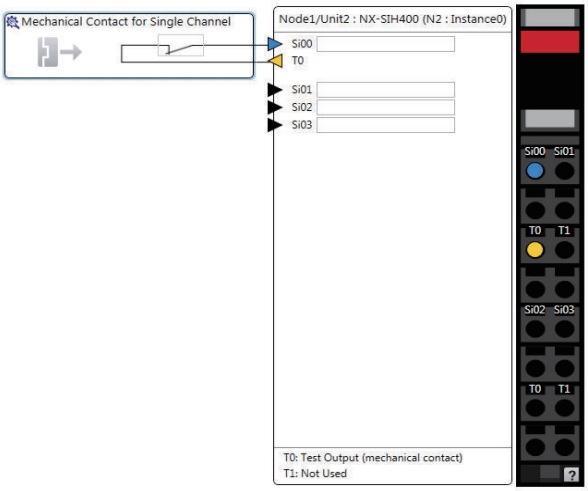
● Devices with Mechanical Contacts

A device with mechanical contacts, such as an emergency stop pushbutton or safety limit switch, is used with the safety input terminal (Si) and test output terminal (To).

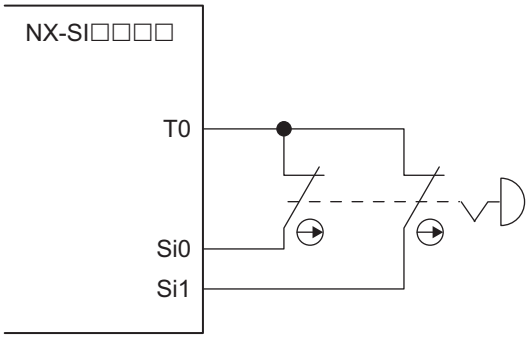
- Single-channel Input



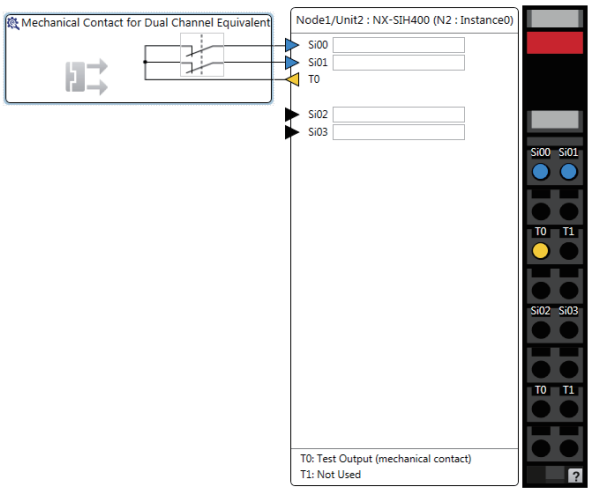
Example of Sysmac Studio Settings:



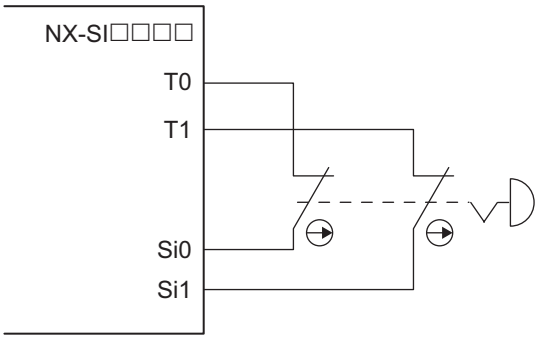
- Dual-channel Input When I/O Short Detection between Lines Is Not Required



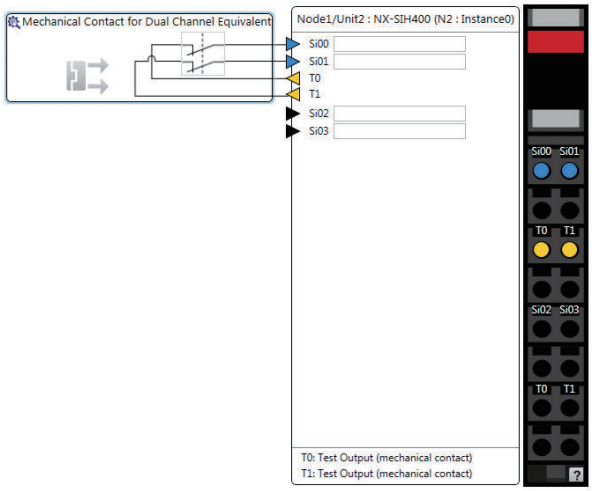
Example of Sysmac Studio Settings:



- Dual-channel Input When I/O Short Detection between Lines Is Required

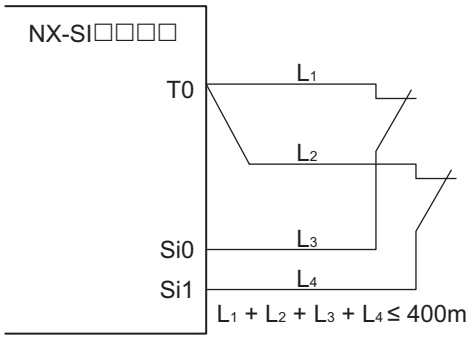


Example of Sysmac Studio Settings:



Precautions for Correct Use

- Configure dual-channel inputs with safety input terminals on the same Unit. It is not always possible to detect short circuits between safety input terminals on different Units.
- The total length of cable connected to one test output must be as follows:
  NX-SIH400 and NX-SID800: 400 m max.

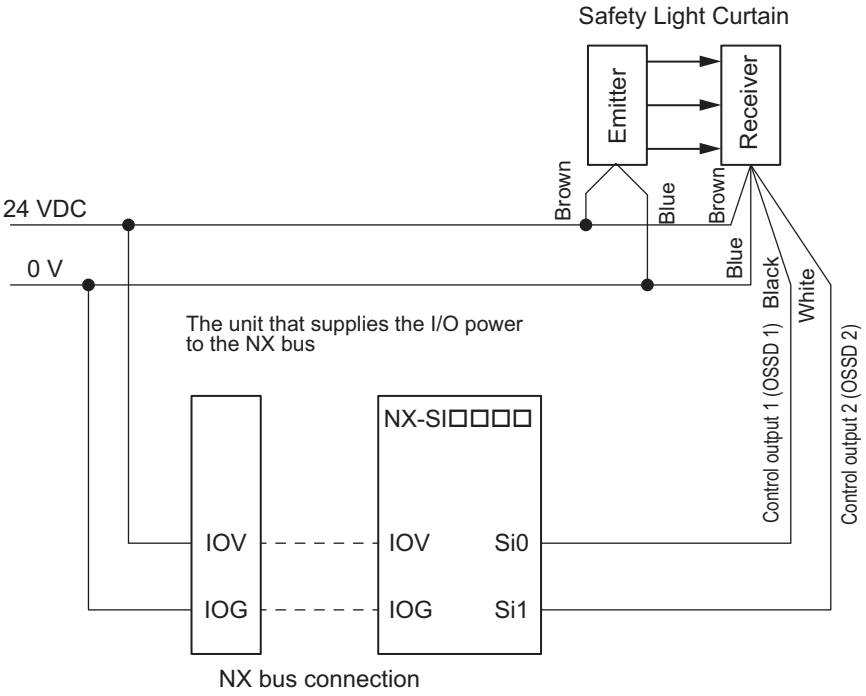


Additional Information

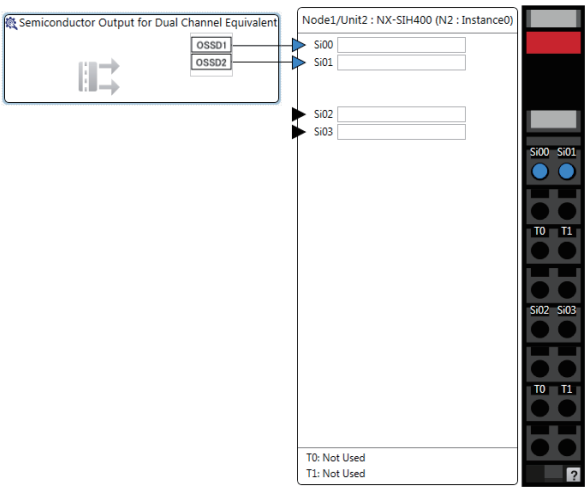
You can detect short-circuits between two input channels with the following methods:
- Dual-channel equivalent input: "With Test Pulse"
- Dual-channel complementary input: "Without Test Pulse" and "With Test Pulse"

● Devices with Semiconductor Outputs

The signal from a device with a semiconductor output, such as a light curtain, is input to a safety input terminal (Si).



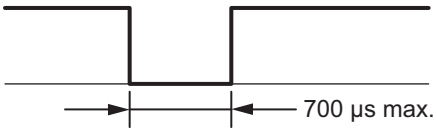
Example of Sysmac Studio Settings:



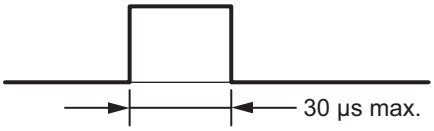
Precautions for Correct Use

Safety devices with semiconductor outputs, such as safety light curtains, sometimes provide a pulse output that is used to detect wiring errors. Observe the following when connecting a Safety Device with a semiconductor output to a safety input terminal.

- OFF pulse width when semiconductor output is ON: 700 μs max.



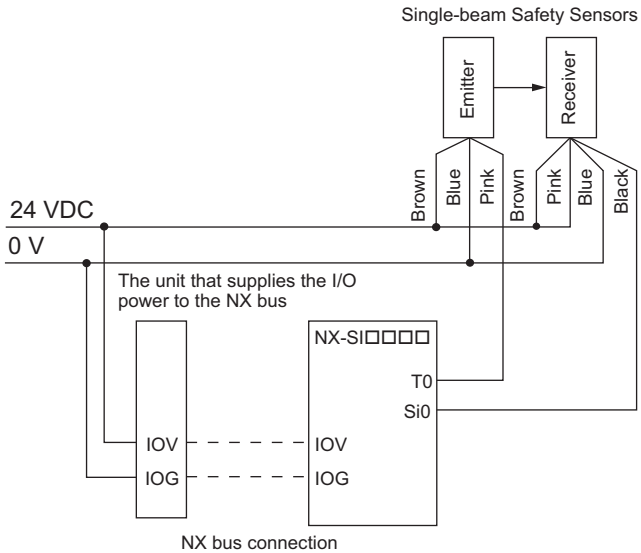
- ON pulse width when semiconductor output is OFF: 30 μs max.



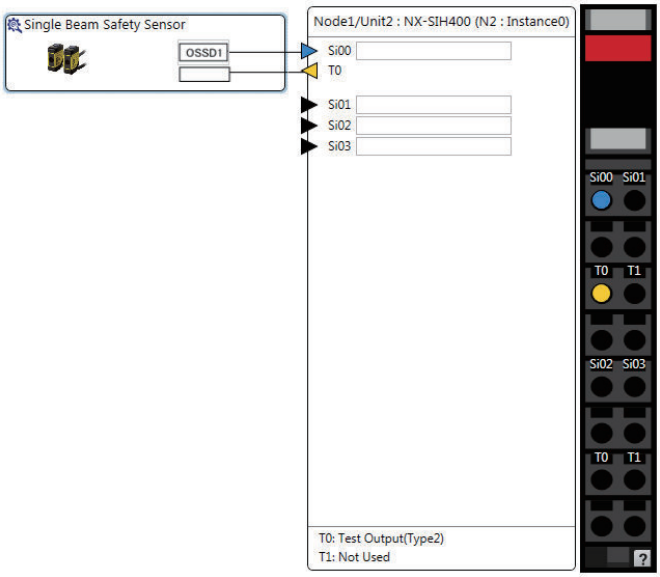
Check the specifications of the connected device for the maximum cable length.

● E3ZS/E3FS Single-beam Safety Sensors

An OMRON E3ZS/E3FS Single-beam Safety Sensor is connected as shown in the following figure.

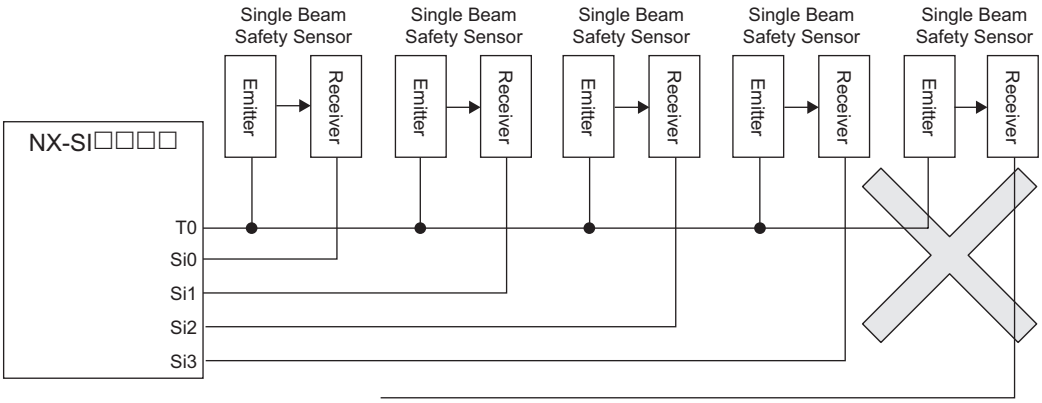


Example of Sysmac Studio Settings:

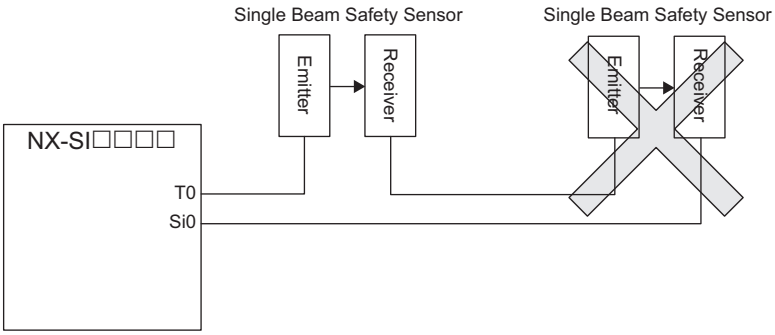


Precautions for Correct Use

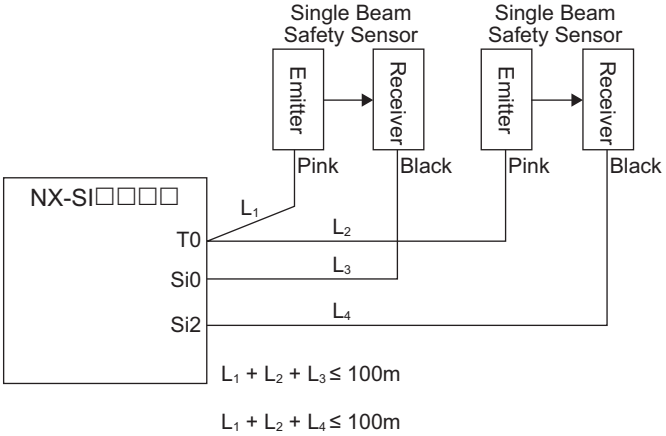
- The maximum number of connections per Unit is as follows:
  NX-SIH400: 4
- You can branch the connections to up to four Single-beam Safety Sensors for each test output.



- Series connections are not possible.



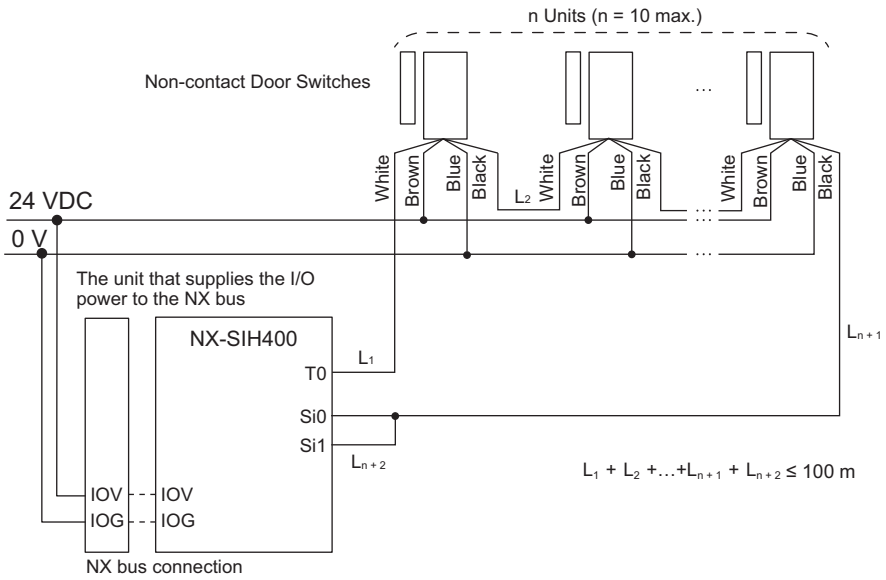
- The total wiring length for the E3ZS/E3FS Single-beam Safety Sensors is 100 m max.



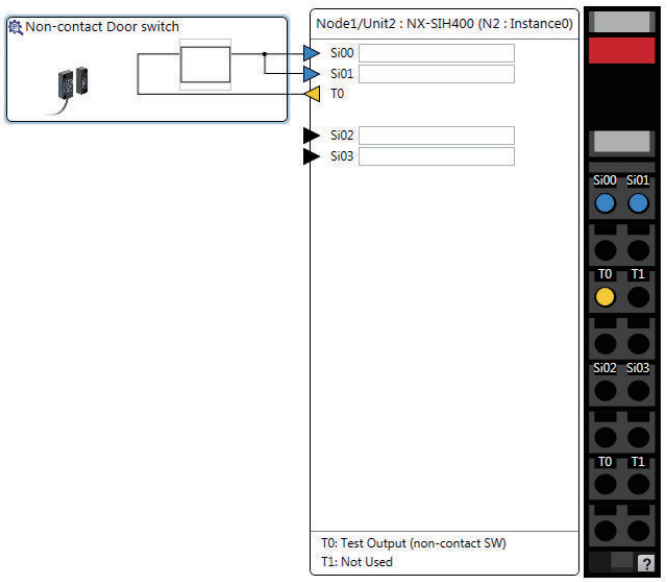
- The E3ZS/E3FS Single-beam Safety Sensor can be used in a Type 2 or lower or PLc or lower application. It cannot be used in a Type 3 or higher, or PLd or higher application.
- If you use more than one Single-beam Safety Sensor, it may not always be possible to detect shorts between wires. Therefore, to satisfy safety category 2, the cables must be protected from external damage for connections to single beam safety sensors. Use ducts or separate cables for each system to protect the cables from external damage when you connect the Single-beam Safety Sensors. You can also use special XS2F Cables for protection.
- The test period for a Single-beam Safety Sensor is 1,200 ms.
  Use this value for reference to determine the standard compliance of your system.

● D40A-2/D40A/D40Z Non-contact Door Switches

The non-contact door switch output (black line) from the OMRON D40A-2, D40A or D40Z Non-contact Door Switch is input to a safety input terminal. This is a one-line signal. When connecting it, branch it as shown at Si0 and Si1 in the following figure. Only one test output terminal is used. Connect the D40A-2, D40A or D40Z Non-Contact Door Switch input (white line).

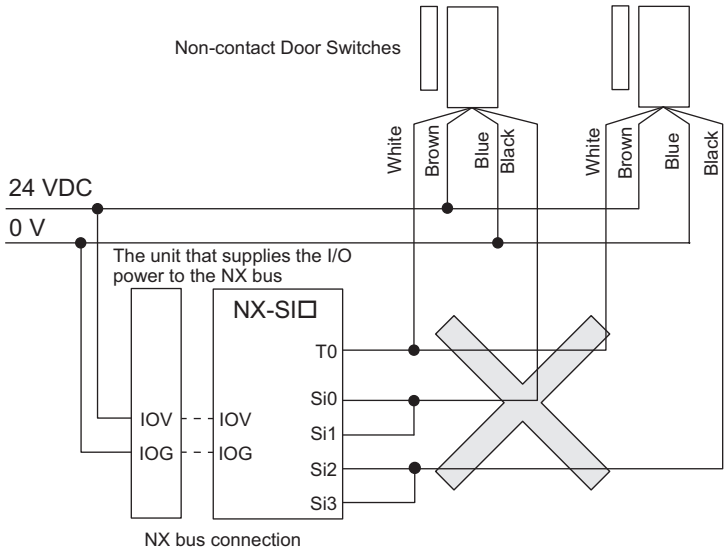


Example of Sysmac Studio Settings:



Precautions for Correct Use

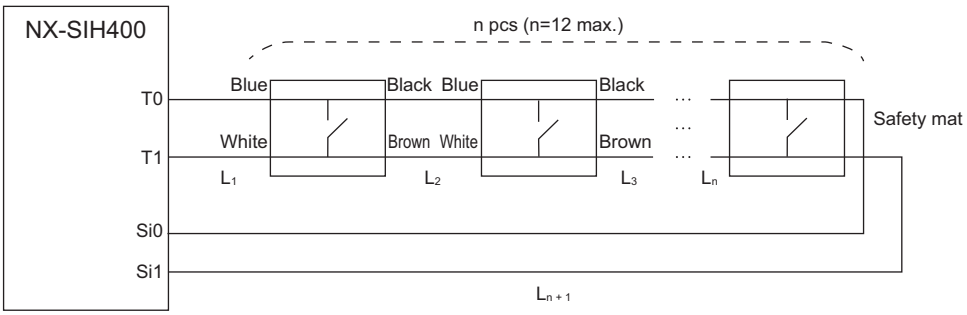
- The maximum number of connections per Unit is as follows:
  NX-SIH400: 20 (10 connected in series × 2 series)
- You can connect up to 10 Non-contact Door Switches to each test output terminal.
- You cannot branch the connections to more than one Non-contact Door Switch from the same test output terminal.



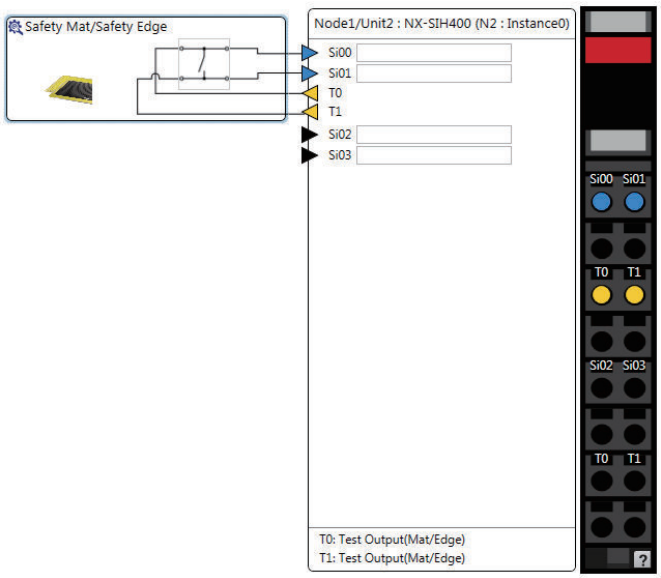
- The total wiring length (L1 + L2 +…+ Ln+2 in the figure above) for the D40A-2, D40A or D40Z Non-contact Switches is 100 m max.
- The D40A-2 Non-contact Door Switch can be used in a Safety Category 4 or lower or a PLe or lower application.
- The D40A Non-contact Door Switch can be used in a Safety Category 3 or lower or a PLd or lower application. It cannot be used in a Safety Category 4 or PLe application.
- The D40Z Non-contact Door Switch can be used in a Safety Category 4 or lower or a PLe or lower application.

● UM/UMA Safety Mats

OMRON UM/UMA Safety Mats are connected as shown in the following figure.



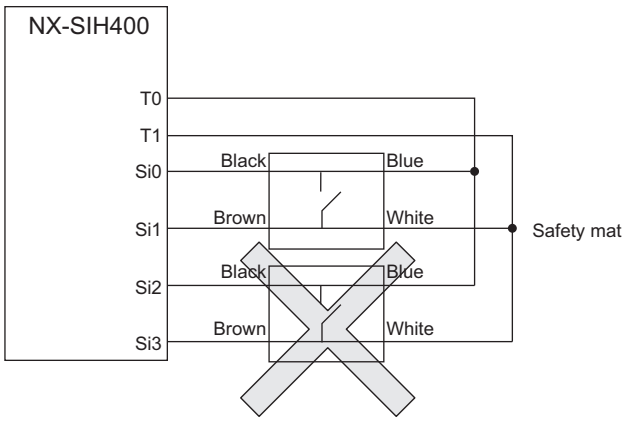
Example of Sysmac Studio Settings:



Refer to *Precaution for Conformance to ISO 13856-1:2013* on page 10-4 for a precaution on conformance to ISO 13856-1:2013.

Precautions for Correct Use

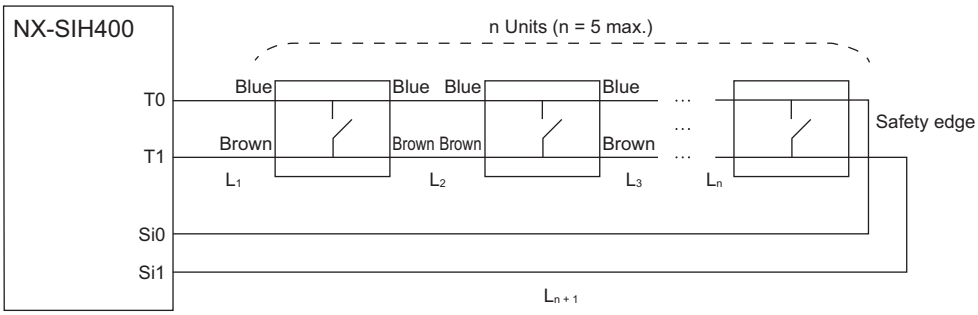
- The maximum number of connections per Unit is as follows:
  NX-SIH400: 12 (12 connected in series × 1 series)
- A Safety Mat requires two test output terminals when it is used. If a Safety Mat is connected to the NX-SIH400 Unit, you cannot connect any additional safety input devices that require test output terminals.
- You can connect up to 12 Safety Mats to the two test output terminals.
- You cannot branch the connections to more than one Safety Mat or Safety Edge from the same test output terminal.



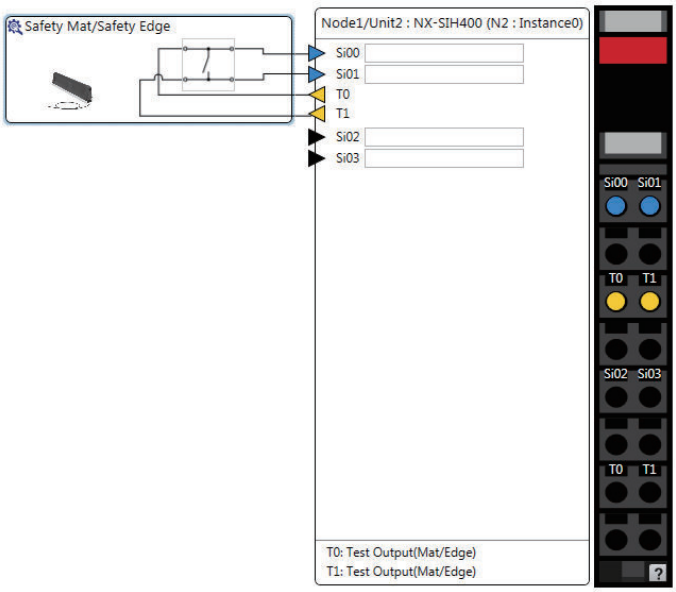
- The total wiring length (L1 + L2 +…+ Ln+1) for the UM/UMA Safety Mats is 100 m max.
- The UM/UMA Safety Mats can be used in a Safety Category 3 or lower or a PLd or lower application. They cannot be used in a Safety Category 4 or PLe application.

● SGE Safety Edges

OMRON SGE Safety Edges are connected as shown in the following figure.

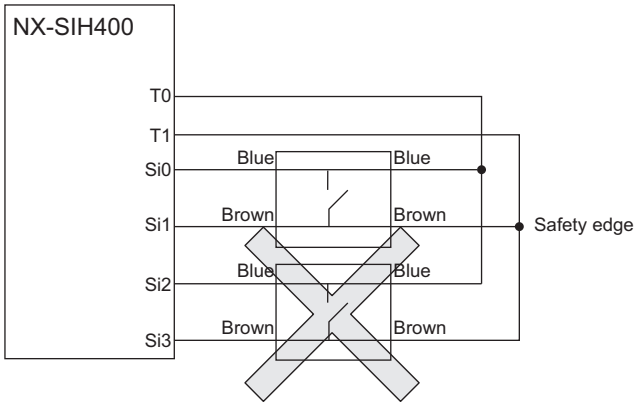


Example of Sysmac Studio Settings:



Precautions for Correct Use

- The maximum number of connections per Unit is as follows:
  NX-SIH400: 5 (5 connected in series × 1 series)
- A Safety Edge requires two test output terminals when it is used. If a Safety Edge is connected to the NX-SIH400 Unit, you cannot connect any additional safety input devices that require test output terminals.
- You can connect up to five Safety Eddges to the two test output terminals.
- You cannot branch the connections to more than one Safety Edge or Safety Mat from the same test output terminal.

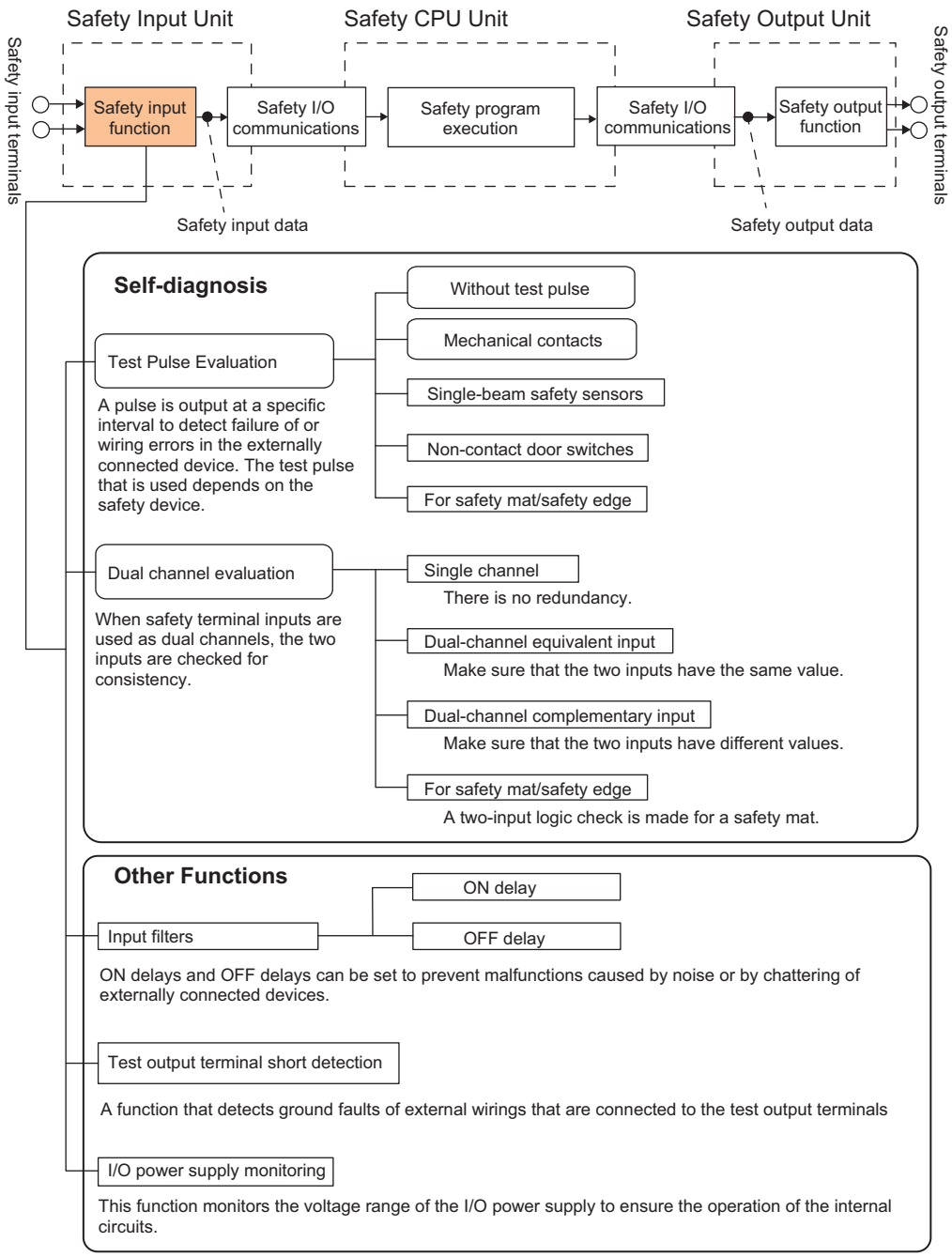


- Safety Edges can be connected only with two wires on each side (no terminating resistance). You cannot connect terminating resistance.
- The total wiring length (L1 + L2 +…+ Ln+1 in the figure above) for the SGE Safety Edges is 100 m max.
- The SGE Safety Edge can be used in a Safety Category 3 or lower or a PLd or lower application. It cannot be used in a Safety Category 4 or PLe application.

Types of Safety Input Functions

The types of safety input functions that are performed by the Safety Input Unit is shown below.

For the safety input functions, the safety signals that are input to the safety input terminals are evaluated and safety input data that can be used in the safety program is created.
The configuration of the safety input functions is shown in the following figure.
The values that are read from the safety input terminals are passed to the safety program only after they are evaluated by the safety input functions.



The following pages describe the details of the individual safety input functions.

Test Pulse Evaluation

A test pulse with a specific period is output on the 24-VDC power line from a test output terminal to detect wiring errors and failure of the externally connected device. The following parameters are also used.

- Test Pulse Diagnosis
- Test Source
- Test Pulse Mode

● Test Pulse Diagnosis

The Test Pulse Diagnosis setting determines whether to output a test pulse with a specific period from the test output terminal. The parameter determines whether test pulse evaluation is used. This parameter is set according to the type of external device that is connected to the safety input terminal.

Setting	Description
Without Test Pulse	A test pulse from the test output terminal is not output for diagnosis. This setting is used for safety devices with semiconductor outputs that diagnose the OSSD output themselves, such as safety light curtains, and for standard devices.
With Test Pulse	A test pulse from the test output terminal is output for diagnosis. The mode of the test output to use as the test source is selected according to the safety device that is connected.

● Test Source

The Test Source setting determines the test output terminal to use when the Test Pulse Diagnosis parameter is set to *with Test Pulse*. The test output terminal is automatically assigned by the Sysmac Studio, but it can be changed to any test output terminal.

● Test Pulse Mode

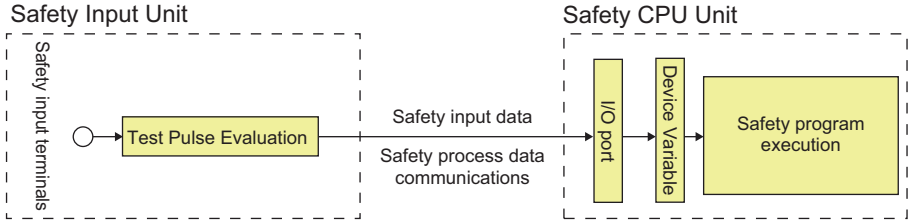
The Test Pulse Mode setting is used to output a test pulse that is suitable for the external device when the Test Pulse Diagnosis parameter is set to *with Test Pulse*.

Setting	Description
Mechanical Contact	The test pulse is connected to a device with mechanical contacts. The test output signal (pulse output) is input to the safety input terminal through the mechanical contact device. The following can be detected: Contact of the input signal line with the positive side of the power supply line, ground faults, and short-circuits to the other input signal lines.
Single Beam Safety Sensor	An OMRON E3ZS/E3FS Single-beam Safety Sensor is connected. A test signal for Single-beam Safety Sensor diagnosis is output.
Non-contact Door Switch	An OMRON D40A-2, D40A or D40Z Non-contact Door Switch is connected. Test signals for the D40A-2, D40A or D40Z will be output.
Safety Mat/Safety Edge	An OMRON UM/UMA Safety Mat or SGE Safety Edge (4-wire) is connected. A test signal for Safety Mat/Safety Edge diagnosis is output.

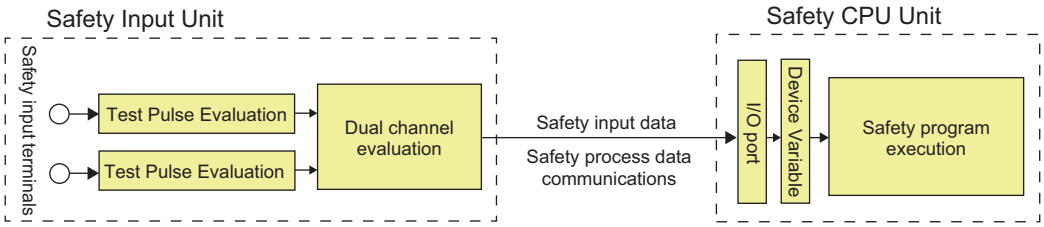
Dual Channel Evaluation

Safety input terminals can be used as dual channels (one pair). The dual channel evaluation evaluates the data for two inputs to check for discrepancy.

- Single Channel



- Dual Channels



The following parameters are also used.

- Single/Dual
- Discrepancy Time

● Single/Dual

Set the evaluation method to use with the safety input terminals.

Setting	Description
Single Channel	The safety input terminals are used as independent safety input terminals.
Dual Channel Equivalent	The safety input terminals are used as dual-channel-equivalent inputs.
Dual Channel Complementary	The safety input terminals are used as dual-channel-complementary inputs.
Safety Mat/Safety Edge	The safety input terminals are used as safety mat/safety edge inputs.

● Discrepancy Time

For two inputs set in a Dual Channel Mode, the time is monitored from a change in the value of one input to a change in the value of the other input. An error occurs if the value of the other input does not change within the set discrepancy time.

The discrepancy time can be set to any of the following eight values between 500 ms and 64,000 ms.

1: 500 [ms], 2: 1000 [ms], 3: 2000 [ms], 4: 4000 [ms], 5: 8000 [ms], 6: 16000 [ms], 7: 32000 [ms], 8: 64000 [ms]

The discrepancy time cannot be set in Single Channel Mode.

● Relationship between the Single/Dual Setting and Safety Input Data

The signals that are input to safety input terminals are evaluated as shown in the following table. This safety input data can be used in the safety program in the Safety CPU Unit.

- Relationship between Input Signals to Safety Input Terminals and Safety Input Data for Single-channel Inputs

Single/Dual	Input signals on the safety input terminals	Safety input data	Meaning of status
	Si (x)	Si (x)	
Single Channel	0	0	Inactive (OFF)
	1	1	Active (ON)

- Relationship between Input Signals to Safety Input Terminals and Safety Input Data for Dual-channel Inputs

n = Even number

Single/Dual	Input signals on the safety input terminals		Safety input data		Meaning of status
	Si (n)	Si (n+1)	Si (n)	Si (n+1)	
Dual Channel Equivalent	0	0	0	0*1	Inactive (OFF)
	0	1	0	0*1	Discrepant status
	1	0	0	0*1	Discrepant status
	1	1	1	0*1	Active (ON)
Dual Channel Complementary	0	0	0	0*1	Discrepant status
	0	1	0	0*1	Inactive (OFF)
	1	0	1	0*1	Active (ON)
	1	1	0	0*1	Discrepant status

*1. If the terminals are set to Dual Channel Mode, the safety program in the Safety CPU Unit must access the safety input data for the even-numbered terminal.

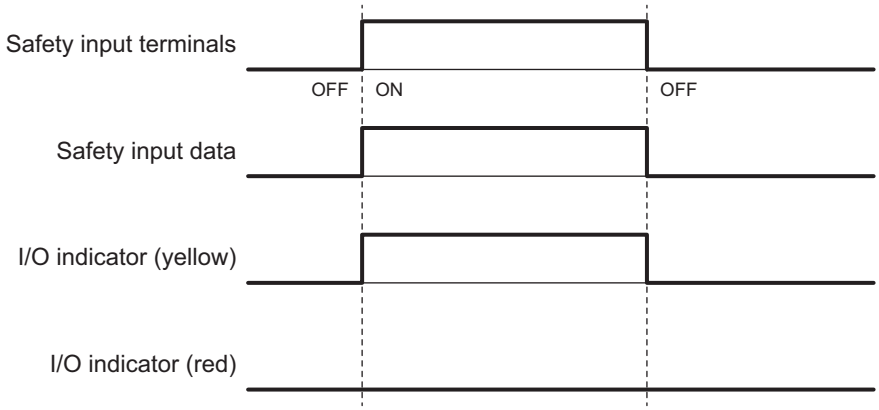
- Relationship between Safety Mat Status and Safety Input Data for Safety Mat/Safety Edge Inputs

n = Even number

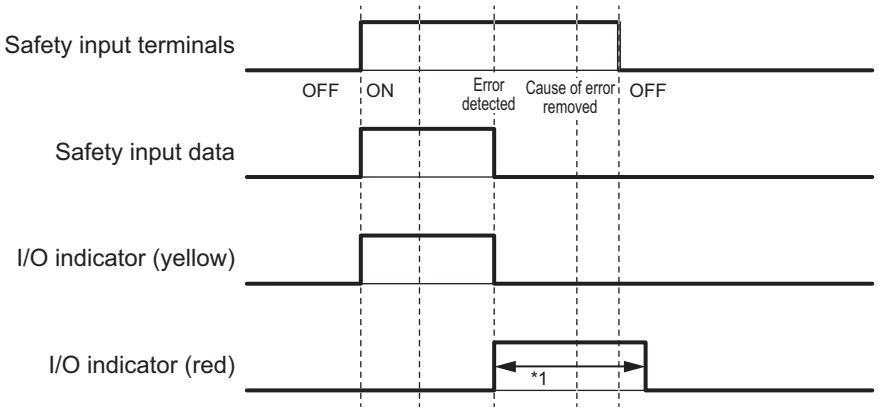
Single/Dual	Safety mat/safety edge status	Safety input data		Meaning of status
		Si (n)	Si (n+1)	
Safety Mat/Safety Edge	Without load	1	0*1	Active (ON)
	With load	0	0*1	Inactive (OFF)

*1. If the terminals are set to Dual Channel Mode, the safety program in the Safety CPU Unit must access the safety input data for the even-numbered terminal.

- Operation for Single Channel: Normal Operation

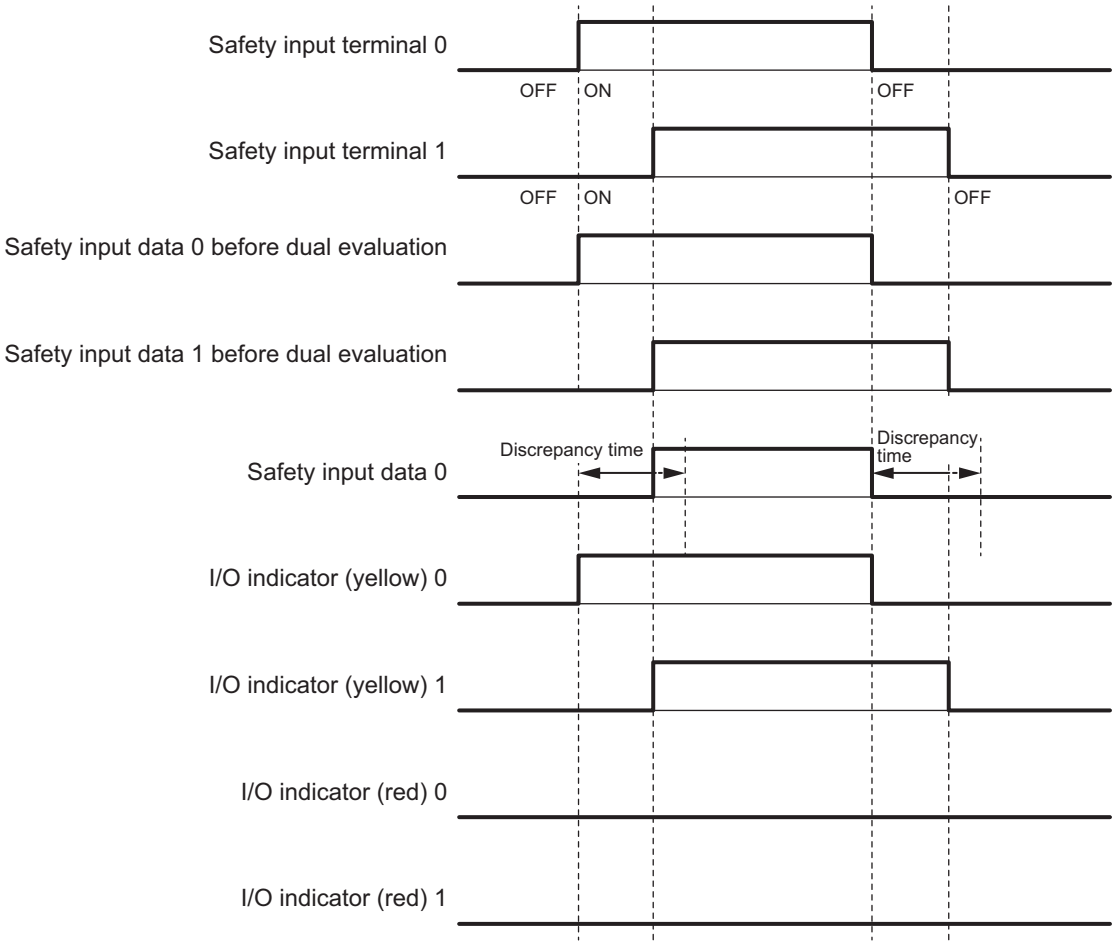


- Operation for Single Channel: Test Pulse Evaluation Error by Stuck-at-high Error

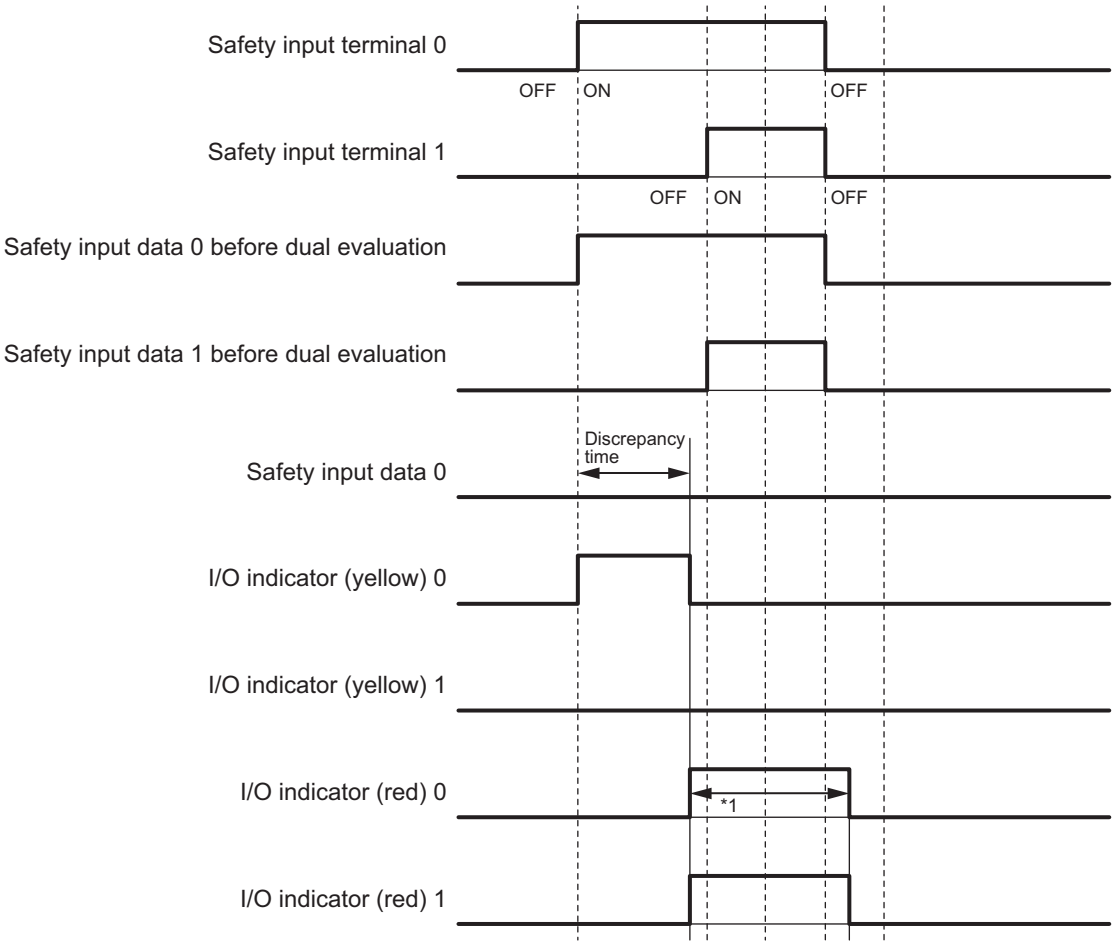


*1. This is the time that the error status (control data, status data, and indicator status) is held (1 s min.).

- Operation for Dual-channel Equivalent Inputs: Normal Operation



- Operation for Dual-channel Equivalent Inputs: Discrepancy Error



*1. This is the time that the error status (control data, status data, and indicator status) is held (1 s min.).

Errors Detected during Self-diagnosis

The errors that can be detected for safety input terminals are determined by the parameter settings. The following table gives the errors that are detected for each parameter setting.

● Devices with Mechanical Contacts and Devices with Semiconductor Outputs

Setting		Error detection			
Single/Dual	Test pulse	Contact with positive side of power line	Ground fault*1	Disconnection	Short circuits in input wiring
Single Channel	Without Test Pulse	Not detectable.	Not detectable.	Not detectable.	---
	With Test Pulse	Detectable.	Detectable when input turns ON.	Not detectable.	---

Setting		Error detection			
Single/Dual	Test pulse	Contact with positive side of power line	Ground fault*1	Disconnection	Short circuits in input wiring
Dual Channel Equivalent	Without Test Pulse	Not detectable.*2	Not detectable.	Detectable when input turns ON.	Not detectable.*2
	Same test source for pair of safety input terminals	Detectable.	Detectable when input turns ON.	Detectable when input turns ON.	Not detectable.
	Different test sources for pair of safety input terminals	Detectable.	Detectable when input turns ON.	Detectable when input turns ON.	Detectable.
Dual Channel Complementary	Without Test Pulse	Detectable when input turns ON or OFF.	Detectable when input turns ON or OFF.	Detectable when input turns ON or OFF.	Detectable.
	Same test source for pair of safety input terminals	Detectable.	Detectable when input turns ON or OFF.	Detectable when input turns ON or OFF.	Detectable.
	Different test sources for pair of safety input terminals	Detectable.	Detectable when input turns ON or OFF.	Detectable when input turns ON or OFF.	Detectable.

*1. To detect ground faults, the 0-V line of the external power supply must be grounded.
*2. Detection is possible with the OSSD diagnostic function of the light curtain or laser scanner.

● Single-beam Safety Sensors, Non-contact Door Switches, Safety Mats, and Safety Edges

Input device	Error detection					
	Contact with positive side of power line	Ground fault*1	Disconnection	Short circuits in input wiring	Failure of input device	Sensor bypass
Single-beam Safety Sensor	Detectable.	Not detectable.	Not detectable.	---	Not detectable.	Detectable.
D40A-2/D40A Non-contact Door Switch	Detectable.	Not detectable.	Not detectable.	---	Detectable.	Detectable.
D40Z Non-contact Switch	Detectable.	Not detectable.	Not detectable.	---	Detectable.	Detectable.
Safety Mat/Safety Edge	Detectable.	Detectable.	Detectable.	Not detectable.	Not detectable.	---

*1. To detect ground faults, the 0-V line of the external power supply must be grounded.



Additional Information

To detect burnouts in a muting lamp, use a PIT si1.2 Muting Lamp manufactured by Pilz, which supports defective lamp detection.

Input Filters

The input filter helps prevent malfunctions that are sometimes caused by chattering or noise from the external device that is connected to a safety input terminal.
You can filter out chattering and noise from the external device for the widths that are set with the ON delay time and OFF delay time.
ON delays and OFF delays can be set to one of the 10 options given below, from 0 to 1,536 ms, for each safety input terminal.

1: 0 [ms], 2: 6 [ms], 3: 12 [ms], 4: 24 [ms], 5: 48 [ms], 6: 96 [ms], 7: 192 [ms],
8: 384 [ms], 9: 768 [ms], 10: 1536 [ms],

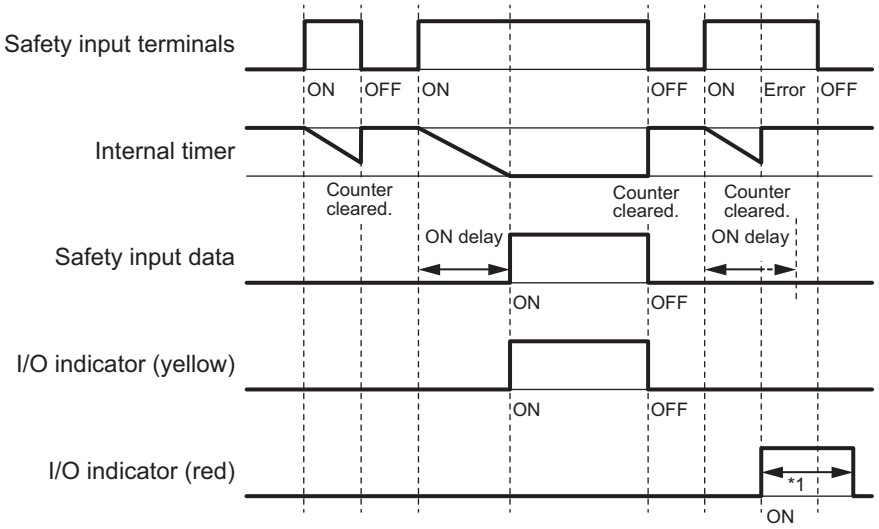
The effect of chattering from external devices can be reduced more by increasing the delay time, but this will slow the response to input signals.
The input filter can be used with dual channel evaluation.

Precautions for Correct Use

If an OFF delay is used, the OFF delay time affects the safety reaction time. Add the OFF delay time to the safety reaction time. (Refer to *Section 10 Calculating Safety Reaction Times* on page 10-1.)

● Operation with an ON Delay

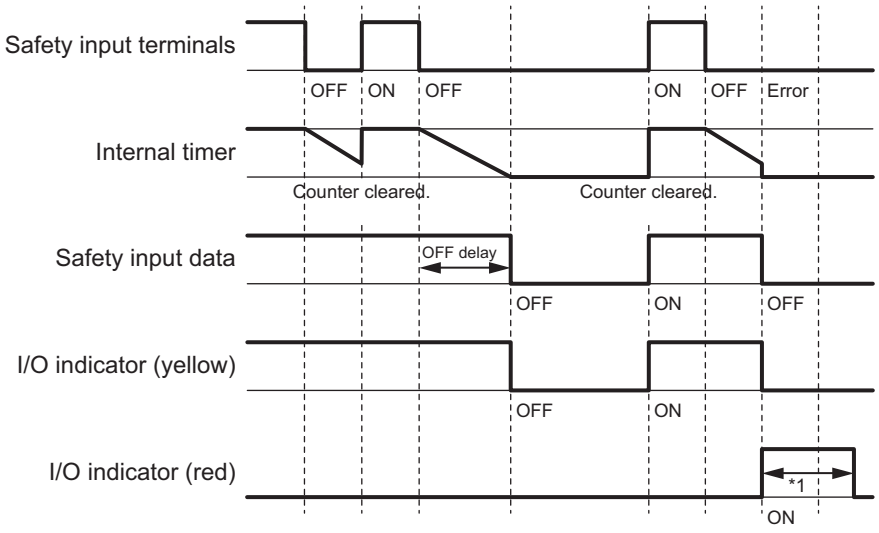
You can filter out ON pulses for the width that is set with the ON delay time.



*1. This is the time that the error status (control data, status data, and indicator status) is held (1 s min.).

● Operation with an OFF Delay

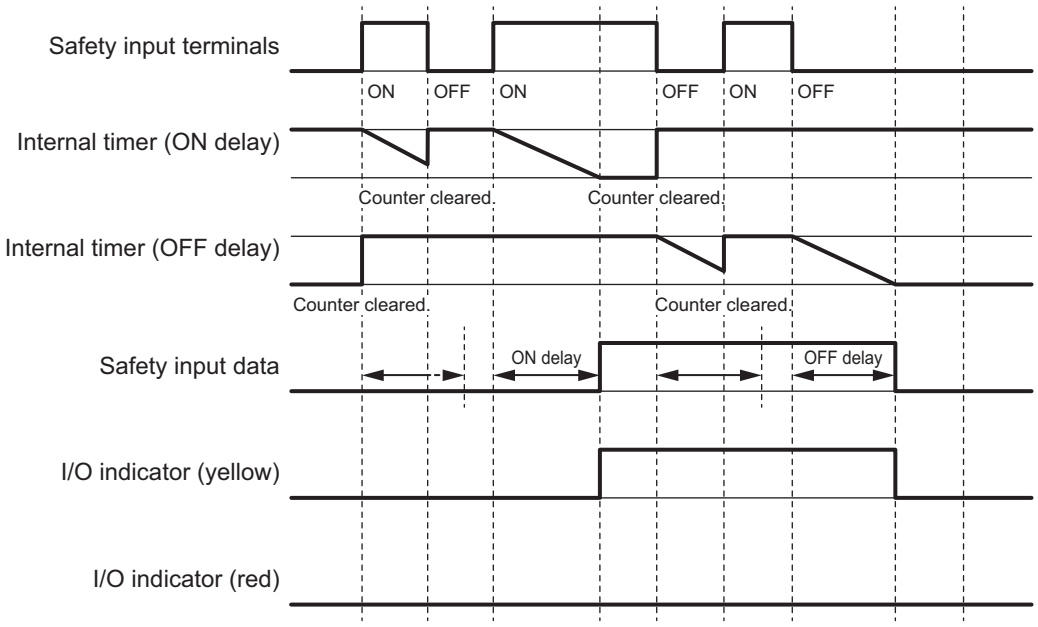
You can filter out OFF pulses for the width that is set with the OFF delay time.



*1. This is the time that the error status (control data, status data, and indicator status) is held (1 s min.).

● Operation with Both an ON Delay and OFF Delay

You can filter out ON pulses for the width that is set with the ON delay time and filter out OFF pulses for the width that is set with the OFF delay time.



Test Output Terminal Short Detection

The test output terminal short detection prevents the internal circuits of the test output terminals from being destroyed if an overcurrent flows due to a ground fault or other cause.

If an overcurrent is detected, the safety input data for the safety input terminal that is being used as the test source for the terminal is turned OFF.

At this time, an *Overload Detected at Test Output* event will occur. To troubleshoot errors, refer to *Section 15 Troubleshooting* on page 15-1.

I/O Power Supply Monitoring

I/O power supply monitoring monitors the voltage range of the I/O power supply.
If a voltage that is less than the specified range is detected, all safety inputs for the Unit are turned OFF.
At this time, an *I/O Power Supply Voltage Error* occurs. To troubleshoot errors, refer to *Section 15 Troubleshooting* on page 15-1.
This function does not work if all of the terminals are set as unused terminals.

6-3-2 Safety Output Function

Connectable Output Devices

The Safety Output Unit diagnoses the connected external devices through the safety output terminals. The general-purpose safety output devices that can be connected to the safety output terminals of a Safety Output Unit are listed in the following table.

Type	Examples
Safety devices that can be connected to PNP outputs	Safety relays, contactors, or safety inputs from servo drives

Additional Information

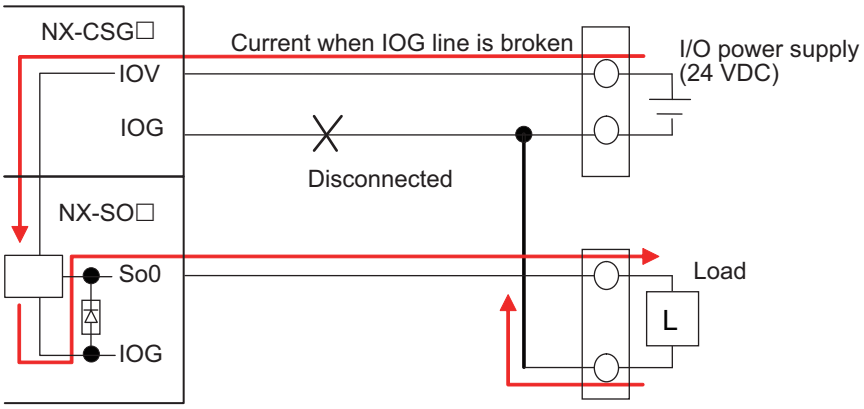
The connection of incandescent lamps is not supported. Connect them to an NX-series Digital Output Unit.

Setting the Safety Functions for Safety Output Terminals

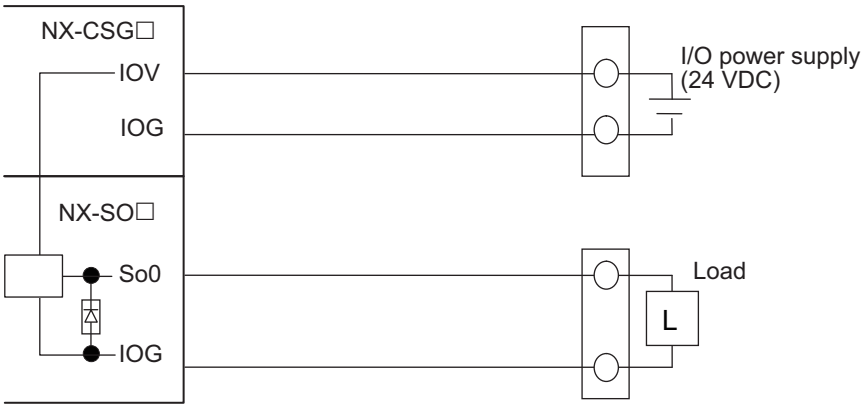
You can easily set the safety functions of the safety output terminals from the Sysmac Studio by selecting the external devices that are connected.
Refer to *6-3 Safety I/O Function* on page 6-16 for details.

Connecting the I/O Power Supply

This section describes the connection methods for the I/O power supply.
If the Safety Output Unit is wired as shown in the following figure and the IOG wire breaks, a floating condition will result. If that occurs, a few volts may be applied to the output terminals of the Safety Output Unit, turning ON the load.



Use the wiring that is shown in the following figure to prevent a floating condition for the IOG of the Safety Output Unit even if the IOG line is broken.

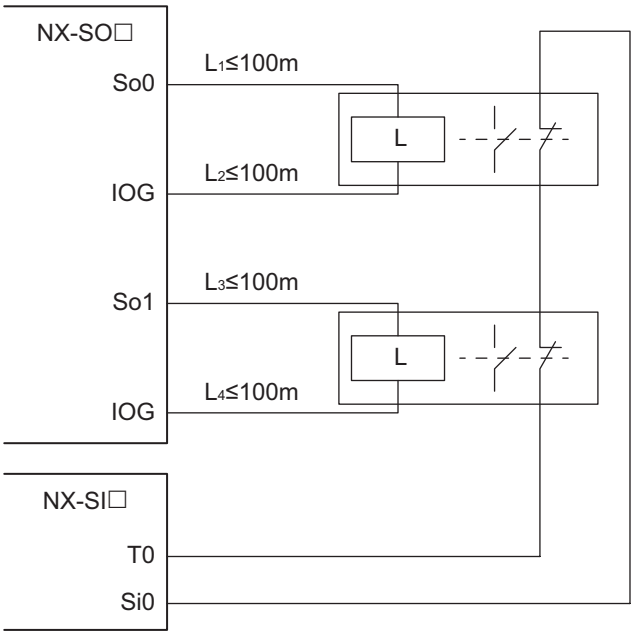


Connecting Output Devices

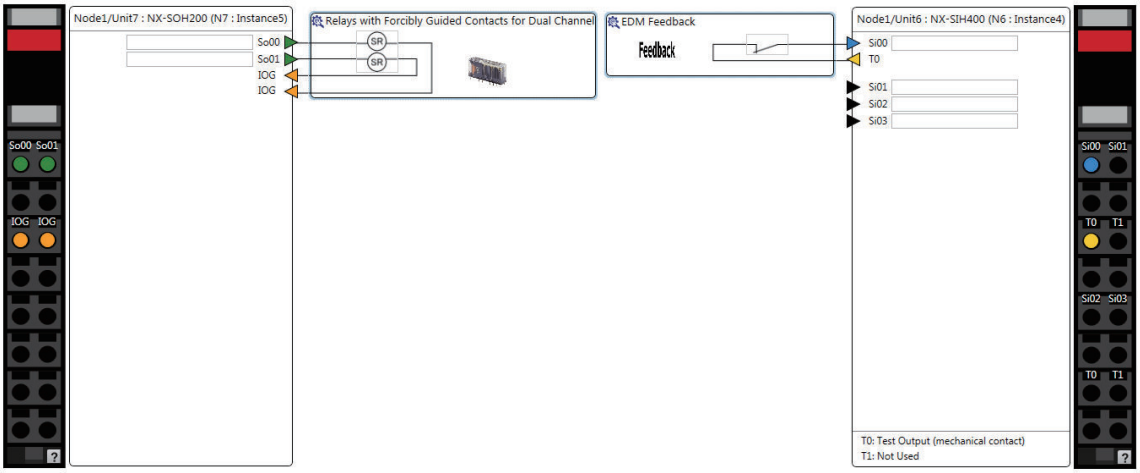
This section describes the connection methods for output devices.

● Safety Relays and Contactors

Connect a safety relay or contactor as shown in the following figure.



Example of Sysmac Studio Settings:



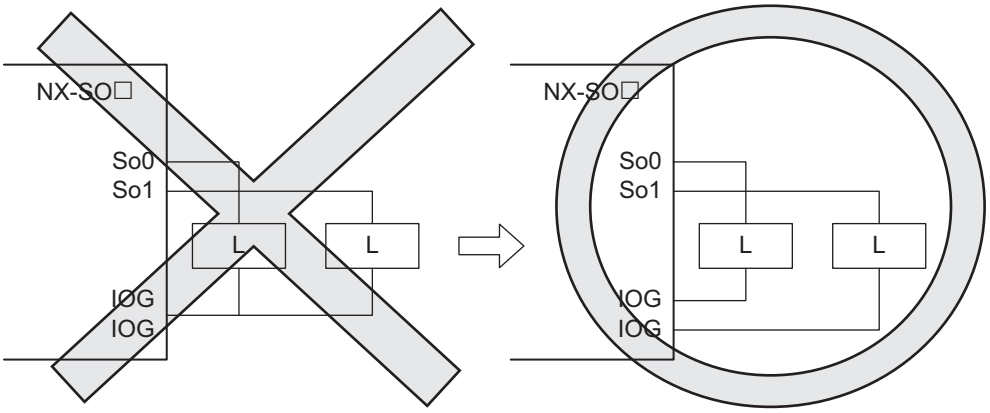
Precautions for Correct Use

- The line length from the safety output terminals to the output devices (L1, L2, L3, and L4) is 100 m max. for each line.
- The total length of cable that is connected to one test output must be as described in *6-3-1 Safety Input Function* on page 6-16.

● Connecting More Than One Output Device

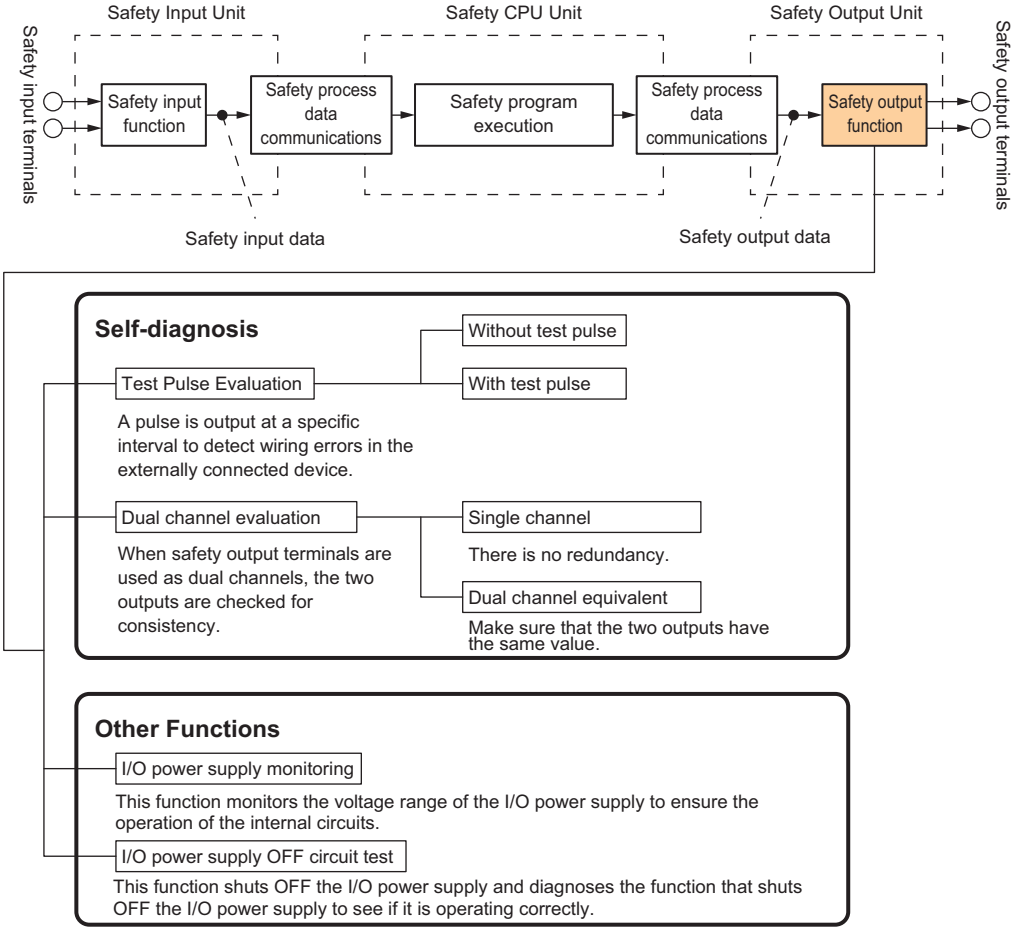
The IOG terminals on the Safety Output Unit are connected internally in the Unit. Make sure that the current that flows through each IOG terminal is less than the current capacity of the I/O power supply terminals.

If the wiring is shared for the IOG lines to the output devices, the sum of the output currents will flow in the IOG line. Therefore, wire the IOG lines separately.



Types of Safety Output Functions

The types of safety output functions that are performed by the Safety Output Unit is shown below.
The safety output functions diagnose the outputs to the safety output terminals and the external device wiring based on the safety output data from the safety program.
The execution results of the safety program are evaluated by the safety output functions and the evaluation results are output from the safety output terminals.



Test Pulse Evaluation

The test pulse evaluation outputs a test pulse with a specific period on the 24-VDC power line from a safety output terminal to detect errors in wiring to the externally connected device. This evaluation is achieved through the *Test Pulse Diagnosis* parameter.

● Test Pulse Diagnosis

The Diagnosis setting determines whether to output a test pulse with a specific period from the safety output terminal. The parameter determines whether test pulse evaluation is used.
The errors that can be detected are determined by the parameter settings.
Refer to *Errors Detected during Self-diagnosis* on page 6-34 for the errors that can be detected for each parameter setting.

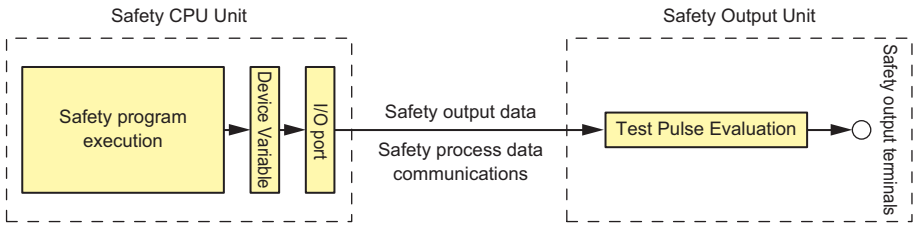
Precautions for Correct Use

When the Test Pulse Diagnosis parameter is set to *with Test Pulse*, OFF pulse signals with a pulse width of 640 µs are output while the safety output is ON to diagnose the output circuit. Check the input response time of the connected control device to make sure it will not malfunction due to these OFF pulses.

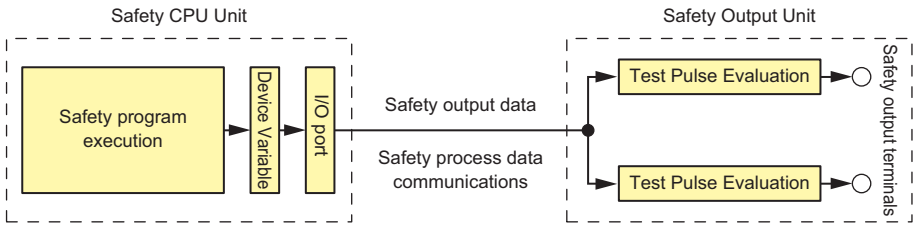
Dual Channel Evaluation

The use of dual-channel-equivalent outputs lets you control two safety output terminals with one safety output data from the safety program. If an error is detected in either of the two output terminals, the outputs to the external devices are both turned OFF.

- Single Channel



- Dual Channels



This evaluation is achieved through the *Single/Dual* parameter.

● Single/Dual

Set the evaluation method to use with the safety output terminals.

Setting	Description
Single Channel	The safety output terminals are used as independent safety output terminals.

Setting	Description
Dual Channel Equivalent	The pair of safety output terminals are used as dual channel outputs. The output is ON if the paired safety output terminals are both normal.

● Relationship between the Single/Dual Setting and Safety Output Data

The safety output data that is used in the safety program is output to the safety output terminals according to the Single/Dual parameter as shown below.

- Relationship between Safety Output Data and Signals Output from Safety Output Terminals for Single-channel Outputs

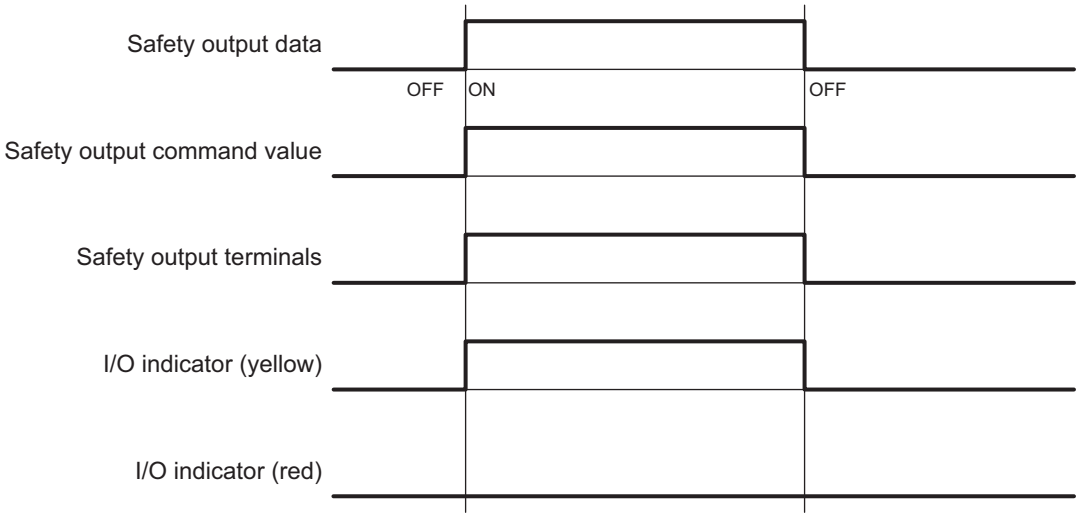
Single/Dual	Safety output data	Output signal on the safety output terminal	Meaning of status
	So (x)	So (x)	
Single Channel	0	0	Inactive (OFF)
	1	1	Active (ON)

- Relationship between Safety Output Data and Signals Output from Safety Output Terminals for Dual-channel Equivalent Outputs

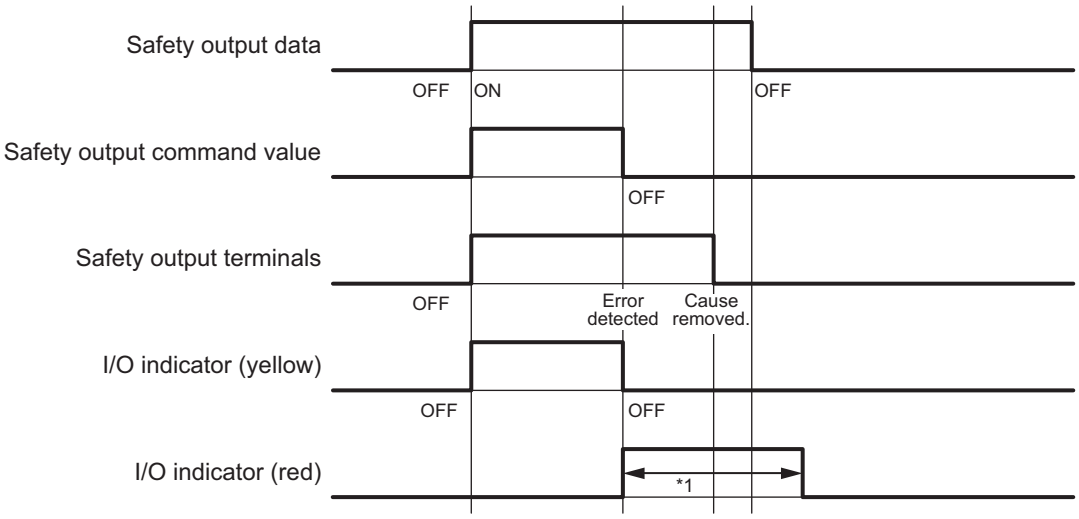
n = Even number

Single/Dual	Safety output data	Output signal on the safety output terminal		Meaning of status
	So (x)	So (n)	So (n+1)	
Dual Channel Equivalent	0	0 (OFF)	0 (OFF)	Inactive (OFF)
	1	1 (ON)	1 (ON)	Active (ON)

- Operation for Single Channel: Normal Operation

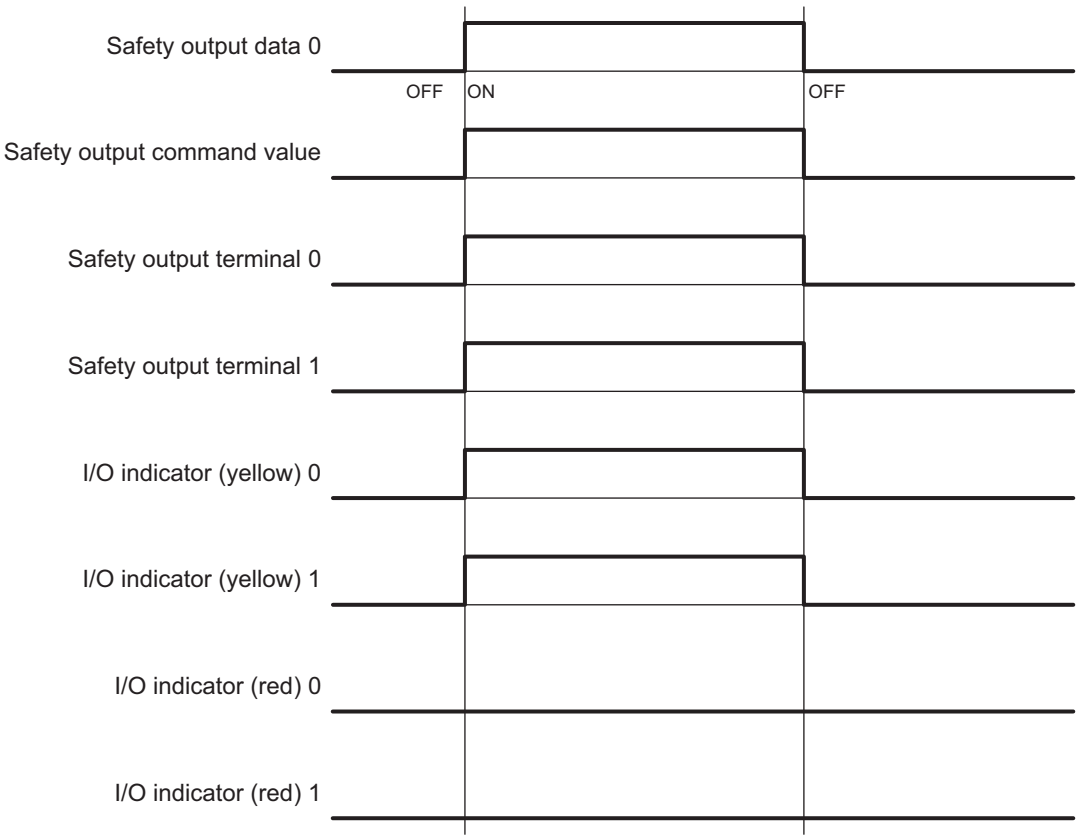


- Operation for Single Channel: Test Pulse Evaluation Error by Stuck-at-high Error

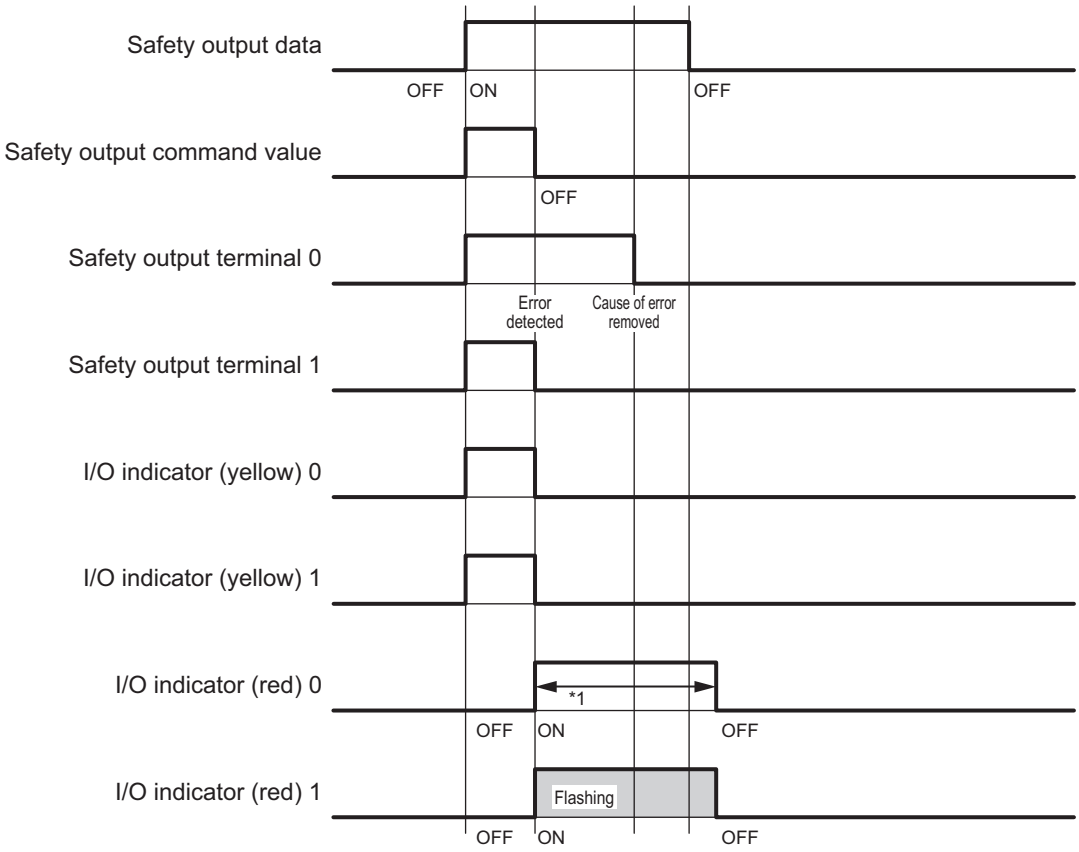


*1. This is the time that the error status (control data, status data, and indicator status) is held (1 s min.).

- Operation for Dual-channel Equivalent Outputs: Normal Operation



- Operation for Dual-channel Equivalent Outputs: Test Pulse Evaluation Error



*1. This is the time that the error status (control data, status data, and indicator status) is held (1 s min.).

Errors Detected during Self-diagnosis

The errors that can be detected for safety output terminals are determined by the parameter settings. The following table gives the errors that are detected for each parameter setting.

Test pulse diagnosis	Description of operation	Error detection						
		Contact with positive side of power line		Ground fault*1		Short circuits in output wiring		
		Output ON	Output OFF	Output ON	Output OFF	Short circuit when both outputs are ON	Short circuit when both outputs are OFF	Short circuit when one output is ON and the other is OFF
Without Test Pulse	Test pulses are not output when the output is ON.	Not detectable.	Detectable.	Detectable.	Not detectable.	Not detectable.	Not detectable.	Detectable.
With Test Pulse	Test pulses are output when the output is ON.	Detectable.	Detectable.	Detectable.	Not detectable.	Detectable.	Not detectable.	Detectable.

*1. To detect ground faults, the 0-V line of the external power supply must be grounded.

Safety Output Terminal Short Detection

The safety output terminal short detection prevents the internal circuits of the safety output terminals from being destroyed if an overcurrent flows due to a ground fault or other cause.
If an overcurrent is detected, the safety output terminal is turned OFF.
At this time, a *Short Circuit Detected at Safety Output* event will occur. To troubleshoot errors, refer to *Section 15 Troubleshooting* on page 15-1.

I/O Power Supply Monitoring

I/O power supply monitoring monitors the voltage range of the I/O power supply to ensure the operation of the internal circuits.
If a voltage that is outside of the specified range is detected, all safety output terminals for the Unit are turned OFF.
At this time, an *I/O Power Supply Voltage Error* occurs. To troubleshoot errors, refer to *Section 15 Troubleshooting* on page 15-1.
This function does not work if all of the terminals are set as unused terminals.

I/O Power Supply OFF Circuit Test (Internal Circuit Diagnosis)

The I/O power supply OFF circuit test shuts OFF the I/O power supply and diagnoses the function that shuts OFF the I/O power supply to see if it is operating correctly.
If an internal circuit fault is detected by this function, all safety output terminals for the Unit are turned OFF.
This test is executed at the following two times. The I/O power supply OFF circuit test is executed only once when the Unit power supply is turned ON. The test is not performed again until the Unit power supply is turned ON again.

● When the Status Changes to Refreshing Status

If the I/O power supply is turned ON before the status changes to refreshing status, the I/O power supply OFF circuit test is performed when the status changes to refreshing status.

● When I/O Power Supply is Turned ON

If the I/O power supply is turned ON after the status changes to refreshing status, the I/O power supply OFF circuit test is performed when the I/O power supply is turned ON.

7

Settings

7-1 Configuration and Setup Procedures 7-2

7-2 Part Names and Functions of the Sysmac Studio Window 7-3

7-3 CPU Rack Configuration and Setup 7-5
7-3-1 Procedures for Creating the CPU Rack Configuration 7-5
7-3-2 Setting and Viewing the NX Unit Settings 7-6
7-3-3 Setting Up the FSoE Communications 7-7

7-4 EtherNet/IP Network Configuration and Setup 7-9
7-4-1 Setting IP Addresses 7-9
7-4-2 Setting Tag Data Links 7-17

7-5 CIP Safety Communication Settings 7-21
7-5-1 Safety Network Number Settings for the NX Bus 7-21
7-5-2 Originator Connection Settings 7-22
7-5-3 Target I/O Assembly Settings 7-33
7-5-4 Connecting Target Devices of Other Manufacturers 7-35

7-6 Setting the Input and Output Functions 7-42
7-6-1 Safety I/O Functions 7-42
7-6-2 Setting the Standard Input and Output Functions 7-45

7-7 Assigning Variables to I/O Ports 7-46
7-7-1 Registering Device Variables 7-46
7-7-2 Settings of Communications between NX Units 7-51

7-8 Exposing Variables to Standard Controllers 7-53
7-8-1 Exposing Global Variables 7-53
7-8-2 Setting Exposed Variables 7-54
7-8-3 Safety CPU Unit Status 7-58
7-8-4 I/O Ports of Safety I/O Units 7-59
7-8-5 I/O Ports for Standard I/O Units 7-59

7-9 Exporting/Importing Settings Data 7-60
7-9-1 Exporting/Importing the All NX Unit Settings 7-60
7-9-2 Exporting/Importing Data for Individual Safety CPU Unit 7-62
7-9-3 Importing the Safety Unit Restore File 7-64

7-10 Offline Comparison 7-65
7-10-1 Procedure for Offline Comparison 7-65
7-10-2 Checking the Comparison Results 7-66
7-10-3 Detailed Comparison 7-67
7-10-4 Target Data of Offline Comparison 7-69

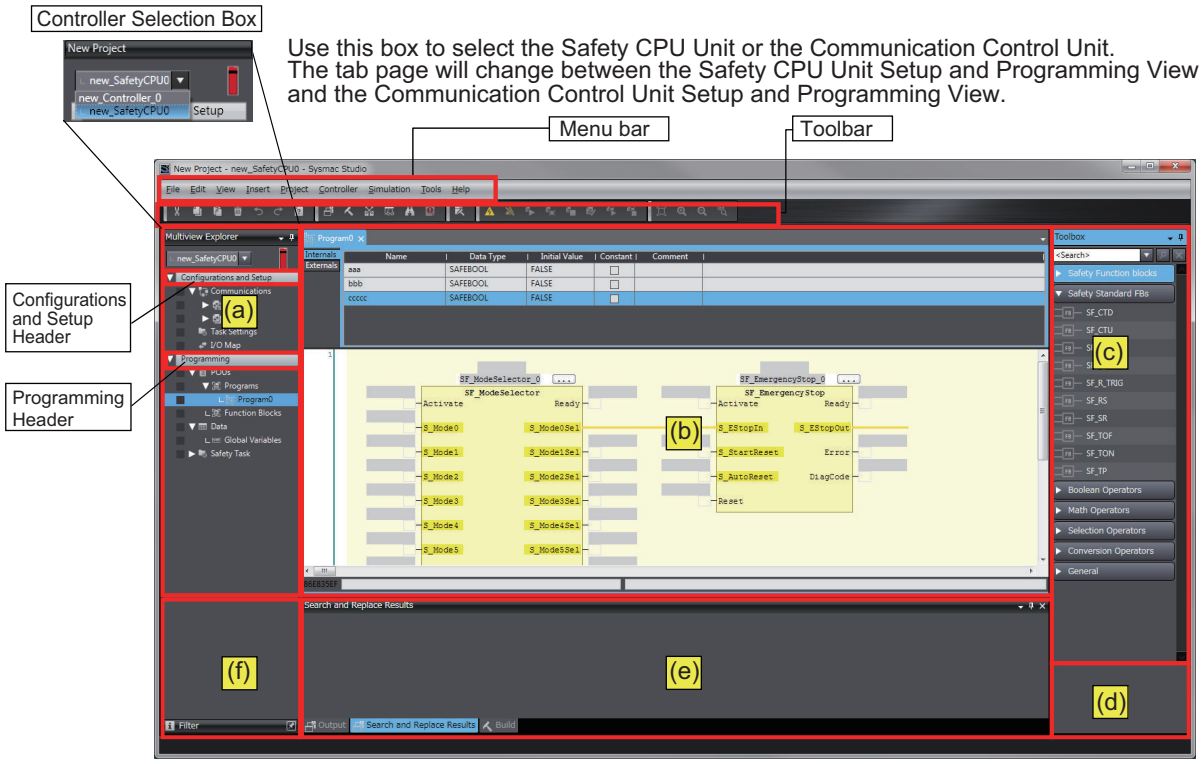
7-1 Configuration and Setup Procedures

This section describes the procedures for using the Sysmac Studio to configure and set up the Safety Network Controller. Make the settings in the following order.

1. CPU Rack Configurations and Setup
2. EtherNet/IP Network Configurations and Setup
3. I/O Terminals Setup
4. Assigning Variables to I/O Ports
5. Exposing Variables to Standard Controllers

7-2 Part Names and Functions of the Sysmac Studio Window

This section gives the names of the parts of the Sysmac Studio Window.



Letter	Name	Function
(a)	Multiview Explorer	This pane is your access point for all Sysmac Studio data that is related to the Safety Network Controller. It has a **Controller Selection** Box, and is separated into a **Configurations and Setup** Layer and a **Programming** Layer. Use the **Controller Selection** Box to select the Safety CPU Unit or the Communication Control Unit.
(b)	Edit Pane	The Edit Pane is used to display and edit the data for any of the items.
(c)	Toolbox	The Toolbox shows the objects that you can use to edit the data that is displayed in the Edit Pane.
	Search and Replace Pane	In this pane, you can search for and replace strings in the data under **Programming** Layer of the Multiview Explorer.
(d)	Controller Status Pane	This pane shows the operating status of the Safety CPU Unit or the Communication Control Unit. The Controller Status Pane is displayed only while the Sysmac Studio is online with the Safety CPU Unit or the Communication Control Unit, or when the Simulator is running.
	Simulation Pane	This pane is used to start and stop the Safety CPU Unit Simulator.

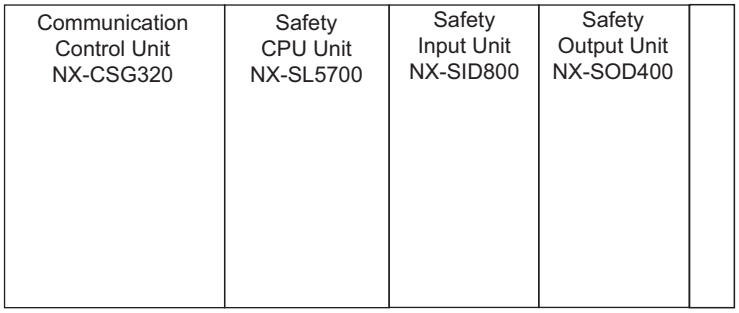
Letter	Name	Function
(e)	Output Tab Page	The Output Tab Page shows the results of building.
	Watch Tab Page	The Watch Tab Page shows the monitor results of the online Safety CPU Unit, the Communication Control Unit, or the Simulator.
	Build Tab Page	The Build Tab Page shows the results of program checks and building.
	Search and Replace Results Tab Page	The Search and Replace Results Tab Page shows the results when Search All or Replace All is executed.
(f)	Filter Pane	The Filter Pane allows you to search for color codes and for items with an error icon. The results are displayed in a list.

This manual describes only the functions and operations of the Sysmac Studio that are related to the Safety Network Controller.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on the Sysmac Studio operation.

7-3 CPU Rack Configuration and Setup

This section describes the configuration and setting procedures for a CPU Rack for the Safety Network Controller.
You configure and set up a CPU Rack of the Communication Control Unit on the CPU and Expansion Racks Tab Page of the Communication Control Unit. Next, set up the FSoE communication between the Safety CPU Unit and the Safety I/O Unit.

This section describes the operations to perform based on the following configuration.



7-3-1 Procedures for Creating the CPU Rack Configuration

Use the following procedure to create a CPU Rack configuration for the Safety Network Controller.

1. Start the Sysmac Studio.
2. Select the model and version of the Communication Control Unit, and create a project file.
3. Select **Configurations and Setup** – **CPU/Expansion Racks** and double-click **CPU Rack** in the Multiview Explorer. The CPU and Expansion Racks Tab Page is displayed.
4. Select **Safety CPU Device** from the Groups List in the Toolbox. The Safety CPU Unit is displayed below it. Drag the model of the Safety CPU Unit to the CPU Rack and add it to the configuration.
5. Select **Safety Digital Input Device** or **Safety Output Device** from the Groups List in the Toolbox. The Safety I/O Units is displayed below it. Drag the model of the Safety I/O Units to the CPU Rack and add it to the configuration.

This completes the creation of a CPU Rack configuration for the Safety Network Controller.
After the Safety CPU Unit is added to the configuration, this Safety CPU Unit will be displayed in the Controller Selection Box in the Multiview Explorer. The Safety CPU Unit that was added is displayed below the Communication Control Unit (i.e. the NX bus master).



Additional Information

- Only one Safety CPU Unit can be placed on the Communication Control Unit. If you add more than one Safety CPU Units, the " ! " icons are displayed under all of the Safety CPU Units, and it will cause an error during the synchronization and download process.
- Be sure to use the Communication Control Unit after configuring the Safety CPU Unit. With no Safety CPU Unit configured, the " ! " icon is displayed under Communication Control Unit, and it will cause an error during the synchronization and download process.
- Up to 32 NX Units can be mounted to the Communication Control Unit.

7-3-2 Setting and Viewing the NX Unit Settings

Set or view the following settings for the NX Unit as necessary.

You can change the device names of registered NX Units, and enable or disable individual Units as NX Units.

Name	Editing	Description	Data range	Initial value
Device name	Possible	This is the name of the NX Unit. The device name is automatically assigned when you register the NX Unit. You can change the device name if necessary. However, device names must be unique within the CPU Rack configuration for Safety Network Controller. If you specify the same name for more than one Unit, an error will occur.	Text string	N* (where * is a serial number from 1)
Model name	Not possible	This is the model number of the NX Unit.	---	---
Product name	Not possible	This is the product name.	---	---
Unit version	Not possible	This is the unit version of the NX Unit.	---	---
NX Unit number	Not possible	This number represents the logical position as an NX Unit. Numbers are automatically assigned from the leftmost mounting position.	---	---
NX Unit Mounting Setting	Possible	This setting enables or disables I/O refreshing for the NX Unit. For details on the function, refer to the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)*.	Enabled or disabled	Enabled
Serial number	Not possible	This is the serial number of the NX Unit. You can get the serial number to set the serial number of the actual EtherCAT Coupler Unit.	---	00000000 hex

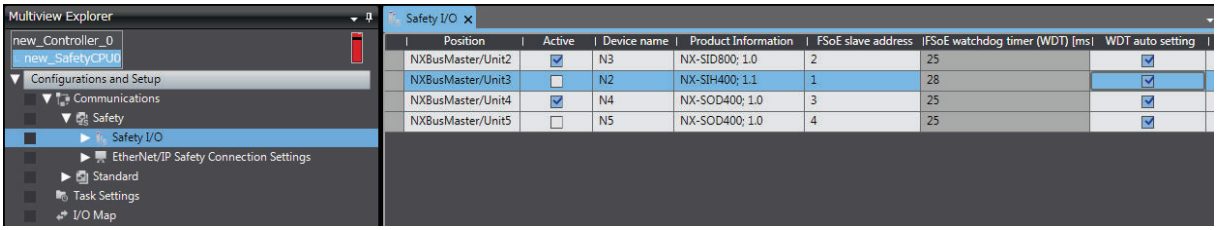
Name	Editing	Description	Data range	Initial value
Power consumption (W)	Not possible	This is the power consumption of the NX Unit from the NX bus. This setting applies to Units other than an Additional NX Unit Power Supply Unit.	---	Depends on the model of the Unit.
Unit width (mm)	Not possible	This is the width of the NX Unit.	---	Depends on the model of the Unit.
I/O allocation settings	Possible	These are the I/O allocation settings for the NX Unit. You cannot change these settings for Safety Control Units.	---	Depends on the model of the Unit.
Unit operation settings	Not possible	These are the unit operation settings for the NX Unit. There are no settings that you can edit for the Safety Control Units.	---	Depends on the model of the Unit.

7-3-3 Setting Up the FSoE Communications

When you add a Safety Control Unit to the NX bus in the CPU Rack configuration of Sysmac Studio, the FSoE communications are set up automatically.

Use the following procedure to view or change the settings for the FSoE communications.

1. In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.
2. Select **Configurations and Setup** – **Communications** – **Safety**, and then double-click **Safety I/O**.



The meanings of the items in the Safety I/O Tab Page are given below.

Item	Editing	Description
Position	Not possible	The NX Unit number of the Safety I/O Unit is displayed.

Item	Editing	Description
Active (Enable/ Disable)	Possible	The communications setting for FSoE communications is displayed. Selected: *Enabled* This setting assigns the Safety I/O Unit to the Safety CPU Unit as a communications node, and displays the I/O ports for that Unit in the I/O Map. Not selected: *Disabled* This setting does not assign the Safety I/O Unit to the Safety CPU Unit as a communications node, and does not display the I/O ports for that Unit in the I/O Map.
Device	Not possible	It displays the device name specified at *7-3-2 Setting and Viewing the NX Unit Settings* on page 7-6.
Product Information	Not possible	This is the model and version of the Unit.
FSoE Slave Address	Possible	When the Active setting described above is set to **Enabled**, the **FSoE Slave Address** is automatically set as an internal address for use with FSoE communications. You can change the FSoE slave address. The setting range is from 1 to 65,535. Set a unique FSoE slave address for each FSoE slave in FSoE communications. If the same FSoE slave address is set more than once, an error is displayed on the Sysmac Studio.
FSoE Watchdog Timer*1	Possible	This is the setting of the timeout value for FSoE communications between the Safety CPU Unit and a Safety I/O Unit. The setting range is from the lowest value of the FSoE watchdog timers to 65,535 ms.
WDT auto setting*1	Possible	This setting specifies the setting method for the FSoE watchdog timer (WDT). Selected: The minimum value is set for FSoE Watchdog Timer (WDT). Cleared: You can set the FSoE watchdog timer (WDT) to the desired value.

*1. Refer to *Section 10 Calculating Safety Reaction Times* on page 10-1 for the FSoE watchdog timer.



Precautions for Safe Use

The relevant Units will maintain the safe states for I/O data with FSoE connections after an error is detected in FSoE communications. However, when the cause of the error is removed, FSoE communications will recover automatically.
If you need to prevent equipment from restarting when FSoE communications recover automatically, implement suitable restart conditions in the user program.

7-4 EtherNet/IP Network Configuration and Setup

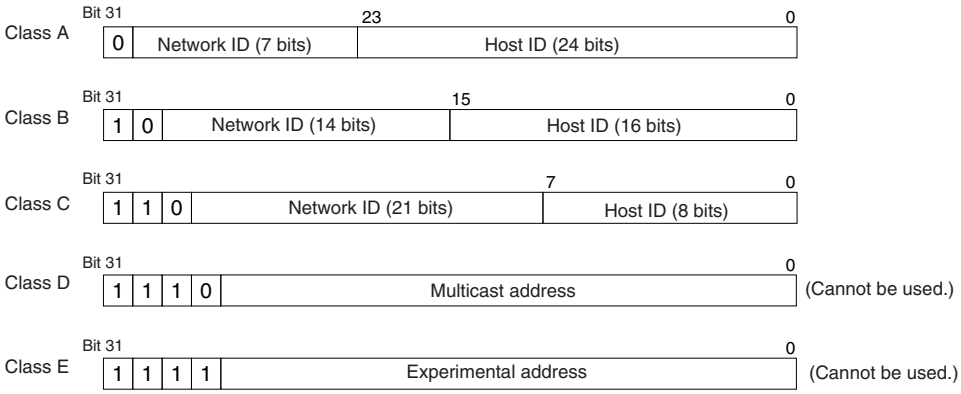
7-4-1 Setting IP Addresses

IP Addresses

● IP Address Configuration

IP addresses are made up of 32 bits of binary data that specify the network number (net ID) and host number (host ID). The network number identifies the network, and the host number identifies the node (or host) on the network.

IP addresses are divided into three classes, A, B, and C, so that the address system can be selected according to the scale of the network. (Classes D and E are not used.)



The number of networks in each class and the number of hosts possible on the network differ according to the class.

Class	Number of networks	Number of hosts
Class A	Small	2^{24}–2 max. (16,777,214 max.)
Class B	Medium	2^{16}–2 max. (65,534 max.)
Class C	Large	2^{8}–2 max. (254 max.)

The 32 bits of binary data in an IP address are divided into four sections of eight bits each. IP addresses are represented by the decimal equivalent of each of the four octets in the 32-bit address, each separated by a period.

For example, the binary address 10000010 00111010 00010001 00100000 would be represented as 130.58.17.32.

● Allocating IP Addresses

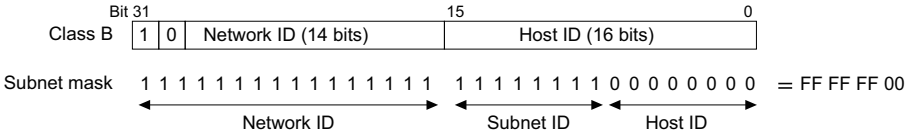
You must assign IP addresses nodes so that each IP address is assigned only once in the network or between several networks.

Subnet Mask

Operation and management of a network can become very difficult if too many nodes are connected on a single network. In such a case it can be helpful to configure the system so that a single network is divided up into several subnetworks. Internally the network can be treated as a number of subnetworks, but from the outside it acts as a single network and uses only a single network ID. To establish subnetworks, the host ID in the IP address is divided into a subnet ID and a host ID by using a setting called the subnet mask.

The subnet mask indicates which part of the host ID is to be used as the subnet ID. All bits in the subnet mask that correspond to the bits in the IP address used either as the network ID or subnet ID are set to "1", and the remaining bits, which correspond to the bits in the IP address actually used for the host ID, are set to "0".

The following example shows the subnet mask for an 8-bit subnet ID used in the class-B IP address.



Set the same subnet mask for all of the nodes on the subnetwork. The built-in EtherNet/IP port supports CIDR (Classless Inter-Domain Routing). The subnet mask can be set to 192.0.0.0 to 255.255.255.252.

If subnetworks are not used, set the following subnet mask values for IP address classes A to C.

Class	Subnet mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

A network address is information derived from a subnet mask and used to identify each network. A network address enables users to determine whether multiple nodes belong to the same network. A network address is calculated by performing a logical AND operation on the IP address and subnet mask of a node.

The following are examples of network address calculation.

In this example, the IP address of node 1 is set to *192.168.250.20*, the IP address of node 2 is set to *192.168.245.30*, and the subnet mask is set to *255.255.240.0*. The network addresses of the two nodes are calculated as follows.

- Calculating network address of node 1

Item	Decimal notation	Binary notation
IP address	192.168.250.20	11000000.10101000.11111010.00010100
Subnet Mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

- Calculating network address of node 2

Item	Decimal notation	Binary notation
IP address	192.168.245.30	11000000.10101000.11111010.00010100
Subnet Mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

As shown in the above tables, node 1 and node 2 have the same network address, which means these nodes belong to the same network.

● CIDR

CIDR, or classless interdomain routing, is used to assign IP addresses that do not use classes.
IP addresses that use classes are separated into blocks according to network IDs and host IDs, resulting in inefficient usage of IP address space.
CIDR does not use classes, so IP address space can be divided as required to more efficiently use IP address space.
For example, using a subnet mask setting with CIDR enables building a horizontally distributed network exceeding 254 nodes even if a class C address block (e.g., 192, 168...) is used.

Subnet Mask Range
192.0.0.0 to 255.255.255.252

Built-in EtherNet/IP Port IP Address Settings

● Determining IP Addresses

Use one of the following methods to set the IP address of the built-in EtherNet/IP port.
You can select different IP address setting method for Port 1 and Port 2, respectively.
No matter which method you use, you cannot specify the IP address that makes Port 1 and Port 2 belong to the same network.

Using the IP Address Switch

When you select **Fixed setting** for the IP address setting method under **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings on the Sysmac Studio and then set a value between *01* and *FE* to the IP address switch on the Communication Control Unit, you can specify the IP addresses as defined below.

Port 1:

Upper 24 bits: The IP address setting value for **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings (The default is 192.168.1)

Lower 8 bits: The settings of IP Address Switch 1

Port 2:

Upper 24 bits: The IP address setting value for **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings (The default is 192.168.250)

Lower 8 bits: The value set to IP Address Switch 2

Setting a User-specified IP Address

When you select **Fixed setting** for the IP address setting method under **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings on the Sysmac Studio and then set the IP address switch on the Communication Control Unit to *00*, the IP address specified on the Sysmac Studio is assigned to the port.

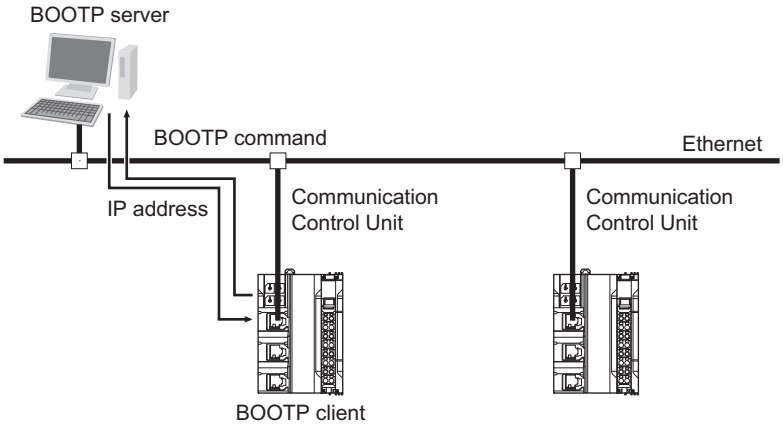
Automatically Obtaining an IP Address from the BOOTP Server

You can obtain an IP address from the BOOTP server in the following two methods.

- Obtaining an IP address from the BOOTP server at every power-on
  Set the IP address switch on the Communication Control Unit to *FF*.

You can also select **Obtain from BOOTP Server** for the IP address setting method in **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings on the Sysmac Studio and then set the IP address switch on the Communication Control Unit to *00*.

- Obtaining an IP address from the BOOTP server at initial power-on and setting the address as a fixed IP address
  Select **Fix at the IP address obtained from BOOTP server** for the IP address setting method in **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings on the Sysmac Studio and then set the IP address switch on the Communication Control Unit to *00*.



The relationship between the IP address switch on the Communication Control Unit and **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings is defined as follows.

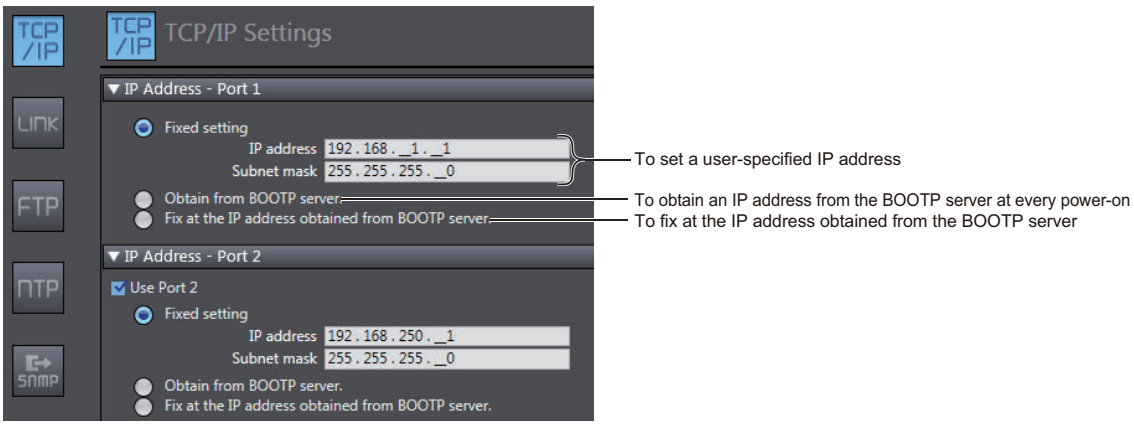
IP Address Switch Settings	TCP/IP Settings		
	Fixed setting	**Obtain from BOOTP server.**	**Fix at the IP address obtained from BOOTP server.**
00	The port will have the IP address specified in the **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings.	The port will have the IP address obtained from the BOOTP server at every power-on.	The port will have the IP address that was successfully obtained from the BOOTP server at the initial power-on. **Fixed setting** will be applied to **TCP/IP Settings** thereafter.

IP Address Switch Settings	TCP/IP Settings		
	Fixed setting	Obtain from BOOTP server.	Fix at the IP address obtained from BOOTP server.
01 to FE	The ports will have the following IP addresses.*1 Port 1: • Upper 24 bits: The IP address setting value for **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings (The default is 192.168.1) • Lower 8 bits: The value set to IP Address Switch 1 Port 2: • Upper 24 bits: The IP address setting value for **TCP/IP Settings** of the Built-in EtherNet/IP Port Settings (The default is 192.168.250) • Lower 8 bits: The value set to IP Address Switch 2	The *IP Address Switch Settings Error* is triggered and the communications are disabled.	
FF	The port will have the IP address obtained from the BOOTP server at every power-on.		

*1. If the network number portions of the Port 1 and Port 2 IP addresses are the same, the *IP Address Switch Settings Error* is triggered and the network communications are disabled.

● IP Address Setting using the Sysmac Studio

1 Select the setting method for IP addresses.
Make the following settings on the **TCP/IP** Settings Display of the Built-in EtherNet/IP Port Settings Tab Page in the Controller Setup to set a local IP address.



IP addresses must be set separately for built-in EtherNet/IP ports 1 and 2.

Precautions for Correct Use

You cannot set IP addresses that make two built-in EtherNet/IP ports belong to the same network.

2 Connect the personal computer in which the Sysmac Studio is installed to the Communication Control Unit via the Ethernet network.

3 Connect the Sysmac Studio online to the Communication Control Unit.



Additional Information

The first time you establish an online connection to the Communication Control Unit with Windows Firewall enabled after you installed Sysmac Studio, a dialog box may be displayed to confirm the connection. Click the **Allow access** button on the dialog box.
If you do not unblock (or allow access), you may not be able to download the settings of the built-in EtherNet/IP port.

4 Use one of the following methods to download the IP address settings that were specified on the Sysmac Studio to the Communication Control Unit.

1) Go online with the Controller, and then select **Synchronization** from the **Controller** Menu. The data on the computer and the data in the physical Controller are compared automatically.
2) Click the **Transfer to Controller** Button.

Note Use the "Synchronization" Menu of the Sysmac Studio to upload and download data.

5 After the IP address settings are downloaded, the IP address is reflected in the Communication Control Unit as follows:

- **Setting the User-specified IP Address**
  After the IP address settings are downloaded, the set IP address is automatically saved in the Communication Control Unit.
- **Obtaining the IP Address from the BOOTP Server Each Time the Power Is Turned ON**
  After the data is downloaded, the IP address from the BOOTP server is automatically saved in the Communication Control Unit.
  Each time the power supply is turned ON, the IP address from the BOOTP server is automatically saved in the Communication Control Unit.



Additional Information

If you cannot obtain the IP address from the BOOTP server or the obtained IP address is not correct, select the **Fixed setting** Option in the **IP Address** Area and manually set the IP address, subnet mask, and default gateway.
Requests to the BOOTP server to obtain the IP address will continue if there is a failure to connect to the BOOTP server.

- **Obtaining the IP Address from the BOOTP Server Once When the Power Is Turned ON and Then Not Allow It to Change**
  After the data is downloaded, an IP address is obtained from the BOOTP server and automatically saved in the Controller, and set as a fixed address in the **Fixed setting** Option.

Additional Information

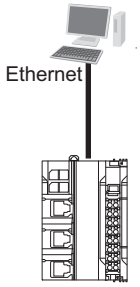
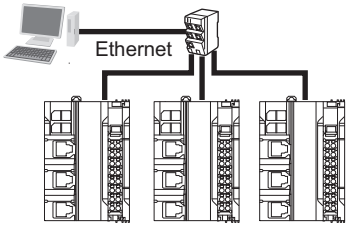
- The **TCP/IP** Settings Display is not updated even after the IP address is normally obtained from the BOOTP server.
  To check the IP address that was obtained from the BOOTP server, upload the project from the Communication Control Unit and check the Controller Status Pane.
- If you fail to obtain an IP address from the BOOTP server, the **Fix at the IP address obtained from BOOTP server** Option is selected in the **TCP/IP** Settings Display.
  If you do not obtain an IP address from the BOOTP server, select the **Fixed setting** Option in the **IP Address Settings**, and then manually set the IP address, subnet mask, and default gateway.
- If you fail to obtain an IP address from the BOOTP server, the setting still remains as **Fix at the IP address obtained from BOOTP server** when the Controller power is cycled.
- If the **Fix at the IP address obtained from BOOTP server** Option is selected, an IP address obtained from the BOOTP server for the built-in EtherNet/IP port is automatically set as **Fixed setting**. Therefore, the IP address will not match when the program is verified on the Sysmac Studio.

● Online Connection

Connect the Sysmac Studio online to the Communication Control Unit.

Types of Connection between the Communication Control Unit and Computer That Runs the Sysmac Studio

The Communication Control Unit and the computer that runs Sysmac Studio are connected via Ethernet as shown below:

Direct Connection via Ethernet (1:1 Connection with AutoIP)	Ethernet Connection via Hub (1:N Connection)
	
*1. An Ethernet switch is not necessarily required. *2. You can use a straight or cross Ethernet cable to connect. *3. 1:1 connection is possible only for the built-in EtherNet/IP port 1.	*1. An Ethernet switch is required to connect. Refer to the *Precautions for Ethernet Switch Selection* on page 5-40 for details.

Additional Information

- AutoIP is an automatic IP address assignment function supported by Windows 98 and later versions. Each node is automatically assigned a unique address, which is arbitrarily chosen from reserved addresses ranging from *169.254.0.0 to 169.254.255.255*.
- If the IP address of the connected EtherNet/IP port is changed when the Sysmac Studio is connected online via a built-in EtherNet/IP port, a timeout will occur in the Sysmac Studio. In the case, switch the Sysmac Studio status to offline, change to the IP address of the connected built-in EtherNet/IP port, and then switch back the Sysmac Studio status to online. This will allow you to reconnect.

Precautions for Correct Use

If there is more than one node with the same IP address in the EtherNet/IP network, the built-in EtherNet/IP port will connect to the node that is detected first.
Note that an IP Address Duplication Error will not be detected in this case.

Online Connection Procedure

Connect the Communication Control Unit and the computer that runs Sysmac Studio via Ethernet, and then perform the following procedure.

1. Select **Controller** - **Communications Setup** and click the **OK** Button in the Sysmac Studio Project Window.

· For 1:1 connection

● Direct connection

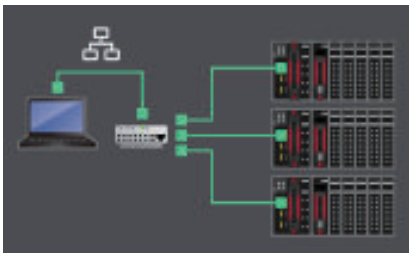
· Ethernet - Direct Connection



· For 1:N connection

● Ethernet connection

· Ethernet - Hub Connection



Additional Information

If there is an error in the set IP address, the Communication Control Unit behaves as follows:

- The NS (Port1/Port2) on Communication Control Unit turns off and the ERROR flashes in red.
- An *IP Address Setting Error* is recorded in the event log.

Precautions for Correct Use

- If the IP address is duplicated or not set correctly, communications are not possible via the EtherNet/IP network. Set the IP address again.
- The IP address range shown below is used by the system and cannot be specified.
  169.254.0.0 to 169.254.255.255
  192.168.255.0 to 192.168.255.255
- Due to Ethernet restrictions, you cannot specify the IP addresses that are described below.
  a) An IP address that is all 0's or all 1's
  b) IP addresses that start with 127, 0, or 255 (decimal)
  c) IP addresses that have a host ID that is all 0's or all 1's
  d) Class-D IP addresses (224.0.0.0 to 239.255.255.255)
  e) Class-E IP addresses (240.0.0.0 to 255.255.255.255)

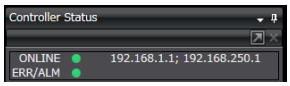
Connecting from a Saved Project

The connection configuration that is set is saved in the project.
If you open a saved project on the Sysmac Studio, you can connect to the EtherNet/IP network without redoing the settings.

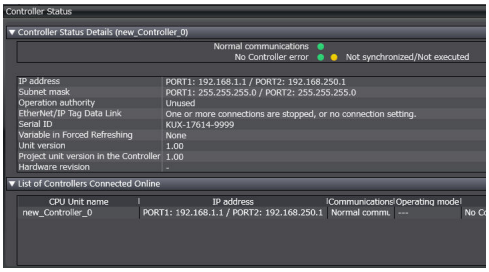
● Checking the Current IP Address

The current IP address can be confirmed in the Controller Status Pane of the Sysmac Studio, whether it is manually set or obtained from the BOOTP server.

- Basic Controller Status Pane



- Controller Status Pane with Details



Additional Information

- If you obtain the IP address from the BOOTP server, you can check the obtained IP address by synchronizing and uploading the controller settings from the Sysmac Studio.
- If the IP address of the built-in EtherNet/IP port is not registered due to the following reasons, the IP address field shows "0.0.0.0".
  a) The IP address was not obtained from the BOOTP server.
  b) The built-in EtherNet/IP port is set to disable. Refer to *TCP/UDP Message Communications* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for details on setting an IP address of the built-in EtherNet/IP port.

7-4-2 Setting Tag Data Links

This section explains the settings to establish a tag data link between the standard controller that acts as the originator device and the Communication Control Unit as the target device.

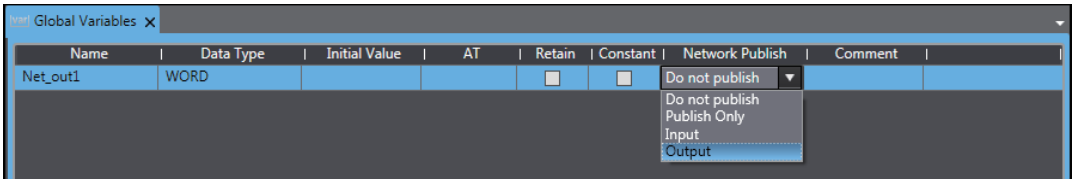
Creating Tags and Tag Sets

Use the following procedure to create tags and tag sets using Sysmac Studio.

● Registering Network Variables

You can register the data sent and received by the tag data link as the network variables.

1 On the global variable table of the Communication Control Unit, set the global variable setting **Network Publish** to **Input** or **Output**.



Additional Information

The following network variable names are not allowed.

- Variable names that contain only single-byte numerals from 0000 to 6143
- Variable names with the following single-byte letters (uppercase or lowercase) followed by single-byte numerals
  a) H (H000 to H511)
  b) W (W000 to W511)
  c) D (D00000 to D32767)
  d) E0_ to E18_ (E0_00000...E0_32767 to E18_00000...E18_32767)

Registering Tags and Tag Sets

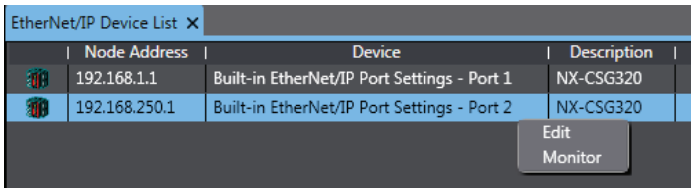
You can register tag sets required for tag data links.

Each tag set represents data that is sent and received through a connection. You can register up to 32 tags in one tag set. The name and size of a tag must be the same as those of the network variable. Set whether to include the Controller status information in tags for the tag sets. You can also set the data output operation at a fatal error occurrence for output tags.

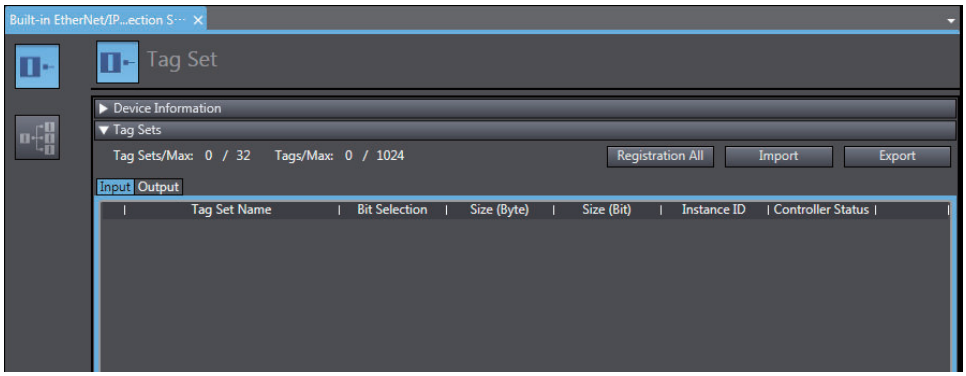
You can register tags and tag sets on the Built-in EtherNet/IP Connection Settings Tab Page.

1 On the main menu, select **Tools** – **EtherNet/IP Connection Settings** and show the EtherNet/IP Device List Tab Page.

2 Select **Built-in EtherNet/IP Port Settings - Port 2** of Communication Control Unit. Right-click and select **Edit** to show the Built-in EtherNet/IP Connection Settings Tab Page.



3 Click the  (Show Tag Set Display) icon in the Built-in EtherNet/IP Connection Settings Tab Page.



4 Click the **Input** Tab to switch to the **Input** Tab Page. Register the tag sets and tags.

You can register tag sets and tags by "Independent registration" or "Batch registration".

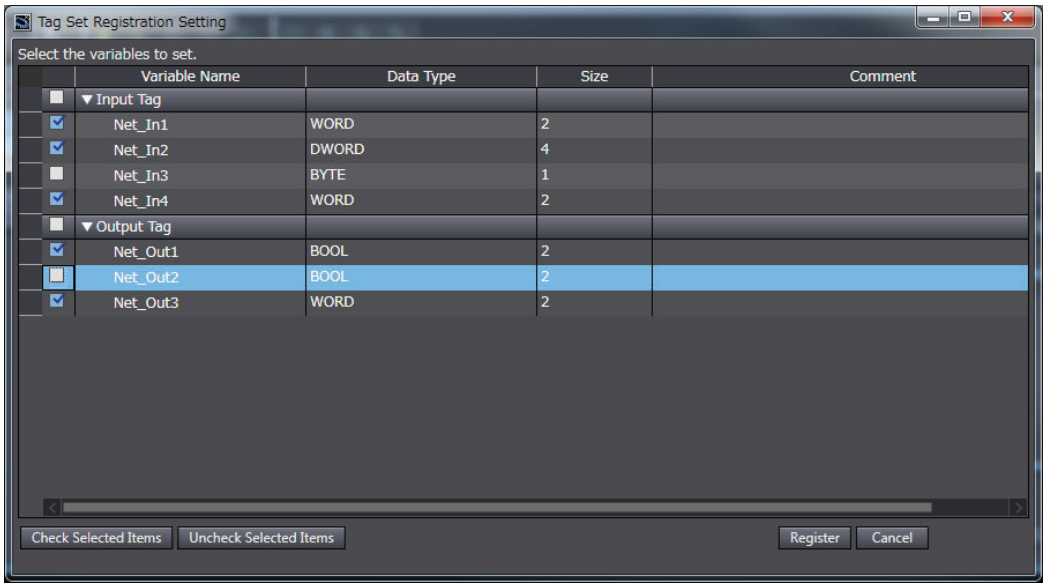
- Independent registration
  You can manually register network variables in the Controller as tags.

a) Right-click anywhere in the Input Tab Page of the Built-in EtherNet/IP Connection Settings Tab Page and select **Create New Tag Set** from the menu.
b) Enter a tag set name for the list in the **Input** Tab Page.
c) Right-click anywhere in the Input Tab Page and select **Create New Tag** from the menu.
d) Enter a tag name.

Precautions for Correct Use

You can specify any name for the tag set, however set the tag name to match one of the registered network variable names in the Controller.
When you enter a text or press the **Ctrl** + **Space** Keys, the input assist function of Sysmac Studio displays a list of variable names registered in the Communication Control Unit. You can select a name from the list.

- Batch registration
  You can register all network variables in the Controller as tags at the same time.
  a) Right-click anywhere on the Input Tab Page of the Built-in EtherNet/IP Connection Settings Tab Page and select **Register All Tag Sets** or click the **Registration All** Button to display the **Tag Set Registration Setting** Dialog Box.
  The **Tag Set Registration Setting** Dialog Box lists variables that are registered in the global variable table and also have the **Network Publish** attribute set to **Input** or **Output**.



  b) Select the variable to register as a tag, and then click the **Register** Button.
  c) The automatically registered tag is added to the list in the Built-in EtherNet/IP Connection Settings Tab Page. With automatic registration, the tag is registered under a tag set having the same name as the tag, i.e., a single tag is registered in a single tag set.
  d) Specify the following settings for the registered tags and tag sets.
  Settings for Tag Sets

Name	Setting Items
Tag Set Name	Enter a tag set name. You can change the tag set name to another one.
Size (Byte)	Gives the total size of the tag in bytes.

Name	Setting Items
Instance ID	Displays the Instance ID. • Auto • IN...{min}...IN...{max} {min} represents the minimum number of Produced Assembly ID recorded in the EDS files for the relevant devices. {max} represents the maximum number of Produced Assembly ID recorded in the EDS files for the relevant devices.
Controller Status	Select whether or not to include the Controller status in the tag set.

Settings for Tags

Name	Setting Items
Tag Name	Enter a tag name. For the tag name, use the name of the corresponding network variable that is registered in the Controller.
Bit Selection	Select whether or not to specify the tag data size in bits. Selected: Specify the size in bits. Not selected: Specify the size in bytes.
Size (Byte)	Gives the size of the tag in bytes.
Size (Bit)	Gives the size of the tag in bits.
Fault Action	When a controller error in the major fault level occurs with the Controller, select whether to clear output data or to continue sending data which was obtained before the error occurrence. • Retained • Cleared

5 Click the **Output** tab to switch to the **Output** Tab Page. Register the tag set and the tag.

Tag Data Link Connection Settings

You will configure the connection settings on the originator device only. For details on the setup method, refer to the user's manual for the originator device.

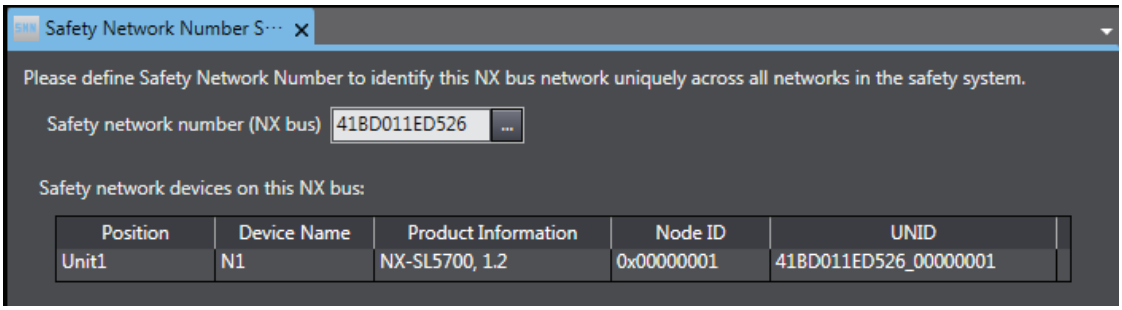
7-5 CIP Safety Communication Settings

7-5-1 Safety Network Number Settings for the NX Bus

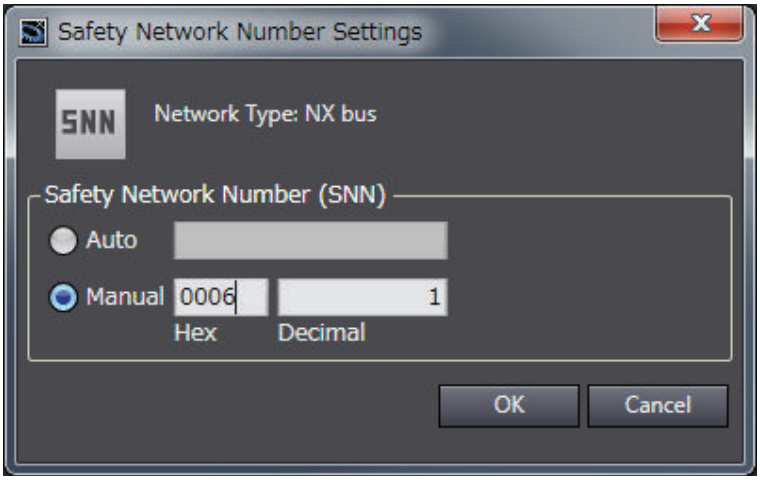
Use the following procedure to set the Safety Network Number (SNN) for the NX bus.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Select **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Safety Network Number Settings**.
The Safety Network Number Settings Tab Page is displayed.



3 Click the button located on the right side of Safety network number (NX bus).
The Safety Network Number Settings Dialog Box is displayed.



When you click the **Auto** Option, the Safety Network Number (SNN) is automatically generated from the current time information of the computer on which the Sysmac Studio is running.
When you click the **Manual** Option, enter a unique number that is not used in any other system.

4 Click the OK Button.
The Safety Network Number (SNN) is determined, and UNID is updated.

Additional Information

You can also enter the Safety Network Number (SNN) directly in the Safety Network Number Settings Tab Page.

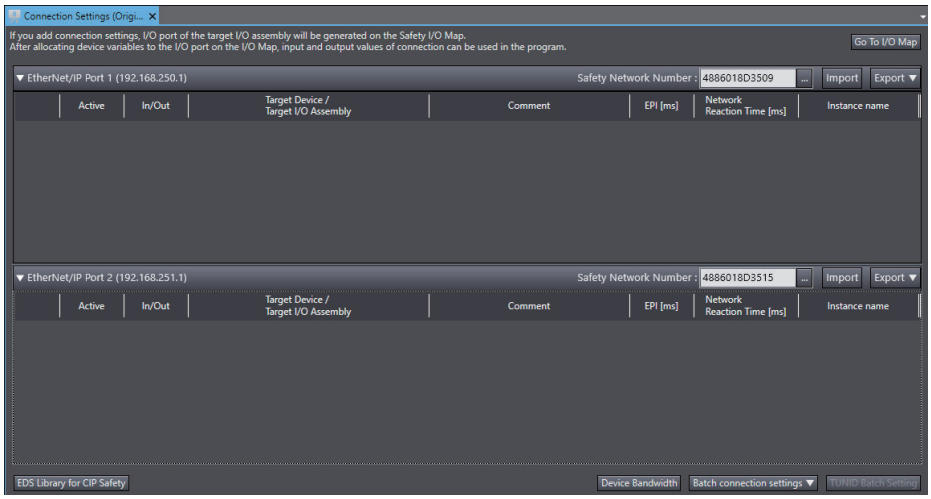
7-5-2 Originator Connection Settings

To use the Safety CPU Unit as an originator device for CIP Safety, the CIP Safety communications need to be set. Use the following procedure to set the CIP Safety communications.

Adding Target Devices

Use the following procedure to add a target device to open a CIP Safety connection.

1. In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.
2. Select **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.
   Connection Settings (Originator) Tab Page is displayed.
   A list of target devices that can be set for the connection is shown in the Toolbox.



The Connection Settings (Originator) Tab Page consists of the items shown in the following table.

Item	Description
EtherNet/IP Port 1	Settings of CIP Safety connections via the EtherNet/IP port 1 are listed. Safety Network Number: Specifies the SNN for the EtherNet/IP network for which the port 1 is connected Connection list: Connections grouped together by each target device are listed.
EtherNet/IP Port 2	Settings of CIP Safety connections via the EtherNet/IP port 2 are listed. Safety Network Number: Specifies the SNN for the EtherNet/IP network for which the port 2 is connected Connection list: Connections grouped together by each target device are listed.

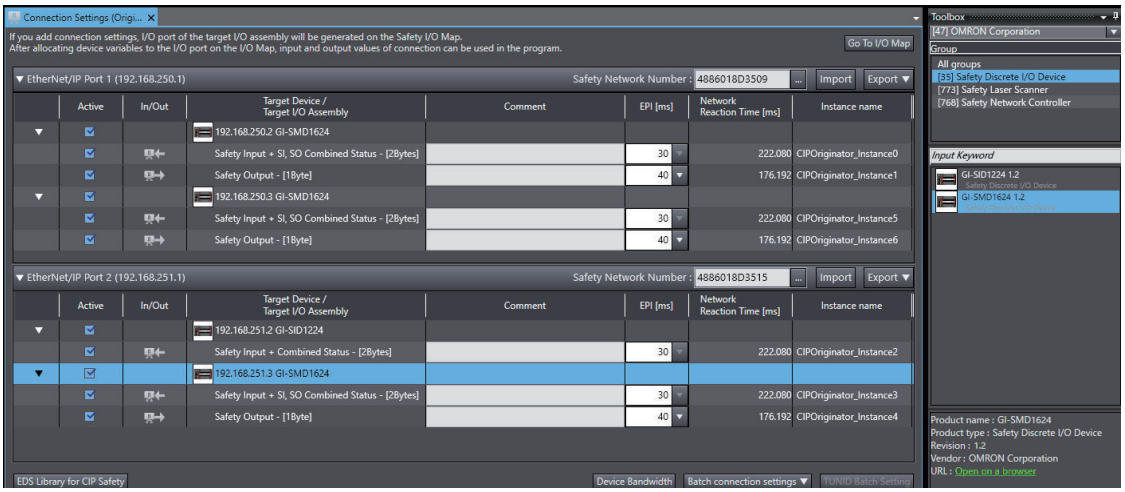
Item	Description
Target Device	IP address, Unit number, and device name are displayed for the target device with which a CIP Safety connection is to be opened.
In/Out	Shows the data direction of each connection.  : In - Data to be received from the target device  : Out - Data to be sent to the target device
Target I/O Assembly	I/O Assembly name of the target device with which a connection is to be opened is displayed.
Active	Enable/disable each connection. Selected: Connection is active. Not selected: Connection is inactive.
EPI [ms]	Specifies the Expected Packet Interval (data update cycle) in ms.
Network Reaction Time [ms]	Displays the value of the Network Reaction Time in ms. This is used in calculating the safety reaction time.
Instance name	Name of the instance being managed in the program. Connection status can be checked if the connection is registered in the Watch Tab Page.
Go To I/O Map Button	Click this button to open the I/O Map Tab Page.
Device Bandwidth Button	Click this button to show bandwidth usage of originator connection.
Import Button	Click this button to open the Import Dialog Box.
Export Button	**Output export file** or **Migrate to other EtherNet/IP port** can be selected from the pull-down menu.
EDS Library for CIP Safety Button	Click this button to display the **EDS Library for CIP Safety** Dialog Box. You can install, uninstall, create, and export EDS files.



Additional Information

If more than one Communication Control Unit is connected to the same EtherNet/IP network via a built-in EtherNet/IP port, the same Safety Network Number should be set for the built-in EtherNet/IP port of each Communication Control Unit.

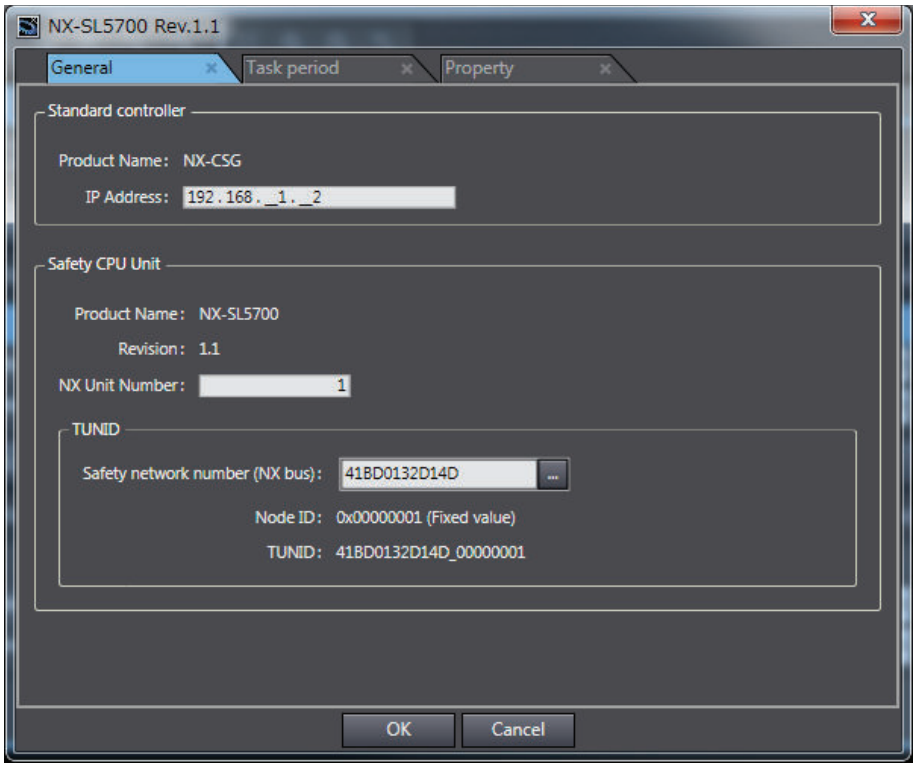
3 Select a target device to open a connection from the Toolbox. Drag and drop it on the connection list for either Port 1 or Port 2 to add the target device and default connection.



Setting the Target Device IP Address

Use the following procedure to set the address of the target device to open CIP Safety connection.

1 Select a target device in the connection list and right-click on it. Click the **Edit** Menu.
The target device settings pane is displayed.



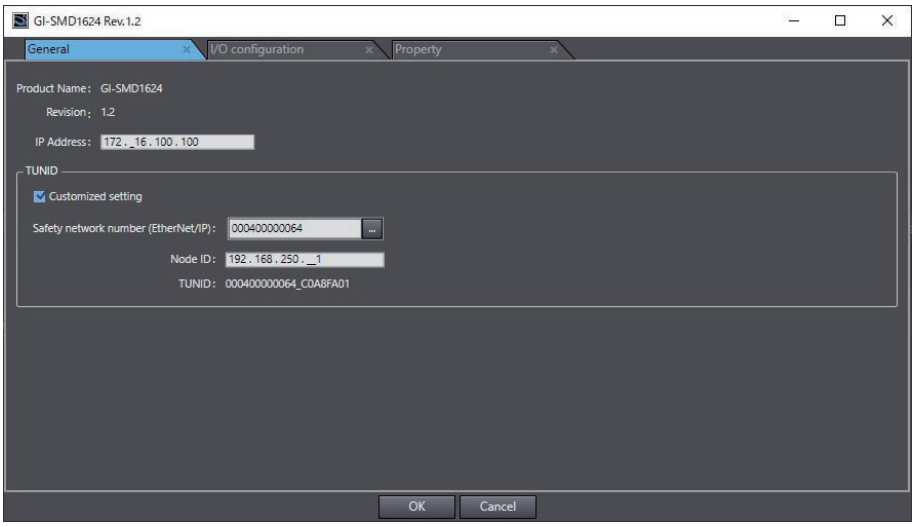
Change the displayed settings according to the actual target device settings.

The settings depend on a type of the target device as shown in the following table.

Target device type	Setting Items
Safety CPU Unit	IP Address: Specify the IP address for the EtherNet/IP port of the CPU Unit, Communication Control Unit, or EtherNet/IP Unit. NX Unit Number: Specify the NX Unit number of the Safety CPU Unit. Safety network number (NX bus): Specify the SNN in the TUNID that is set in the target Safety CPU Unit.
Other EtherNet/IP Safety devices	IP Address: Specify the IP address of the target device. TUNID - Customized setting: Select the check box to set a different safety network number or connection destined for Node ID.

Customized Setting for TUNID

When this setting is selected, you can set a desired TUNID for each target device as follows.



When this setting is used, you can set the connection for CIP Safety even in the following cases.

- When a desired safety network number is specified on the target device side
- When the target device is accessed via a router that uses the NAT function or NAPT function

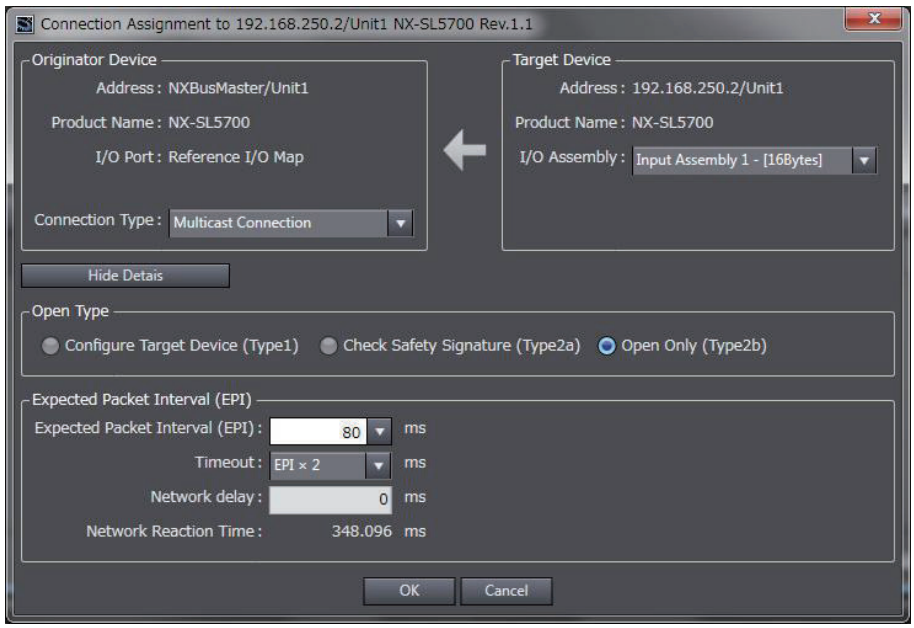
Editing Connection Parameters

Use the following procedure to edit connection parameters for CIP Safety connections.

⚠ WARNING

If you select “Open Only” for the Open Type setting, make sure to verify that the originator/target have correct configurations.
Serious injury may possibly occur due to loss of required safety functions.

1 Select a connection for which the parameters need to be edited in the connection list and right-click on it. Click **Edit** Menu.
The Connection Assignment Dialog Box is displayed.



Item	Description
I/O Assembly	I/O assemblies of the target device for which a safety connection can be opened are listed.
Connection Type	For input connection (receiving from the target device), select either **Point to Point Connection** or **Multicast Connection**.
Open Type	Select a type for connection opening. Configure Target Device: Perform configuration of the target device when a connection is established. For the Safety CPU Unit, this item cannot be selected. Check Safety Signature: Uses the safety signature to check if the target devices are properly configured when establishing the connection. The safety signature consists of the Safety Configuration CRC and the Safety Configuration Time Stamp. When the target device is the Safety CPU Unit, this item cannot be selected. Open Only: Configuration check is not executed when establishing the connection.
Expected Packet Interval (EPI)	Set an interval for communications of safety process data between the originator and the target.
Timeout	Specify a timeout time using a multiple of the EPI value, allowed for determining a communications error. The default setting is EPI x 2 [ms] (timeout is allowed just once).
Network Delay	Set the transmission delay time on the network. The default setting is 0 [ms].
Network Reaction Time	Value of the connection response performance is shown in ms. This is used in calculating safety reaction time.

2 Specify the connection parameter and click the **OK** Button.
A new connection is added to the connection list.

Adding Connections

Use the following procedure to add a CIP Safety connection with the target device.

1 Select a target device in the connection list and right-click on it. Click the **Create New Connection** Menu.
The Connection Assignment Dialog Box is displayed.



2 Specify the connection parameters and click the **OK** Button.
A new connection is added to the connection list.

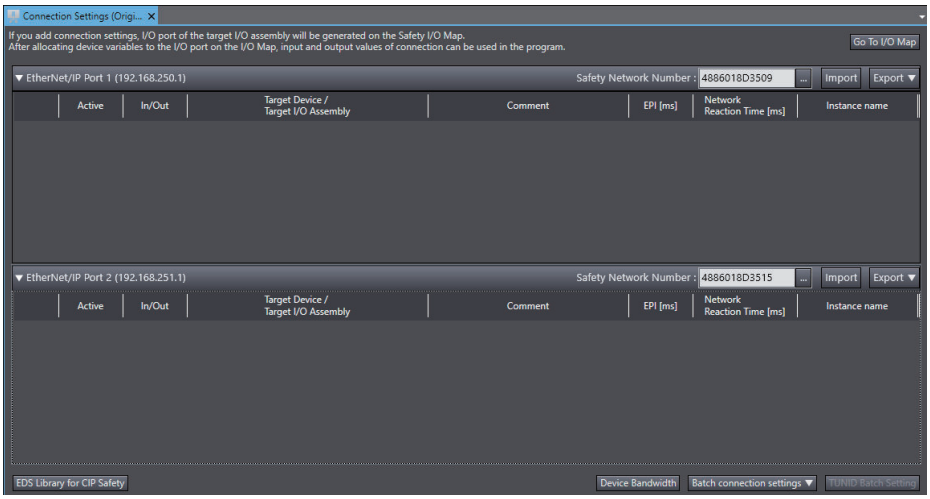
Batch Connection Settings

● EPI Batch Setting

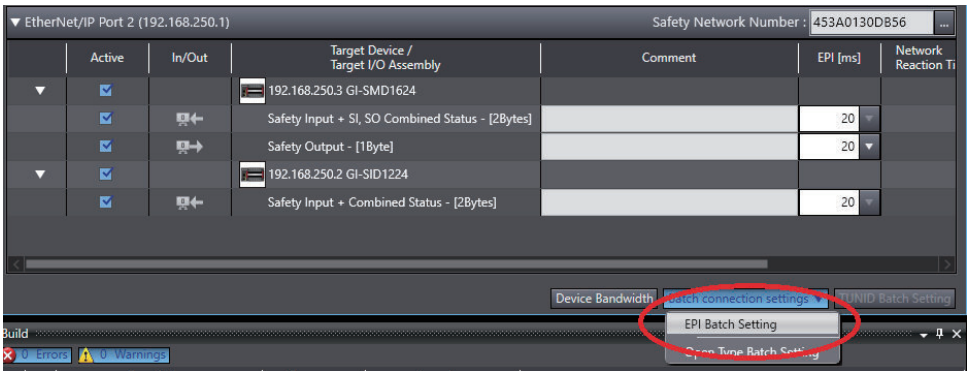
The function of EPI Batch Setting can change the EPI of the CIP Safety connections at once.
Refer to *10-4 EPI (Data Packet Interval)* on page 10-9 for the EPI (Data Packet Interval).
The procedure to use EPI Batch Setting is described below.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

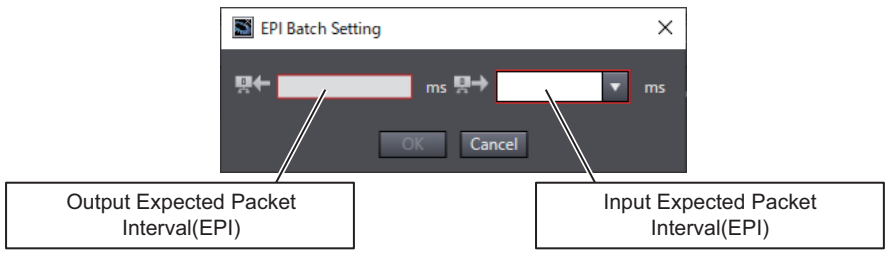
2 Go to **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.
The following Connection Settings (Originator) Tab Page is displayed.



3 Click the **Batch connection settings** button to select **EPI Batch Setting**.



The EPI Batch Setting window is displayed.



Item	Description
Input Expected Packet Interval (EPI)	Enter an EPI value for the CIP Safety input connections.
Output Expected Packet Interval (EPI)	Enter an EPI value for the CIP Safety output connections. You can select from the EPI values that can be set.

4 Click the **OK** button.
The EPI value that you entered or selected will be reflected in each CIP Safety connection setting in the project file.

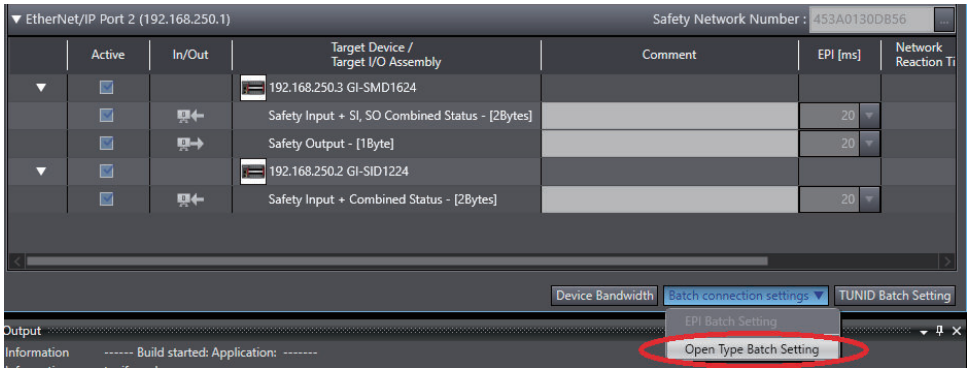
● Connection Open Type Batch Setting

The function of Connection Open Type Batch Setting can switch open types of connection parameters of CIP Safety connections at once. In addition, you can obtain safety signatures online from each target device on the network and reflect it in the target device settings.
Refer to *Editing Connection Parameters* on page 7-25 for connection open types.
The procedure to use Open Type Batch Setting is described below.

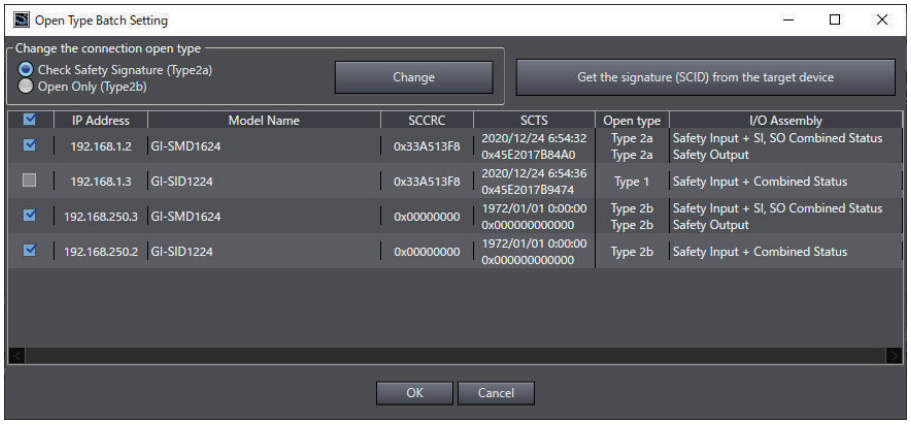
1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Go to **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.
The following Connection Settings (Originator) Tab Page is displayed.

3 Click the **Batch connection settings** button to select **Open Type Batch Setting**.



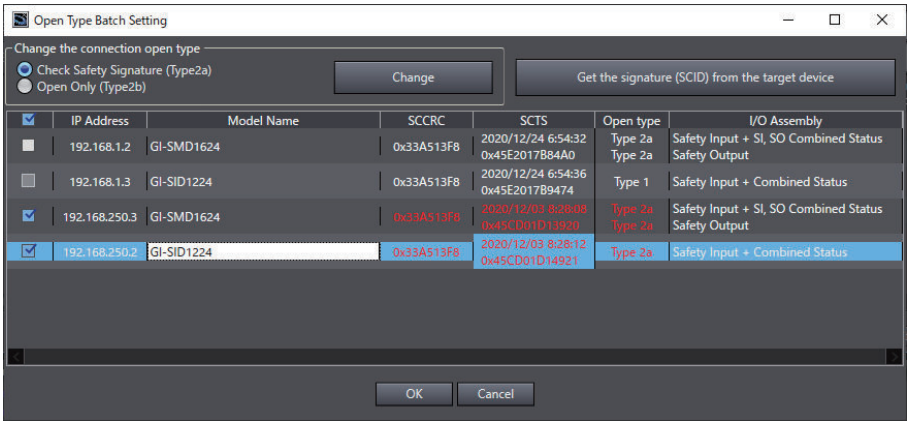
The Open Type Batch Setting window is displayed.



The Open Type Batch Setting window consists of the items shown in the following table.

Item	Description
Target Device Selection Check Box	Select target devices that change the open types or those that obtain and change the signature codes. Unchecked target devices are not be subject to setting changes.
Target List	Displays IP addresses, model names, signature codes (SCCRC and SCTS), open types of each connection, and I/O assemblies, of target devices.
The Type 2a/Type 2b Selection Button	Select the open type. Type2a: Check Safety Signature Type2b: Open Only
The **Change** Button	Reflects the open types selected with the Type 2a/Type 2b buttons in the target list. At that point in time when you click the **Change** button, they are not reflected in the project file. Only after you click the OK button, they will be reflected in the project file.
The **Get the signature (SCID) from the target device** Button	When you connect to the Communication Control Unit online, you can obtain the signature codes from the target devices for which Type 2a are set in the open types.

The text colors will change to red when you change any settings.



4 Confirm the changed contents and click the **OK** button.
The set open types and safety signatures (SCCRC and SCTS) of the target devices will be reflected in the project file.

Additional Information

Change the open type to Type2a and then press the **Get the signature (SCID) from the target device** button to obtain safety signatures from the target devices.

Target Device Operation

This function sets and operates a target device on the network online. The availability of each function depends on the operation specifications of the target device.

Function	Description	Calling method
Clear Memory	Clears the settings of target device.	Right-click the device to be set and select**Target Device–Clear Memory**.
TCP/IP Settings	Sets such as the IP address of the target device.	Right-click the device to be set and select**Target Device–TCP/IP Settings**.

Function	Description	Calling method
TUNID Setting (Individually)	Sets TUNID of the target device.	Right-click the device to be set and select**Target Device**–**TUNID Setting**.
TUNID Batch Setting	Sets TUNID of multiple target devices at once.	Click the**TUNID Batch Setting**button.
Restart	Restarts the target device.	Right-click the device to be set and select**Target Device**–**Restart**.
Lock	Locks the configuration for the target device.	Right-click the device to be set and select**Target Device**–**Lock**.
Unlock	Unlocks the configuration for the target device.	Right-click the device to be set and select**Target Device**–**Unlock**.

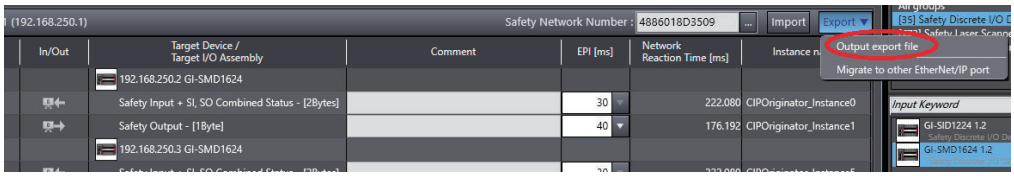
Precautions for Correct Use

- This function depends on the operation specifications of the target device. Some operations are not supported depending on the device functions.
- If you set TUNID to the target device, make sure that the correct TUNID is set to the intended device under your responsibility. Also, ensure that all TUNIDs are unique across the system.

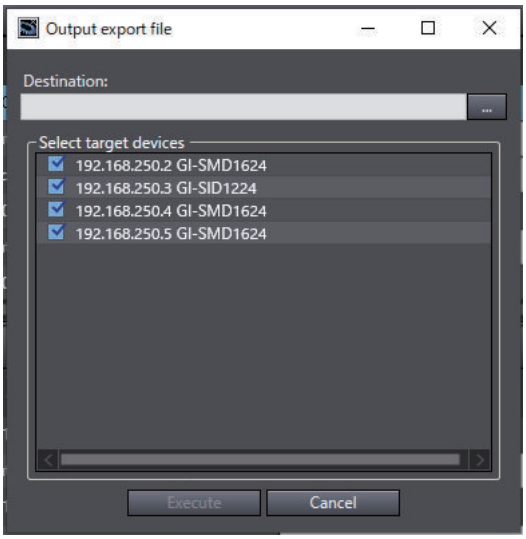
Batch Export

You can use the batch export function to output CIP Safety connection settings for each EtherNet/IP port to an export file or move the settings to other EtherNet/IP port. The procedure for outputting to an export file is shown below.

1. In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.
2. Go to **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.
3. Click the **Export** Button and select **Output export file**.



The Output export file Dialog Box is displayed.



The contents of the setting dialog box are as follows.

Item	Description
Destination	Specify the export file (.tdsg extension) for the destination.
Select target devices	Select the target devices to output to the export file.

4 Select the destination and target devices and click the **Execute** Button.
A batch export file for CIP Safety connection settings with a .tdsg extension is saved.

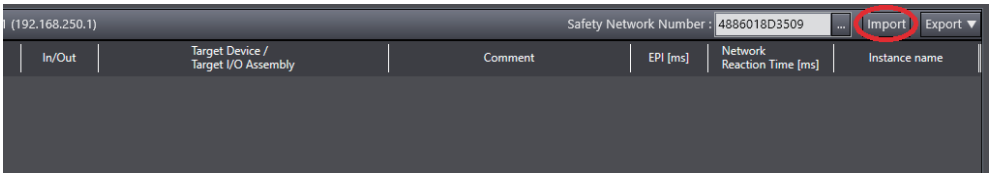
Batch Import

You can use the batch import function to import CIP Safety connection settings for each EtherNet/IP port. Use the following procedure.

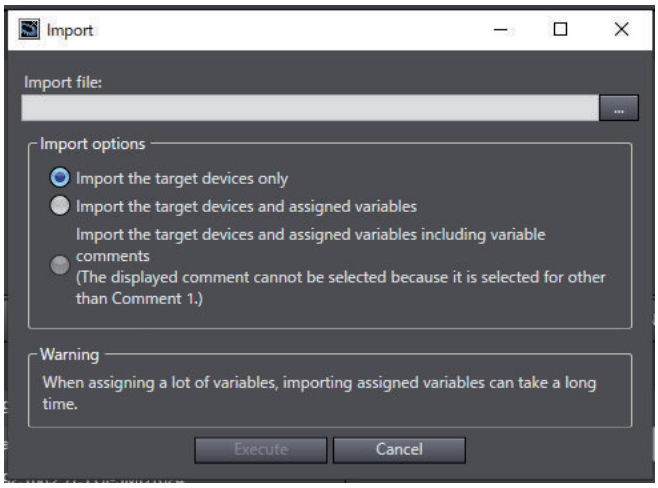
1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Go to **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.

3 Click the **Import** Button.



The Import Dialog Box is displayed.



The contents of the setting dialog box are as follows.

Item	Description
Import file	Specify the file to be imported (extension .tdsg).
Import options	Select the import option. You can import data including assigned variables and variable comments. If the display comment is selected other than comment 1 in the option setting, the variable comments cannot be imported.

4 Select the import file and import option, and click the **Execute** Button.
The connection settings to be imported are added to the Connection Settings (Originator) Tab Page.

Precautions for Correct Use

When you import the target device configuration file, the data integrity is not checked by CRC. Always validate the correct configuration under your responsibility after the import and assure proper execution before you use it for actual operation.

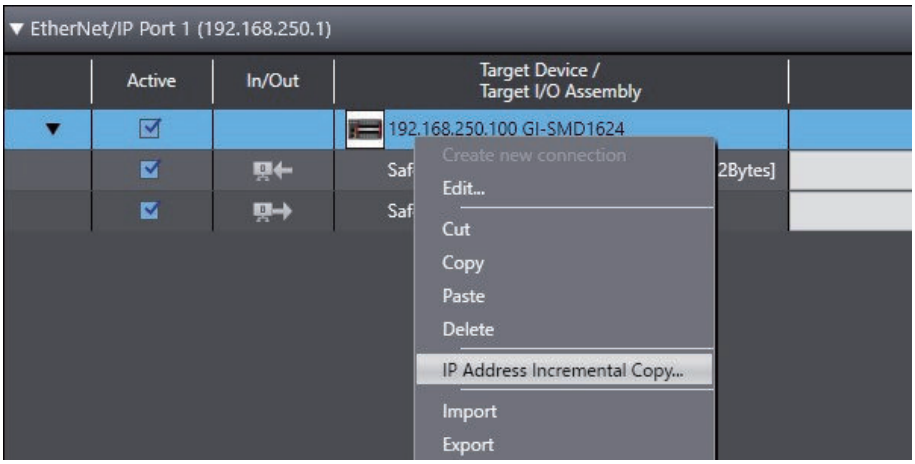
IP Address Incremental Copy

You can use the IP address incremental copy function to replicate the CIP Safety connection setting that has a difference only in the IP address part. Use the following procedure.

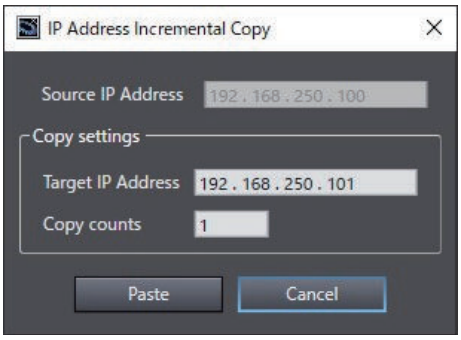
1 In the Multiview Explorer, select the Safety CPU Unit in the Controller Selection Box.

2 Go to **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.

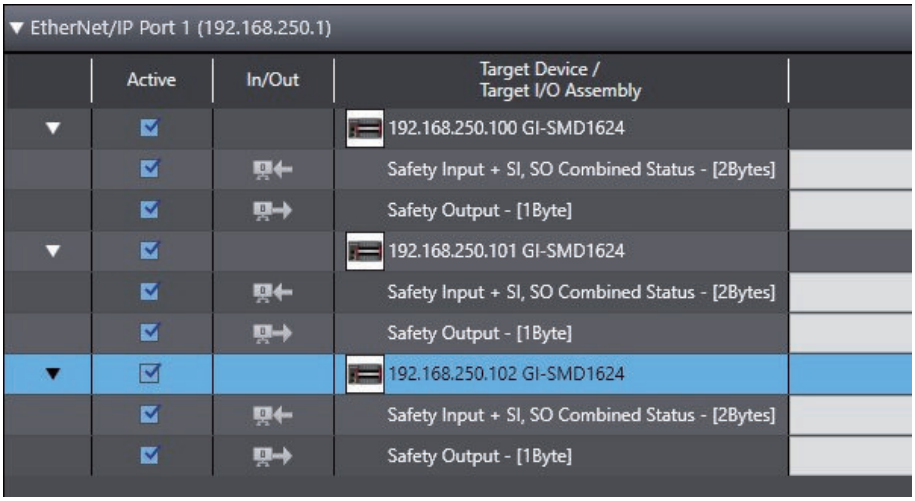
3 Select desired CIP Safety connection, and right-click the connection and select **IP Address Incremental Copy**.



The IP Address Incremental Copy window is displayed.



4 Enter the target IP address and copy counts, and then click the Paste button.
The CIP Safety connection setting will be replicated by adding one to the IP address part for the amount of the copy counts.

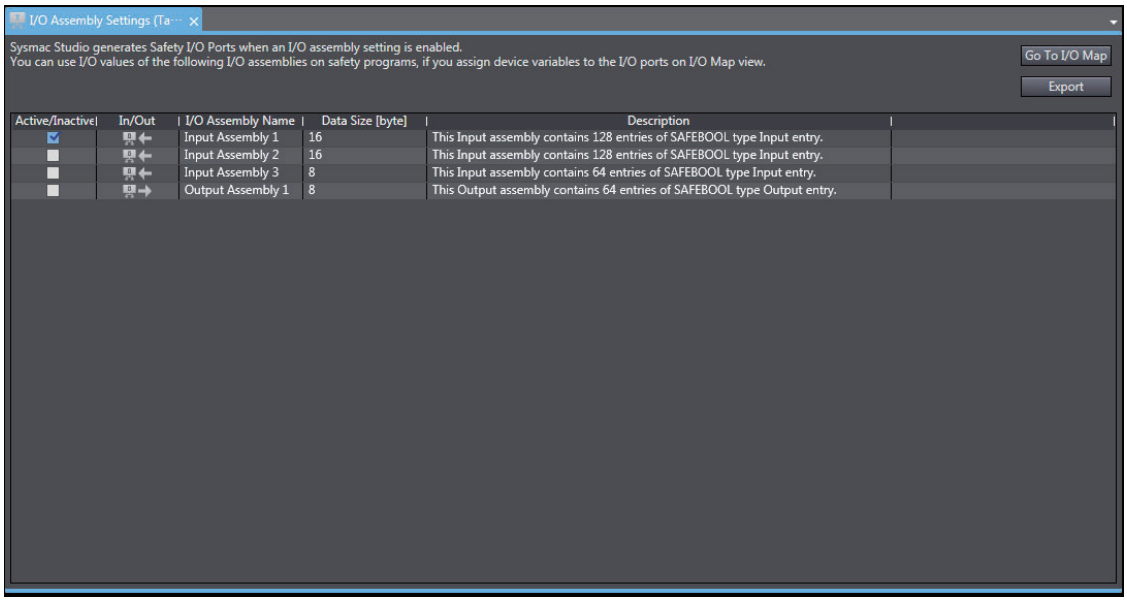


7-5-3 Target I/O Assembly Settings

To execute the CIP Safety I/O communications between the Safety CPU Units, you need to configure the I/O Assembly settings on the target Safety CPU Unit.
This section describes the procedure to enable or disable the I/O Assembly on the I/O Assembly Settings Tab Page in the Sysmac Studio.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Select **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **I/O Assembly Settings (Target)**.
The I/O Assembly Settings (Target) Tab Page is displayed.



The I/O Assembly Settings (Target) Tab Page consists of the items shown in the following table.

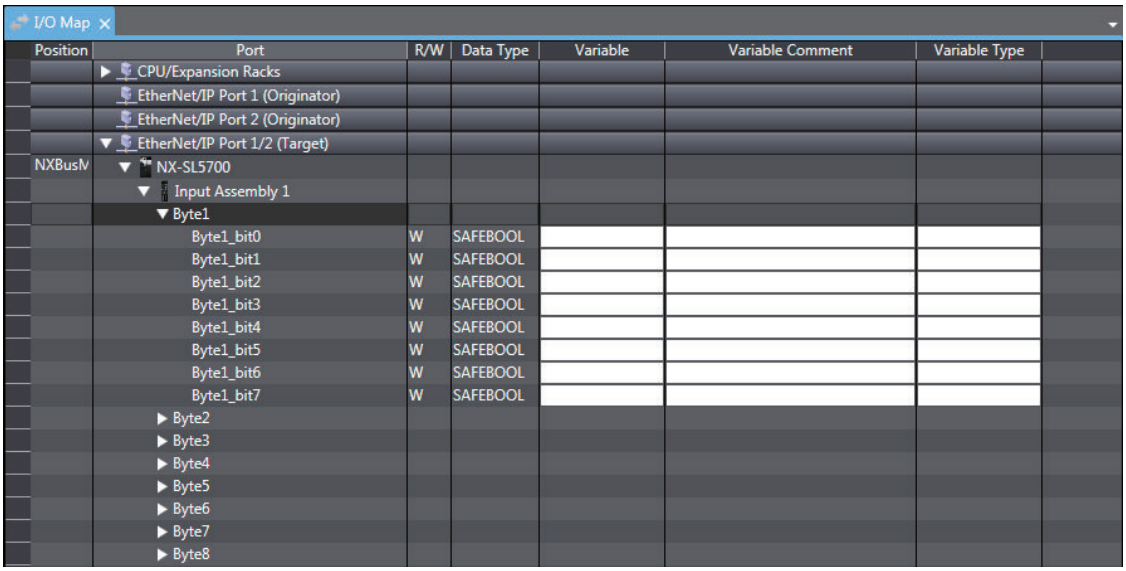
Item	Description
Active/Inactive	Use this box to enable or disable each I/O Assembly. When you enable the assembly, a port is added to the I/O Map. Selected: I/O Assembly is enabled. Not selected: I/O Assembly is disabled.
In/Out	Shows the data direction of each I/O Assembly. : In – Data sent to the originator device. : Out – Data received from the originator device.
I/O Assembly Name	The name of each I/O Assembly is displayed. It is same as the port name displayed on the I/O Map.
Data Size [byte]	The byte size of each I/O Assembly is displayed.
Description	The description of each I/O Assembly is displayed.
Go To I/O Map Button	Click this button to open the I/O Map Tab Page.
Export Button	Exports the target device settings as a file (extension .tds).

The following lists the types of selectable I/O Assembly.

Name	Assembly number	Data direction	Size
InputAssembly 1	768(0x300)	Input – Data sent to the originator device	16 bytes (SAFEBOOL × 128)
InputAssembly 2	769(0x0301)	Input – Data sent to the originator device	16 bytes (SAFEBOOL × 128)
InputAssembly 3	770(0x0302)	Input – Data sent to the originator device	8 bytes (SAFEBOOL × 64)

Name	Assembly number	Data direction	Size
OutputAssembly 1	928(0x03A0)	Output – Data received from the originator device	8 bytes (SAFEBOOL × 64)

The activated I/O Assembly is displayed as a port on the I/O Map of the originator device to communicate with as shown below. You can use it on a safety program by assigning a variable to the I/O port.



Precautions for Correct Use

The I/O Assembly for the Safety CPU Unit cannot be used with the tag data link connection.

7-5-4 Connecting Target Devices of Other Manufacturers

To configure the CIP Safety communication settings for target devices manufactured by other companies, you need to create or install the EDS file for non-OMRON target devices.

Creating an EDS File

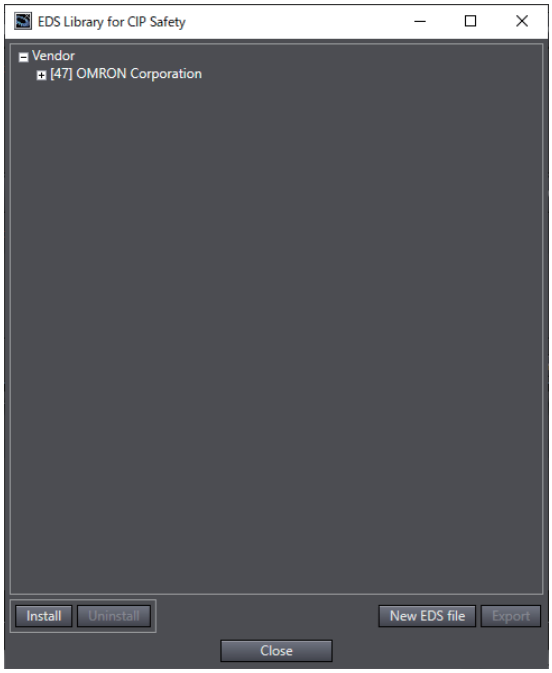
This function can create an EDS file to set CIP Safety connections with a CIP Safety target device.

Precautions for Correct Use

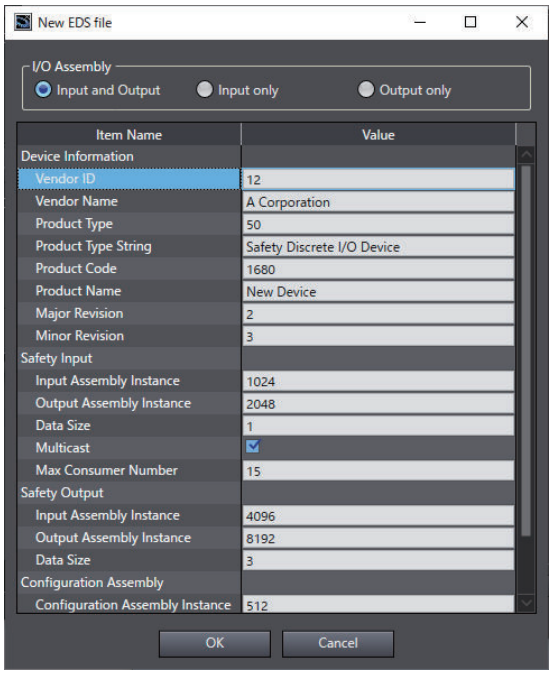
- For contents to be specified, contact the manufacturer of the target devices.
- Always validate correct operations of the connection established by using the created EDS files under your responsibility before you use it for actual operation. If there is an error in the created EDS file, the Safety CPU Unit and the target device may not be able to connect.
- You can determine the created EDS (target device) by the EDSFileCRC since the EDSFileCRC is automatically generated according to the contents of the EDS file. Make sure that the displayed EDSFileCRC is what you intended, when you use the created EDS (target device).

The following procedure describes how to create an EDS file.

1 Right-click on the Connection Settings (Originator) screen and select the menu **EDS Library for CIP Safety**.
The EDS Library for CIP Safety screen is displayed.



2 Click the **New EDS file** button.
The New EDS file window is displayed.

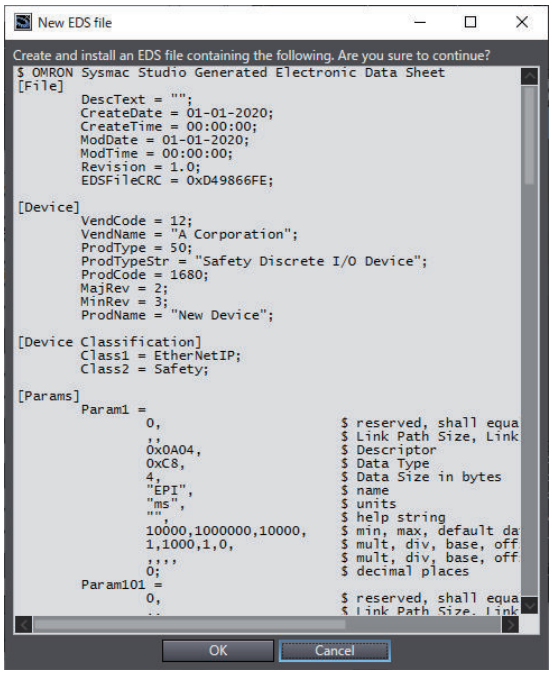


Specify the information of the target device.

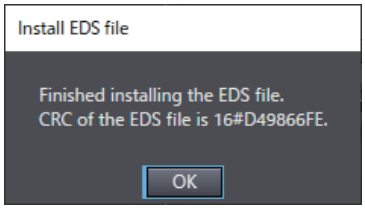
Item	Description
I/O Assembly	Select the I/O assembly supported by the target device. Input and Output: Select Input and Output when the target device supports the input and output connections. Input only: Select Input only when the target device supports the input connection only. Output only: Select Output only when the target device supports the output connection only.
Device Information	Specify the ID information of the device.
Vendor ID	Specify the vendor ID of the target device. Used for the connection settings with the target device.
Vendor Name	Specify the vendor name of the target device. Used for display on the Sysmac Studio.
Product Type	Specify the product type of the target device. Used for the connection settings with the target device.
Product Type String	Specify the vendor name of the target device. Used for display on the Sysmac Studio.
Product Code	Specify the product code of the target device. Used for the connection settings with the target device.
Product Name	Specify the product name of the target device. Used for display on the Sysmac Studio.
Major Revision	Specify the major revision of the target device. Used for the connection settings with the target device.
Minor Revision	Specify the minor revision of the target device. Used for the connection settings with the target device.
Safety Input	Enter the safety input connection information.
Input Assembly Instance	Specify the instance number of the input assembly for the safety input connection.
Output Assembly Instance	Specify the instance number of the output assembly for the safety input connection.
Data Size	Specify the data size of the safety input connection.
Multicast	Check the check box to use the multicast connection.
Max Consumer Number	Specify the maximum number of consumers when you use the multicast connection.
Safety output	Enter the safety output connection information.
Input Assembly Instance	Specify the instance number of the input assembly for the safety output connection.
Output Assembly Instance	Specify the instance number of the output assembly for the safety output connection.
Data Size	Specify the data size of the safety output connection.
Configuration Assembly	Enter the configuration assembly information.
Configuration Assembly Instance	Specify the instance number of the configuration assembly.
Format Type	Specify the format type of the CIP Safety communications.
Safety Format Support	Select the supported format from the following. Base Only: Only Base format is supported. Extended Only: Only Extended format is supported (default). Base and Extended: Both Base and Extended formats are supported.

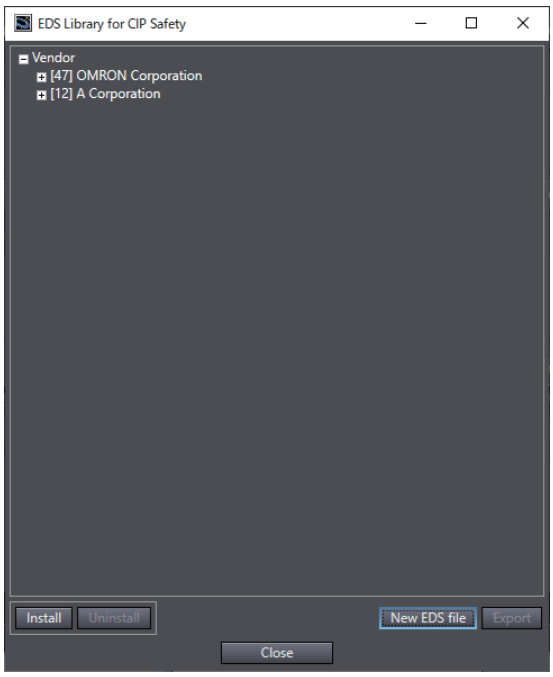
3 Click the **OK** button to display the EDS contents to be created.

Check the contents and click the **OK** button.



4 The created EDS file is registered in the EDS Library for CIP Safety screen. After the registration is completed, the EDSFileCRC will be displayed in the dialog.

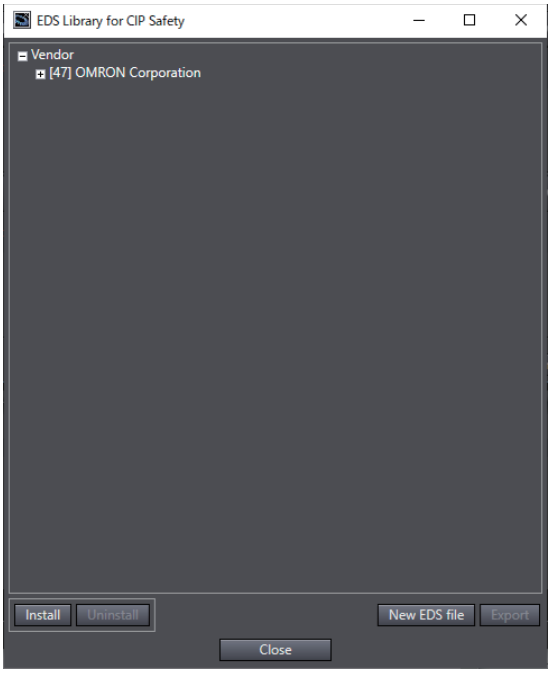




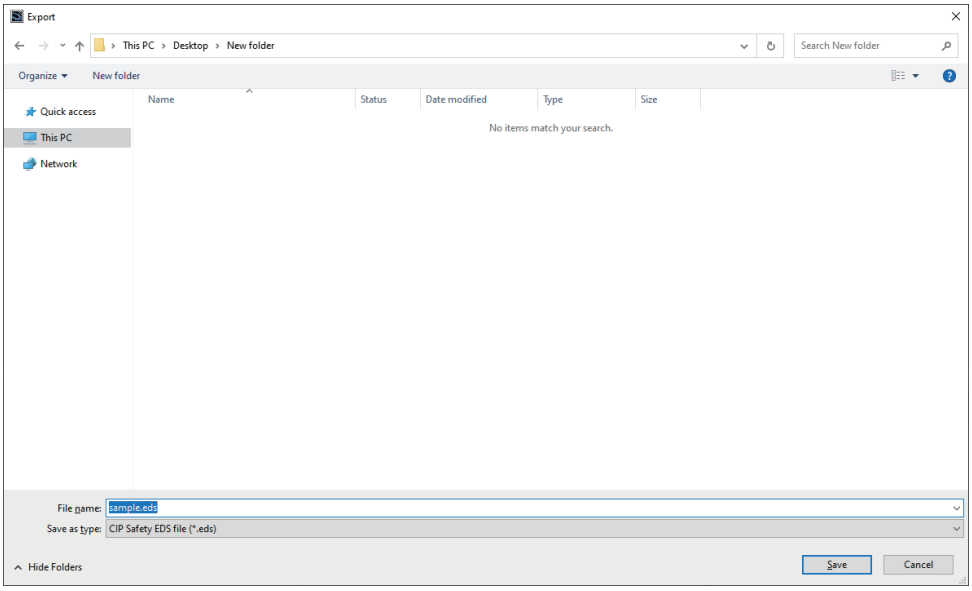
Exporting the EDS File

You can reuse the created EDS file on other computers by exporting it.
The procedure to export the EDS file is described below.

1 Right-click on the Connection Settings (Originator) screen and select the menu **EDS Library for CIP Safety**.
The EDS Library for CIP Safety screen is displayed.



2 Click the **Export** button.
The export window is displayed.

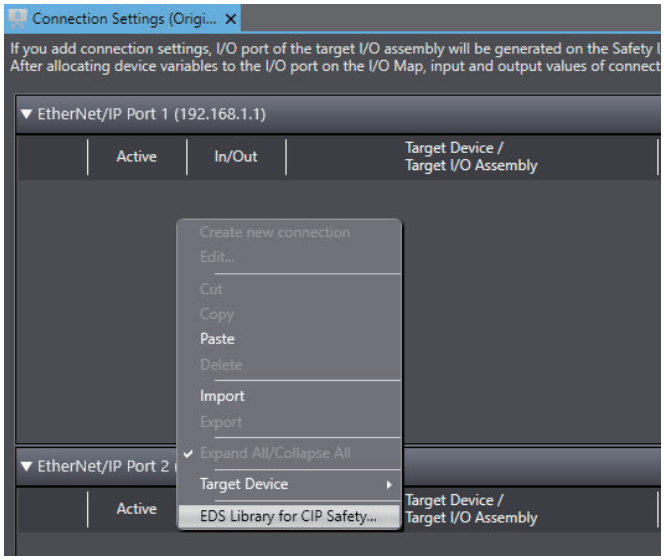


Specify the folder and the file name and then click the **Save** button to save the EDS file.

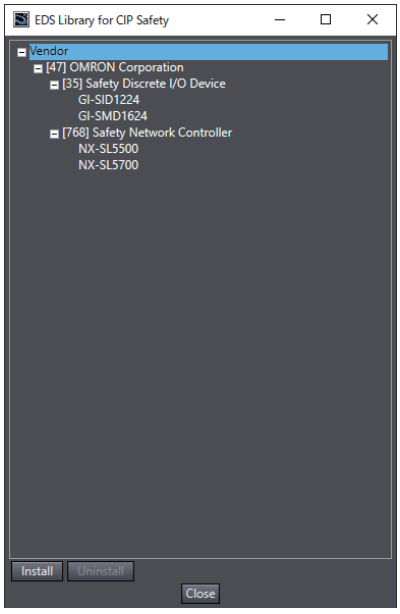
Installing the EDS File

You can install and reuse EDS files created on other computers.
The procedure to install the EDS file is described below.

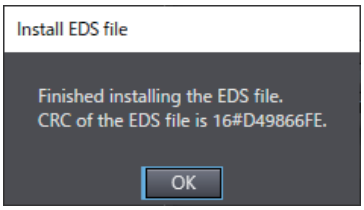
1 Right-click on the Connection Settings (Originator) screen and select the menu **EDS Library for CIP Safety**.



The EDS Library for CIP Safety screen is displayed.



2 Click the **Install** button and select the EDS file for the target device you will add. Then, click the **Open** button.
After the installation is completed, the EDSFileCRC will be displayed in the dialog. Make sure the intended EDS is installed.



3 The non-OMRON target device is added to the EDS Library for CIP Safety.

4 Click the **Close** button to close the EDS Library for CIP Safety screen. The device registered to the EDS Library for CIP Safety is displayed in the list of connectable target devices in the Toolbox on the Connection Settings (Originator) screen.

Precautions for Correct Use

- If you install third-party EDS files, always validate correct operations of the connection established by using the installed EDS files under your responsibility before you use it for actual operation.
- Make sure that the displayed EDSFileCRC is what you intended, when you use the installed EDS (target device).
- EDS files (target devices) with different EDSFileCRCs are registered as different target devices.
- In order to open a project file, you need to install the EDS files for the target devices included in the project file.

Additional Information

For details on the target devices that can be configured in the CIP Safety communication settings, contact the manufacturer of the target devices.

Uninstalling the EDS File

To uninstall the EDS file, select a target device to delete from the list on the EDS Library for CIP Safety screen, and then click the **Uninstall** button.

7-6 Setting the Input and Output Functions

This section describes setting procedures of the input and output functions for NX Units.

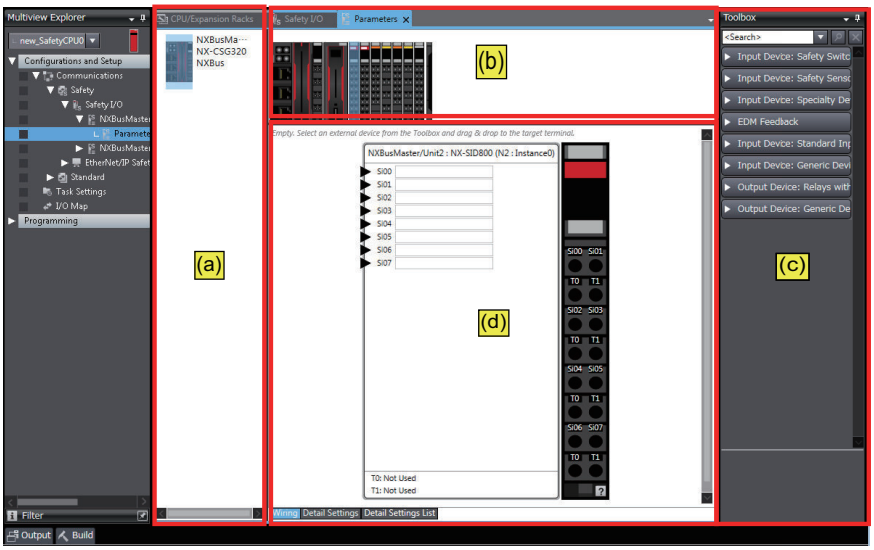
7-6-1 Safety I/O Functions

You set the safety input functions and safety output functions of the Safety I/O Units when you assign input devices and output devices to the Safety I/O Units with the Sysmac Studio.

This section describes how to assign devices that are connected. Refer to *6-3-1 Safety Input Function* on page 6-16 and *6-3-2 Safety Output Function* on page 6-38 for details on the safety input functions and safety output functions.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Go to **Configurations and Setup** – **Communications** – **Safety** – **Safety I/O**. Under the Safety I/O Unit name, double-click **Parameters**.
The Parameters Tab Page shown below is displayed.

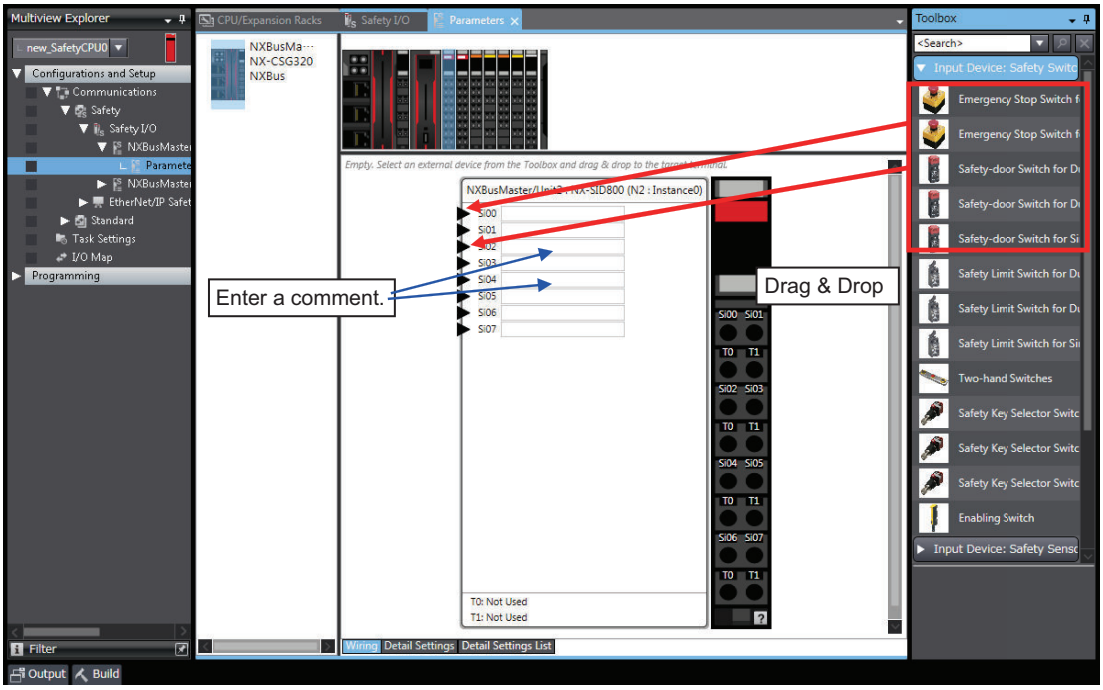


The items in the Parameters Tab Page of safety slave unit setting are described below.

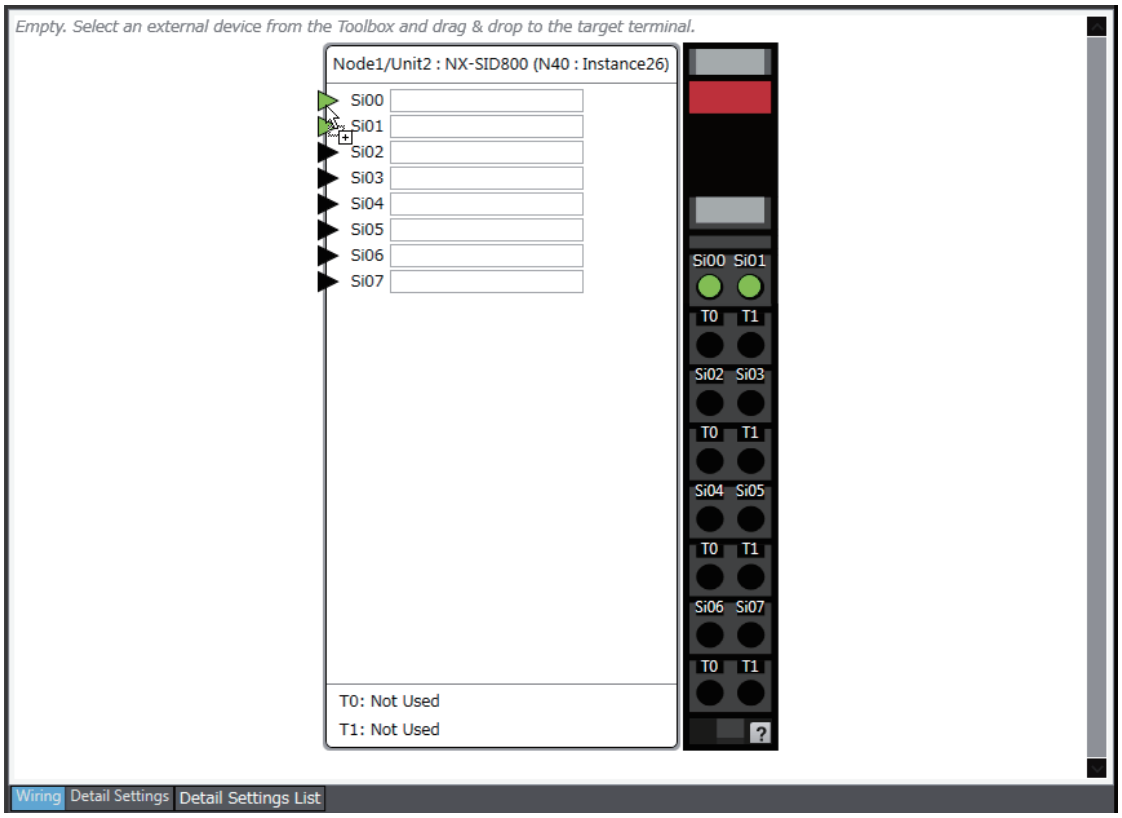
Letter	Name	Function
(a)	NX Bus Master List Pane	This pane lists NX bus masters to which the Safety I/O Unit that can perform safety communications with the Safety CPU Unit is mounted.
(b)	NX Unit Configuration Pane	This pane shows the configuration of the NX Units that are connected to the NX bus master.
(c)	Toolbox	The toolbox displays the input and output devices that can be set for the Safety I/O Units.

Letter	Name	Function
(d)	Parameter Settings Pane	This pane is used to make settings for the input and output devices that are set for the Safety I/O Units. You can arrange the devices, set diagnosis functions, change icons, etc. Refer to *A-9 Icon list for Safety Slave Unit Parameters* on page A-83 for details on changing icons.

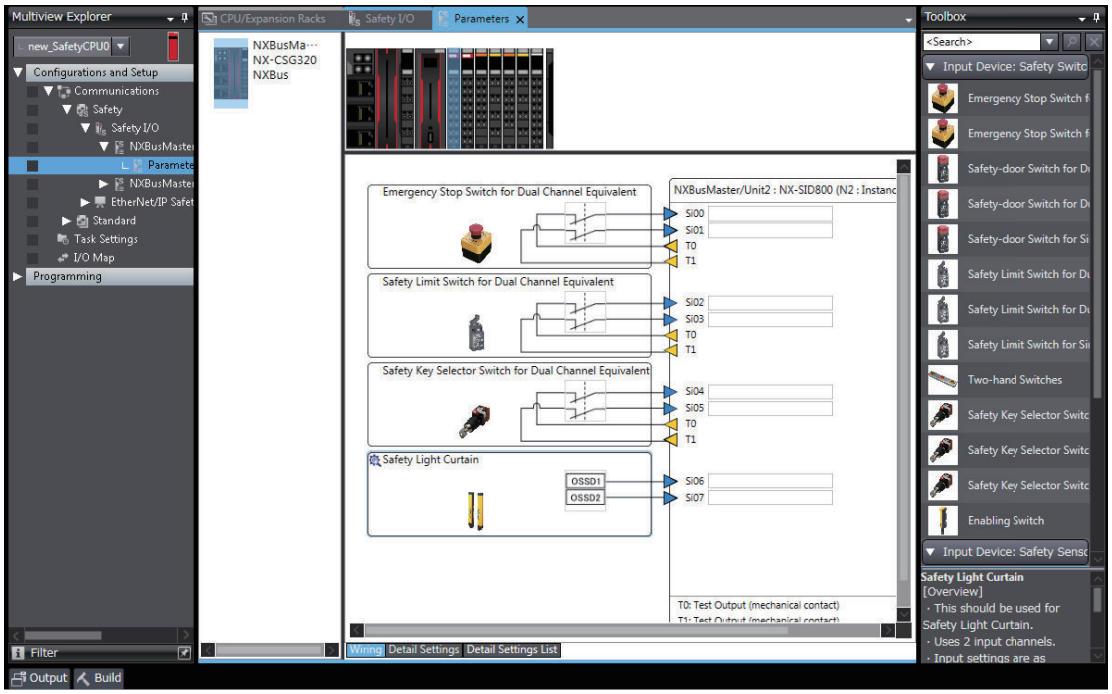
3 Select a device from the Toolbox to connect to the safety input terminal or safety output terminal of the Safety I/O Units, and drag it to the desired I/O terminal.



When you drag the device to connect to a terminal where it can be dropped, a + mark appears below the mouse cursor as shown below.



4 When you complete the settings, the following is displayed. Change the settings and enter comments.



Refer to *6-3-1 Safety Input Function* on page 6-16 and *6-3-2 Safety Output Function* on page 6-38 for the I/O devices that you can connect and the settings for each I/O device.

Precautions for Correct Use

If you select an input device that cannot be set for a Safety Input Unit, an error will occur and the frame around the input device will be displayed in red.



Additional Information

The I/O terminal comments on the Parameters Tab Page are linked to the device variable comments and the global variable comments.

7-6-2 Setting the Standard Input and Output Functions

Refer to the manuals for respective NX Units.

7-7 Assigning Variables to I/O Ports

7-7-1 Registering Device Variables

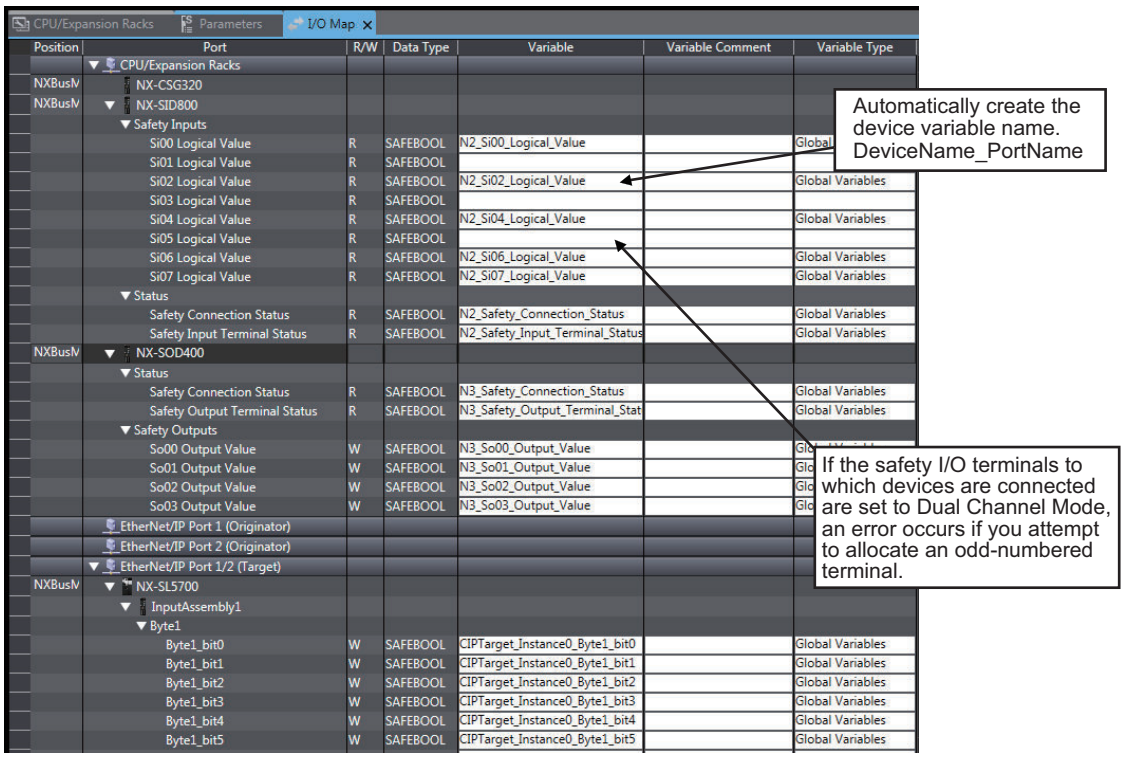
Device variables are used to access data in devices (slaves and Units).
This data is accessed through a port that acts as an interface to an external device. This logical port is called an "I/O Port".

To make the values of the I/O on the Safety I/O Units, Safety I/O Terminal and the other Safety CPU Unit available in the safety program in the Safety CPU Unit, you must register device variables for the I/O ports on the Safety I/O Units, Safety I/O Terminal and the other Safety CPU Unit.
This section describes how to assign device variables to I/O ports through the I/O Map of the Safety CPU Unit.

● Registering New Variables or Creating Them Automatically

If the Controller configuration and the external devices to connect are finalized before you register the variables that are used in the program, you can create the device variable for the I/O ports by manually entering the device variable name, or by creating them automatically.

1 On the Safety CPU Unit Setup and Programming View, select **Configurations and Setup** and double-click **I/O Map**.
The I/O Map will be displayed.



2 Select an I/O port in the I/O Map for the Safety CPU Unit, and enter a variable name directly in the **Variable** Column. Or, select a Unit or I/O port, and then right-click and select **Create Device Variable** from the menu.

If you choose the **Create Device Variable** command, the device variables are automatically named with the device name and port name. The device variables that you enter or automatically create are registered in the global variable table.

● Selecting from the Registered Variables

If the variables that are used in the program are registered before you finalize on the Controller configuration and the external devices to connect, you can select and assign variables to the I/O ports for the safety I/O terminals as long as the variables are registered in the variable table.

1 On the Safety CPU Unit Setup and Programming View, select **Configurations and Setup** and double-click **I/O Map**.
The I/O Map will be displayed.

2 Select an I/O port and select a user-defined variable from the list of variables that are registered in the variable table to assign the variable to that I/O port.

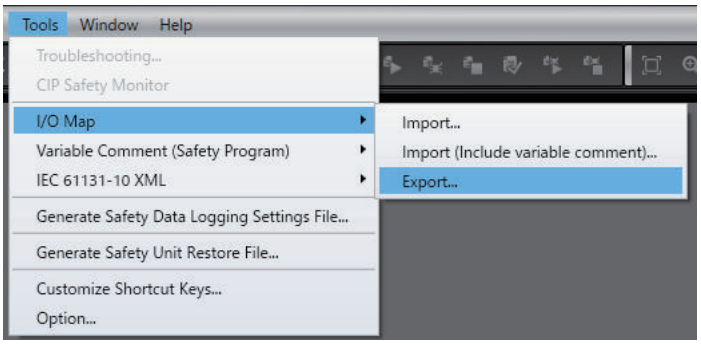
Additional Information

If the I/O terminals on the Safety I/O Units are set to Dual Channel Mode, the device variable can only be assigned to an even-numbered terminal.

● Importing from a CSV File

You can register device variables all at once by exporting the current I/O Map display content as a CSV format file and importing the content after editing with a spreadsheet application.

1 On the **Tools** menu, select **I/O Map** - **Export**.



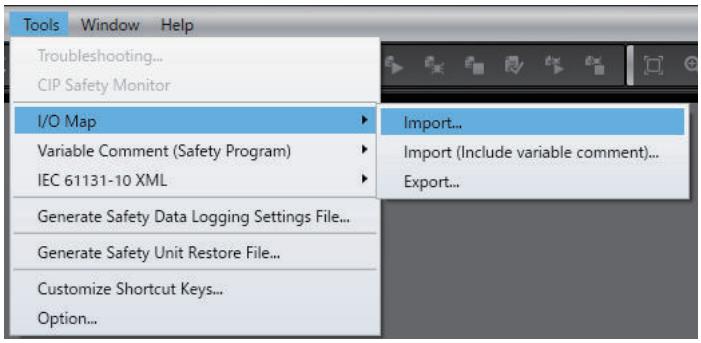
2 Save the CSV file to any location.

3 Open the CSV file in a spreadsheet application.

Sysmac St	Ver.1.0					
Level	Position	Port	R/W	Data Type	Variable	Variable Comment
0	[Network]	CPU/Expansion Racks				
1	NXBusMaster	NX102-1200				
1	NXBusMaster/Unit2	NX-SID800				
2		Safety Inputs				
3		Si00 Logical Value	R	SAFEBOOL	ESTOP_Si01	Emergency Stop S-IN01
3		Si01 Logical Value	R	SAFEBOOL		
3		Si02 Logical Value	R	SAFEBOOL	Door_Si02_R	Door S-IN02
3		Si03 Logical Value	R	SAFEBOOL		
3		Si04 Logical Value	R	SAFEBOOL	Door_Si03_L	Door S-IN03
3		Si05 Logical Value	R	SAFEBOOL		
3		Si06 Logical Value	R	SAFEBOOL	ResetSwitch_R01	Reset Switch R01
3		Si07 Logical Value	R	SAFEBOOL		
2		Status				
3		Safety Connection Status	R	SAFEBOOL	N2_Safety_Connection_Status	
3		Safety Input Terminal Status	R	SAFEBOOL	N2_Safety_Input_Terminal_Status	
1	NXBusMaster/Unit3	NX-SIH400				
2		Safety Inputs and Status				
3		Si00 Logical Value	R	SAFEBOOL	SR1_EDM_Si05	EDM_S-IN05
3		Si01 Logical Value	R	SAFEBOOL	SR1_EDM_Si06	EDM_S-IN06
3		Si02 Logical Value	R	SAFEBOOL	SR2_EDM_Si07	EDM_S-IN07
3		Si03 Logical Value	R	SAFEBOOL	SR2_EDM_Si08	EDM_S-IN08
3		Safety Connection Status	R	SAFEBOOL	N3_Safety_Connection_Status	
3		Safety Input Terminal Status	R	SAFEBOOL	N3_Safety_Input_Terminal_Status	

4 In the **Variable** and **Variable Comment** columns, set any variable name and variable comment.
After you edit data with a spreadsheet application, save the data in the CSV format (UTF-8).

5 From the main menu, select **Tools** - **I/O Map** - **Import** or **Import (Include variable comment)**.



Import imports only the **Variable** column of the CSV file. Even if you edited the **Variable Comment** column in the CSV file, the changes are not applied to the I/O Map.
Import (Include variable comment) imports the content of the **Variable** column and the **Variable Comment** column of the CSV file. If the registered variable is assigned by the **Import (Include variable comment)** function, the content of the **Variable Comment** column is applied.

Precautions for Correct Use

- When you register device variables by importing a CSV file, the data integrity is not checked by CRC. Always validate the correct variable assignments under your responsibility after the import and assure proper execution before you use it for actual operation.
- When the display comment is set to other than **Comment 1**, the I/O Map **Import (Include variable comment)** and **Export** cannot be executed.
- When you import a CSV file with its **Variable** column left blank, the variable assignments are canceled.

I/O Ports for Safety I/O Units That Are Displayed in the I/O Map of the Safety CPU Unit

The I/O ports for Safety I/O Units that are displayed in the I/O Map of the Safety CPU Unit are described in this section.

● NX-SIH400 Safety Input Unit

Port	Data type	R/W	Name	Description	Default
Si00 Logical Value	SAFEBOOL	R	Si00 Logical Value	Gives the status of safety input terminal Si00. 0: OFF, 1: ON	0
Si01 Logical Value	SAFEBOOL	R	Si01 Logical Value	Gives the status of safety input terminal Si01. 0: OFF, 1: ON	0
Si02 Logical Value	SAFEBOOL	R	Si02 Logical Value	Gives the status of safety input terminal Si02. 0: OFF, 1: ON	0
Si03 Logical Value	SAFEBOOL	R	Si03 Logical Value	Gives the status of safety input terminal Si03. 0: OFF, 1: ON	0
Safety Connection Status	SAFEBOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0
Safety Input Terminal Status	SAFEBOOL	R	Safety Input Terminal Status	This flag indicates the status of the safety input terminals. 0: An error has occurred on one of the safety input terminals. 1: All of the safety input terminals are normal (no errors).	0

● NX-SID800 Safety Input Unit

Port	Data type	R/W	Name	Description	Default
Si00 Logical Value	SAFEBOOL	R	Si00 Logical Value	Gives the status of safety input terminal Si00. 0: OFF, 1: ON	0
Si01 Logical Value	SAFEBOOL	R	Si01 Logical Value	Gives the status of safety input terminal Si01. 0: OFF, 1: ON	0
Si02 Logical Value	SAFEBOOL	R	Si02 Logical Value	Gives the status of safety input terminal Si02. 0: OFF, 1: ON	0
Si03 Logical Value	SAFEBOOL	R	Si03 Logical Value	Gives the status of safety input terminal Si03. 0: OFF, 1: ON	0
Si04 Logical Value	SAFEBOOL	R	Si04 Logical Value	Gives the status of safety input terminal Si04. 0: OFF, 1: ON	0
Si05 Logical Value	SAFEBOOL	R	Si05 Logical Value	Gives the status of safety input terminal Si05. 0: OFF, 1: ON	0
Si06 Logical Value	SAFEBOOL	R	Si06 Logical Value	Gives the status of safety input terminal Si06. 0: OFF, 1: ON	0
Si07 Logical Value	SAFEBOOL	R	Si07 Logical Value	Gives the status of safety input terminal Si07. 0: OFF, 1: ON	0

Port	Data type	R/W	Name	Description	Default
Safety Connection Status	SAFEBOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0
Safety Input Terminal Status	SAFEBOOL	R	Safety Input Terminal Status	This flag indicates the status of the safety input terminals. 0: An error has occurred on one of the safety input terminals. 1: All of the safety input terminals are normal (no errors).	0

● NX-SOH200 Safety Output Unit

Port	Data type	R/W	Name	Description	Default
Safety Connection Status	SAFEBOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0
Safety Output Terminal Status	SAFEBOOL	R	Safety Output Terminal Status	This flag indicates the status of the safety output terminals. 0: An error has occurred on one of the safety output terminals. 1: All of the safety output terminals are normal (no errors).	0
So00 Output Value	SAFEBOOL	W	So00 Output Value	Gives the status of safety output terminal So00. 0: OFF, 1: ON	0
So01 Output Value	SAFEBOOL	W	So01 Output Value	Gives the status of safety output terminal So01. 0: OFF, 1: ON	0

● NX-SOD400 Safety Output Unit

Port	Data type	R/W	Name	Description	Default
Safety Connection Status	SAFEBOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0
Safety Output Terminal Status	SAFEBOOL	R	Safety Output Terminal Status	This flag indicates the status of the safety output terminals. 0: An error has occurred on one of the safety output terminals. 1: All of the safety output terminals are normal (no errors).	0
So00 Output Value	SAFEBOOL	W	So00 Output Value	Gives the status of safety output terminal So00. 0: OFF, 1: ON	0
So01 Output Value	SAFEBOOL	W	So01 Output Value	Gives the status of safety output terminal So01. 0: OFF, 1: ON	0
So02 Output Value	SAFEBOOL	W	So02 Output Value	Gives the status of safety output terminal So02. 0: OFF, 1: ON	0

Port	Data type	R/W	Name	Description	Default
So03 Output Value	SAFE-BOOL	W	So03 Output Value	Gives the status of safety output terminal So03. 0: OFF, 1: ON	0

7-7-2 Settings of Communications between NX Units

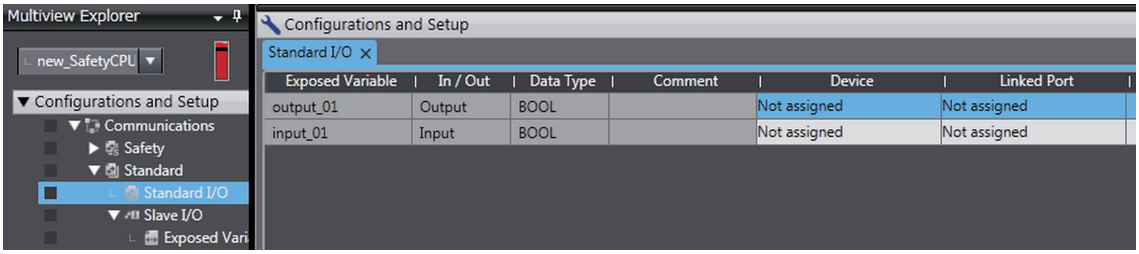
Communications between NX Units are used for standard process data communications between a Safety CPU Unit and standard I/O Units. Communications between NX Units are performed by allocating the data of the standard I/O Units for the exposed variables of the Safety CPU Unit.
Refer to *A-13 Units That Support Communications between NX Units* on page A-103 for the models of the NX Units that you can connect.

Use the following procedure to set up NX Unit communications between a Safety CPU Unit and standard I/O Units.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Register the exposed variables in the Safety CPU Unit.
Refer to *7-8-2 Setting Exposed Variables* on page 7-54 for information on registering exposed variables.
Set the data types of the exposed variables to the same data types as the allocated standard I/O Unit data.

3 Double-click **Standard I/O** under **Configurations and Setup** − **Communications** − **Standard**.
The Standard I/O Unit Setting Tab Page is displayed.

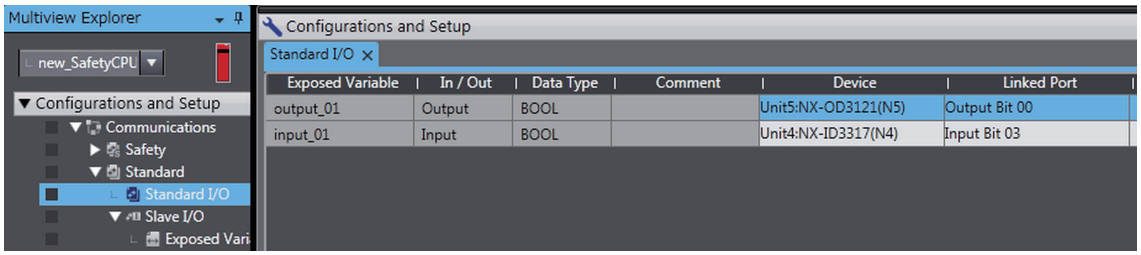


The meanings of the items in the Standard I/O Unit Setting Tab Page are given below.

Item	Editing	Description
Exposed Variable	Not possible	The registered exposed variables are displayed.
In/Out	Not possible	Whether the exposed variable is an input or output variable is displayed.
Data Type	Not possible	The data type of the variable is displayed.
Comment	Not possible	The comment set for the exposed variable is set.
Device	Possible	Set the NX Unit to which the exposed variable is allocated.
Linked Port	Possible	Set the NX Unit I/O port to which the exposed variable is allocated.

4 Set the devices and ports of the standard I/O Units that correspond to the exposed variables of the Safety CPU Unit.

The I/O data of the standard I/O Units will be allocated to the exposed variables of Safety CPU Unit.



Precautions for Correct Use

The I/O ports of the NX Unit that is set for communications between NX Units are not available to be registered as device variables of the Communication Control Unit. If you want to use them as device variables of the Communication Control Unit, you need to copy them to the exposed variables in a safety program for the Safety CPU Unit.

7-8 Exposing Variables to Standard Controllers

This section describes how to control and monitor the Safety CPU Unit from a standard controller through tag data links.

7-8-1 Exposing Global Variables

To ensure that global variables in the Safety CPU Unit are not accidentally used by a program of the standard controller, they are not assigned to the standard controller at the time of their setting.
When you set global variables in the Safety CPU Unit as exposed variables, the variables are exposed as I/O ports in the I/O Map of the Communication Control Unit.

When the exposed variables are assigned to the I/O ports and registered to tag sets, the standard controller can access the global variables in the Safety CPU Unit through tag data links.
The I/O Map of the Communication Control Unit displays the data types that correspond to the data types of the exposed Safety CPU Unit variables.
The following table gives the variable data types that can be exposed for the Safety CPU Unit and the corresponding data types that are displayed for the Communication Control Unit.

Variable data type that can be exposed for Safety CPU Unit	Data type that is displayed for Communication Control Unit	Data size in bytes
BOOL	BOOL	1
BYTE	USINT	1
WORD	UINT	2
INT	INT	2
DINT	DINT	4

The variables that can be exposed for the Safety CPU Unit are restricted as given in the following table.

Item		Restriction
Number of Exposed Variables	Input	254 variables max.
	Output	253 variables max.

Precautions for Correct Use

- There is a restriction on the data size that can be communicated between the Safety CPU Unit and the Communication Control Unit, as well as the restrictions on the number of exposed variables. This data size limit includes FSoE communications, CIP Safety communications, and communications between NX units. You can check the usage on the Memory Usage Tab Page of the Safety CPU Unit.
- If the settings cause a limit to be exceeded, a red " ! " icon is displayed by **Exposed Variables** in the Multiview Explorer.

7-8-2 Setting Exposed Variables

This section describes how to expose Safety CPU Unit variables to the Communication Control Unit. Exposed Safety CPU Unit variables (exposed variables) appear in the I/O Map of the Communication Control Unit.

Use one of the following methods to set exposed variables.

- Register new variables on the Exposed Variables Tab Page.
- Select global variables on the Exposed Variables Tab Page.
- Set the Expose Column for global variables.
- Copy global variables and paste them on the Exposed Variables Tab Page.

The procedures for these methods are given below.

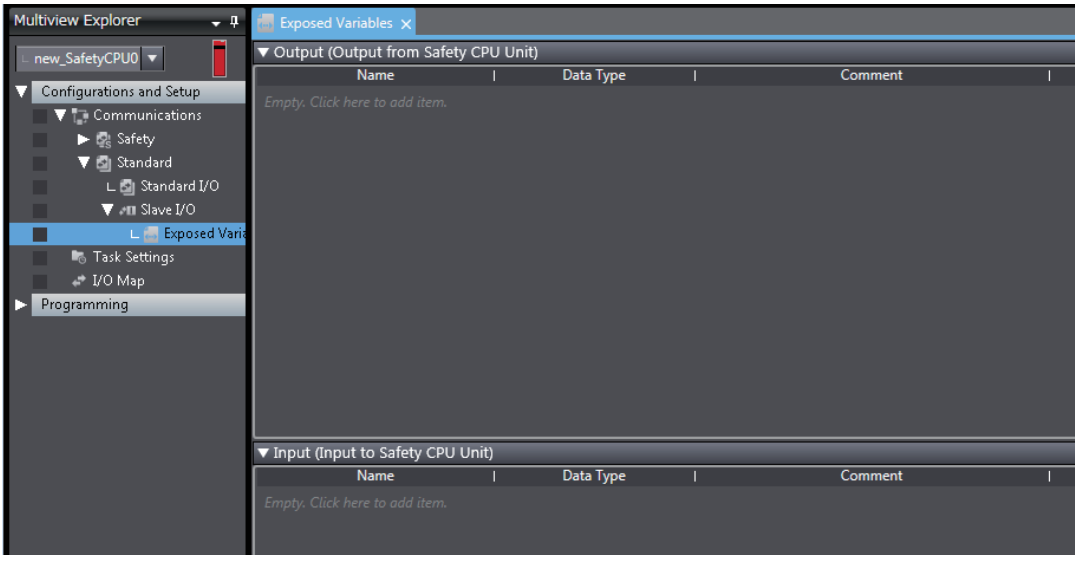
Precautions for Correct Use

- If you change the I/O of exposed variables, the device variable assignments to the Communication Control Unit will be canceled. In this case, you need to assign the device variables again, and then transfer the settings to the Communication Control Unit.
- If you change exposed variables, you need to transfer the settings to the Communication Control Unit. After you transfer the settings, check that the operation of the Communication Control Unit is correct.

Registering New Variables on the Exposed Variables Tab Page

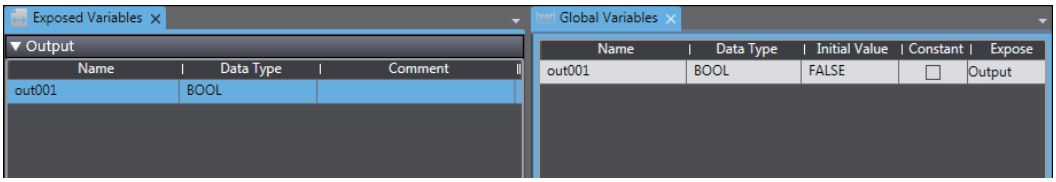
Use the following procedure to register variables on the Exposed Variables Tab Page when those variables are not registered as global variables. The registered exposed variables are automatically registered as global variables.

1 Double-click **Exposed Variables** under **Configurations and Setup** – **Communications** – **Standard** – **Slave I/O**.
The Exposed Variables Tab Page is displayed.



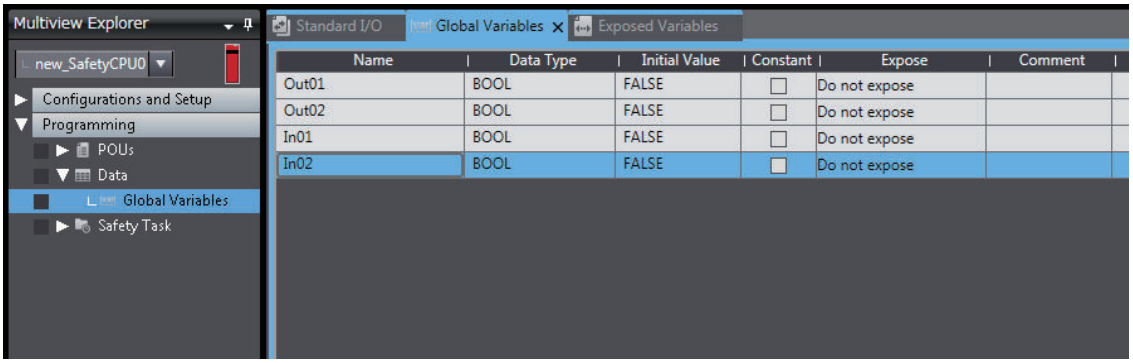
2 Enter the variable name in the Name Column of the output table or input table.

The variable that you entered is registered in the exposed variable table and in the global variable table.

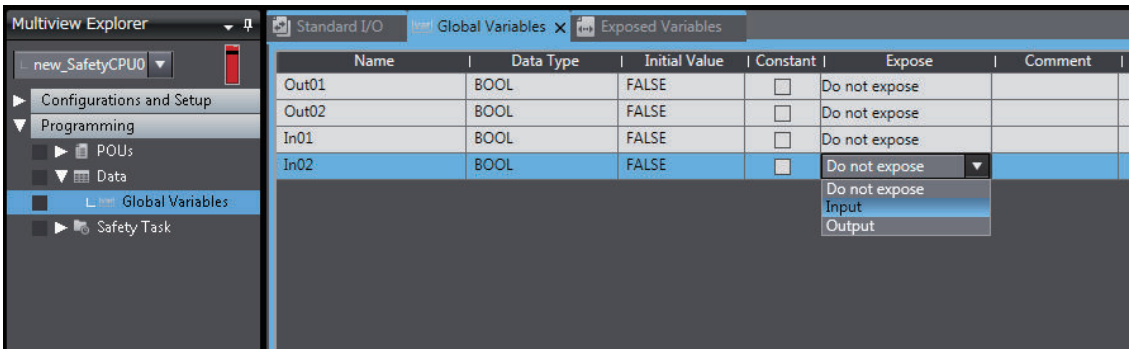


Setting the Expose Column for Global Variables

1 Register global variables with standard data types.
Refer to *8-5-3 Registering Variables* on page 8-38 for details on registering variables.



2 Select the Expose Column for global variables, and then select Input or Output.
The selected variable is registered in the exposed variable input table or output table.

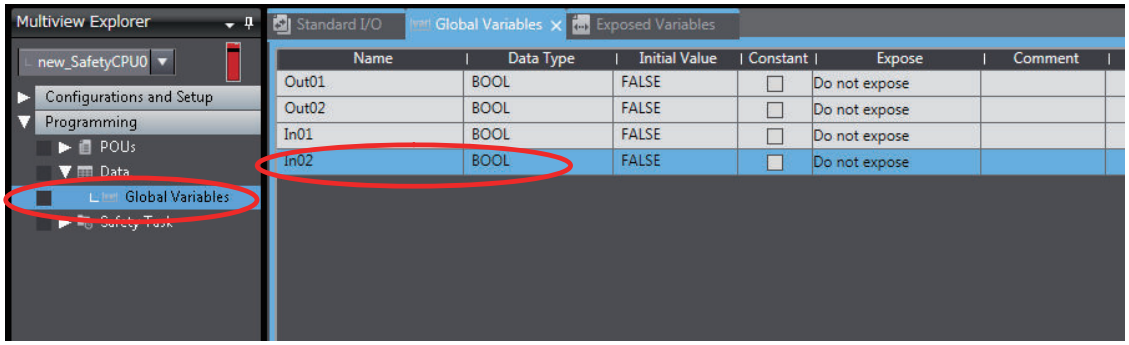


Copying Global Variables and Pasting Them on the Exposed Variables Tab Page

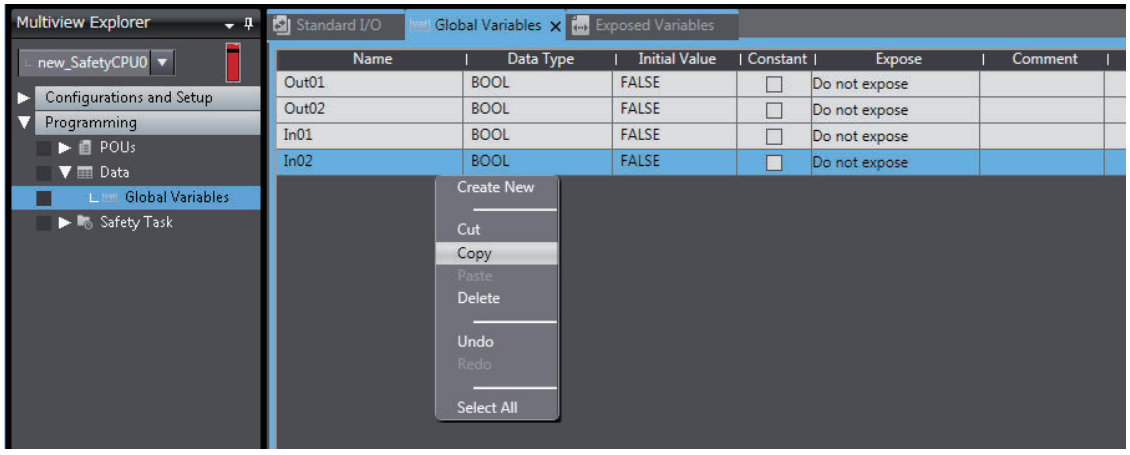
Use the following procedure to select variables on the global variable table and set them as exposed variables.
You can select more than one global variable.

1 Register global variables with standard data types.

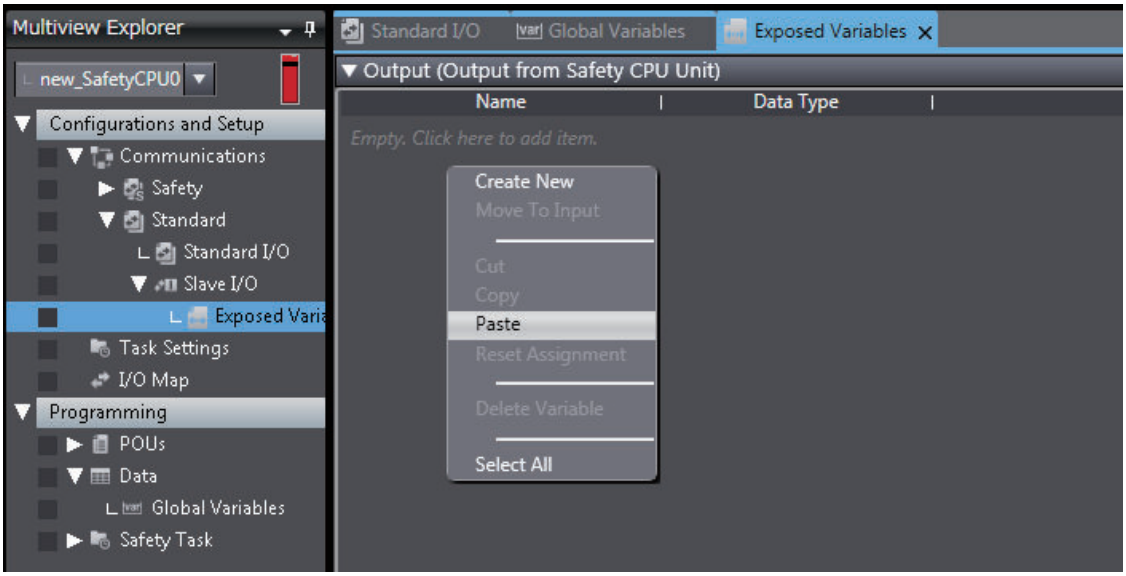
Refer to *8-5-3 Registering Variables* on page 8-38 for details on registering variables.



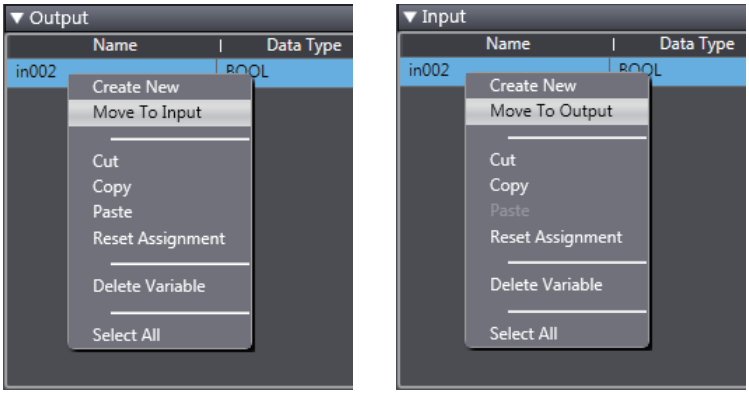
2 Right-click one or more global variables and select **Copy** from the menu.
The selected global variables are copied.
Press the **Shift** Key or **Ctrl** Key to select more than one global variable.



3 Right-click in the Exposed Variables Tab Page and select **Paste** from the menu.
The global variables are set as exposed variables.



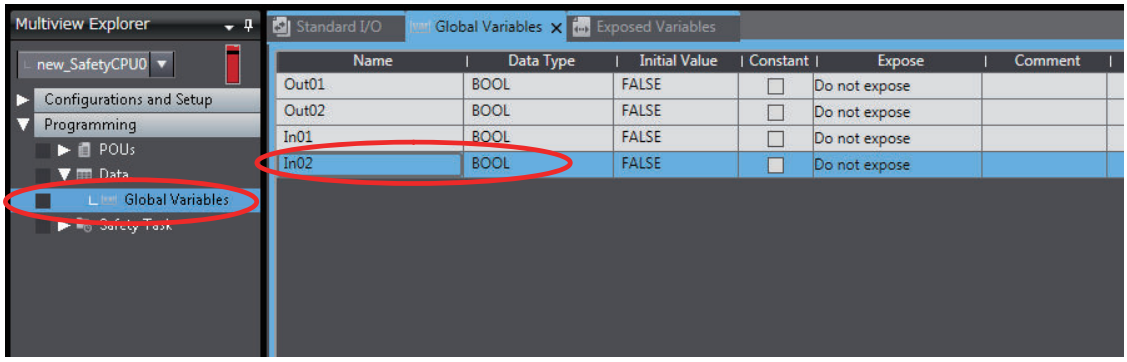
4 To change the **I/O** setting for an exposed variable, right-click the exposed variable and select **Move To Output** or **Move To Input** from the menu.
Press the **Shift** Key or **Ctrl** Key to select more than one exposed variable.



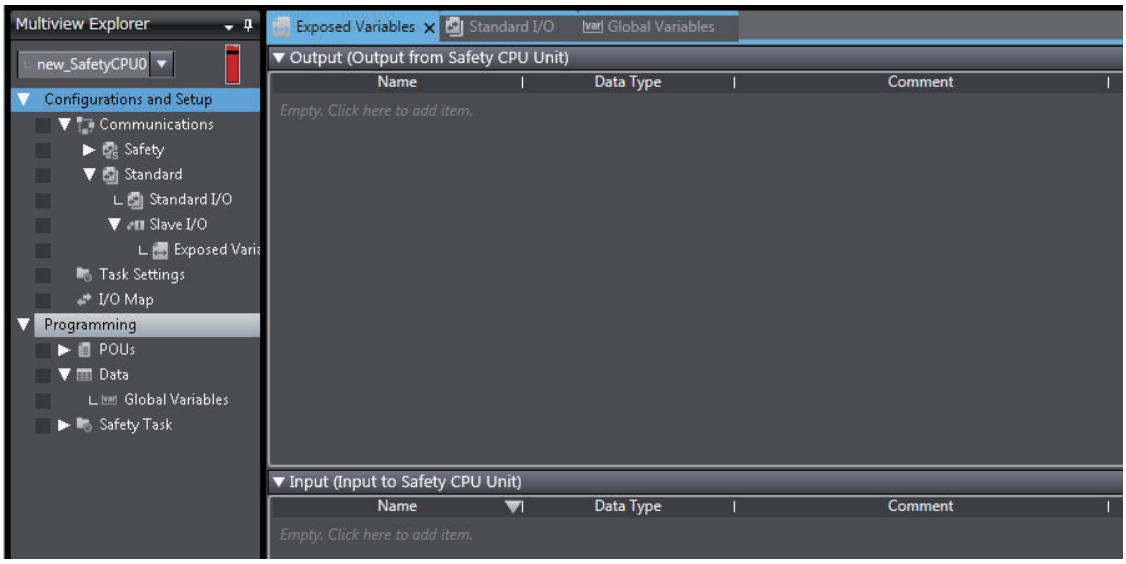
Selecting Global Variables on the Exposed Variables Tab Page

Use the following procedure to select registered global variables on the Exposed Variables Tab Page and set them as exposed variables.

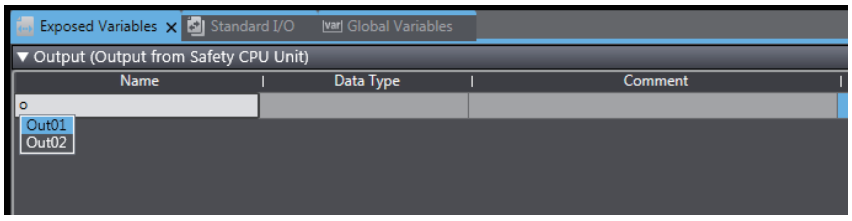
1 Register global variables with standard data types.
Refer to *8-5-3 Registering Variables* on page 8-38 for details on registering variables.



2 Double-click **Exposed Variables** under **Configurations and Setup** – **Communications** – **Standard** – **Slave I/O**.
The Exposed Variables Tab Page is displayed.



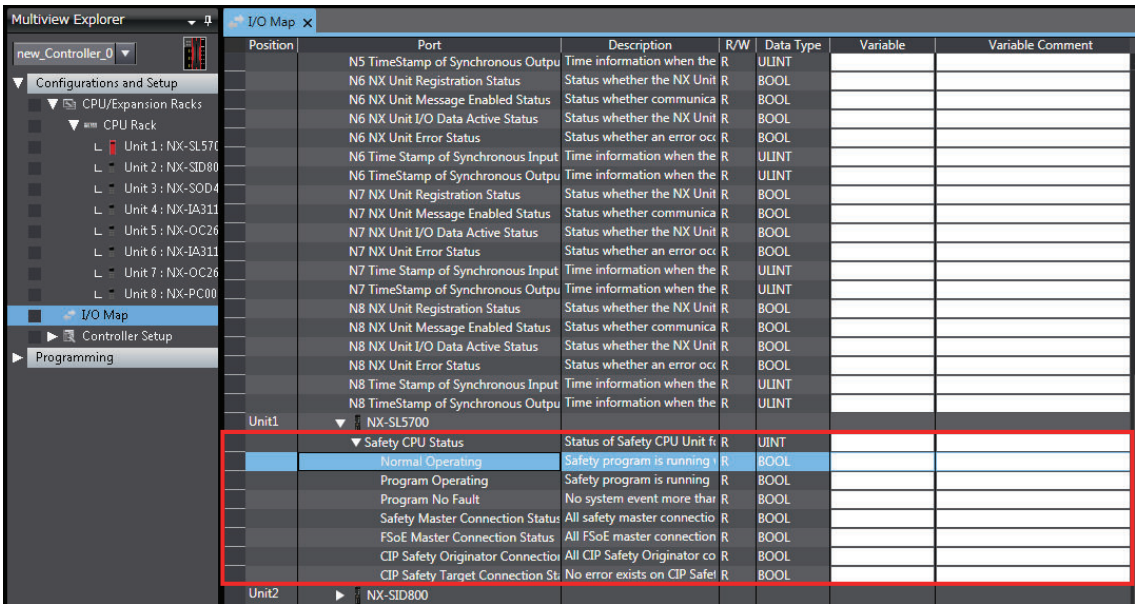
3 Enter the name of the variable to expose (the global variable that was registered in step 1) to the Communication Control Unit.
You can also enter the first letter of the global variable in the Name Box to display a list of candidates, and then double-click the desired variable.



7-8-3 Safety CPU Unit Status

If you place a Safety CPU Unit on the NX bus of a Communication Control Unit, standard process data communications are performed automatically.

The status of a Safety CPU Unit is displayed as I/O ports in the I/O Map of the Communication Control Unit.
Through the I/O ports, the standard controller can monitor the status of Safety CPU Unit using the tag data link connection.



Refer to *A-6 Safety CPU Unit Status* on page A-69 for details on the items in the Safety CPU Unit status.

7-8-4 I/O Ports of Safety I/O Units

The tag data links allow you to view the port values of Safety I/O Units from the standard controller.

The port values can be referenced by assigning variables to the I/O ports that are displayed on the I/O Map of the Communication Control Unit.
Refer to *A-7 I/O Ports of Safety I/O Units* on page A-71 for descriptions of the I/O ports for Safety I/O Units that are displayed on the I/O Map of the Communication Control Unit.

Additional Information

You can only read the port values of Safety I/O Units from the standard controller. You cannot write the values.

7-8-5 I/O Ports for Standard I/O Units

Values of I/O ports for standard I/O Units can be read from or written to the standard controllers.
You can assign variables to I/O ports in the I/O Map of the Communication Control Unit.
Refer to the user's manuals for individual Units for descriptions of the I/O ports displayed in the I/O Map.

Additional Information

The I/O ports of the NX Unit which was specified for the communications between NX Units cannot be registered as the device variables of the Communication Control Unit. To use them as device variables of the Communication Control Unit, you need to copy them to the exposed variables in a safety program for Safety CPU Unit.

7-9 Exporting/Importing Settings Data

This section describes how to reuse the settings data for the entire CPU Rack in the Sysmac Studio or the safety application data in the Safety CPU Unit.

You can export and import the data for the entire CPU Rack or the safety application data in the Safety CPU Unit as a single file.
This function is designed for reusing safety application data from the other projects.

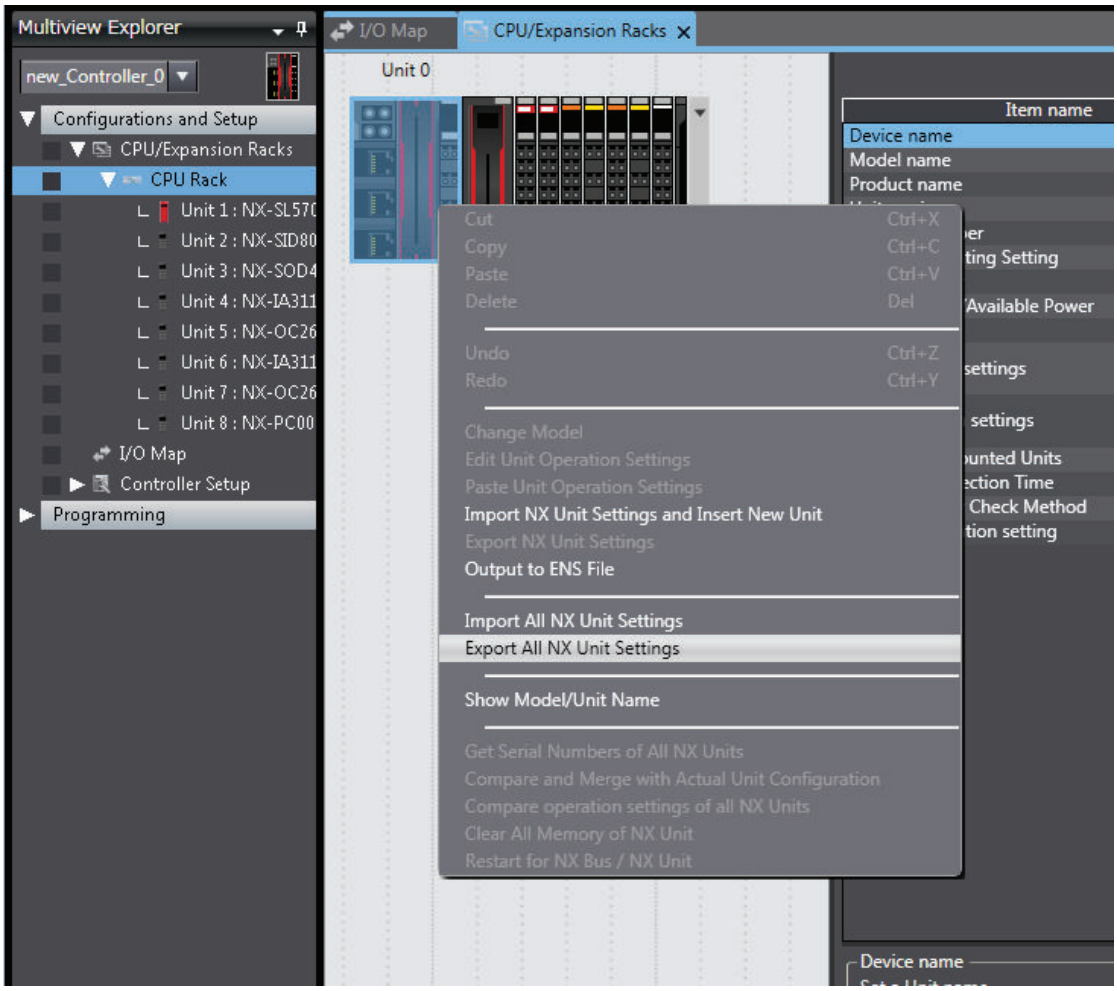
You can export or import the three groups of data that are given below.

- All NX Units
  The settings data for all the NX Units includes the operating settings and the application data (including safety application data) for all the NX Units. The settings data for the Communication Control Unit is not included.
- Safety application data for Individual Safety CPU Unit
- Safety application data in the Safety Unit Restore File
  The safety application data consists of the safety program and the safety tasks and settings.

7-9-1 Exporting/Importing the All NX Unit Settings

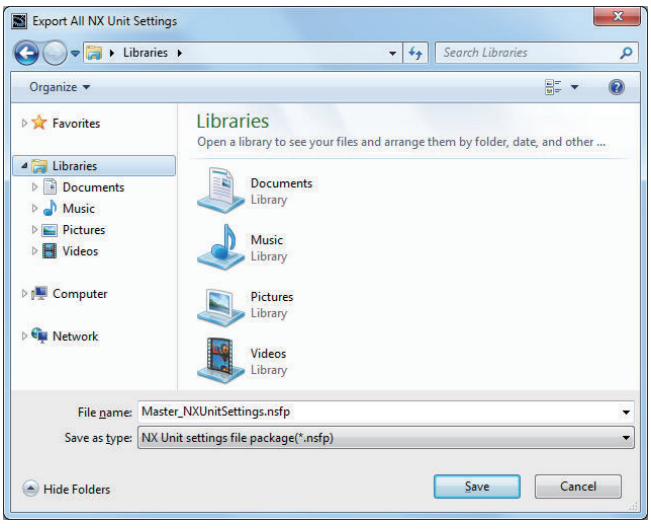
You can export the operating settings and the application data (including safety application data) for all of the NX Units into a single file (extension of .nsfp).

1 Display the CPU and Expansion Racks Tab Page where the Safety CPU Unit to export is configured.



2 Right-click the Communication Control Unit and select **Export All NX Unit Settings** from the menu.

The **Export All NX Unit Settings** Dialog Box is displayed.



3 Enter a file name, and then click the **Save** Button.

A configuration file for all the NX Units with an .nsfp extension is saved.

4 To import a file, right-click the Communication Control Unit in the CPU and Expansion Racks Tab Page, and select **Import All NX Unit Settings** from the menu.
All NX Units including Safety CPU Unit to be imported will be added to the CPU and Expansion Racks Tab Page.

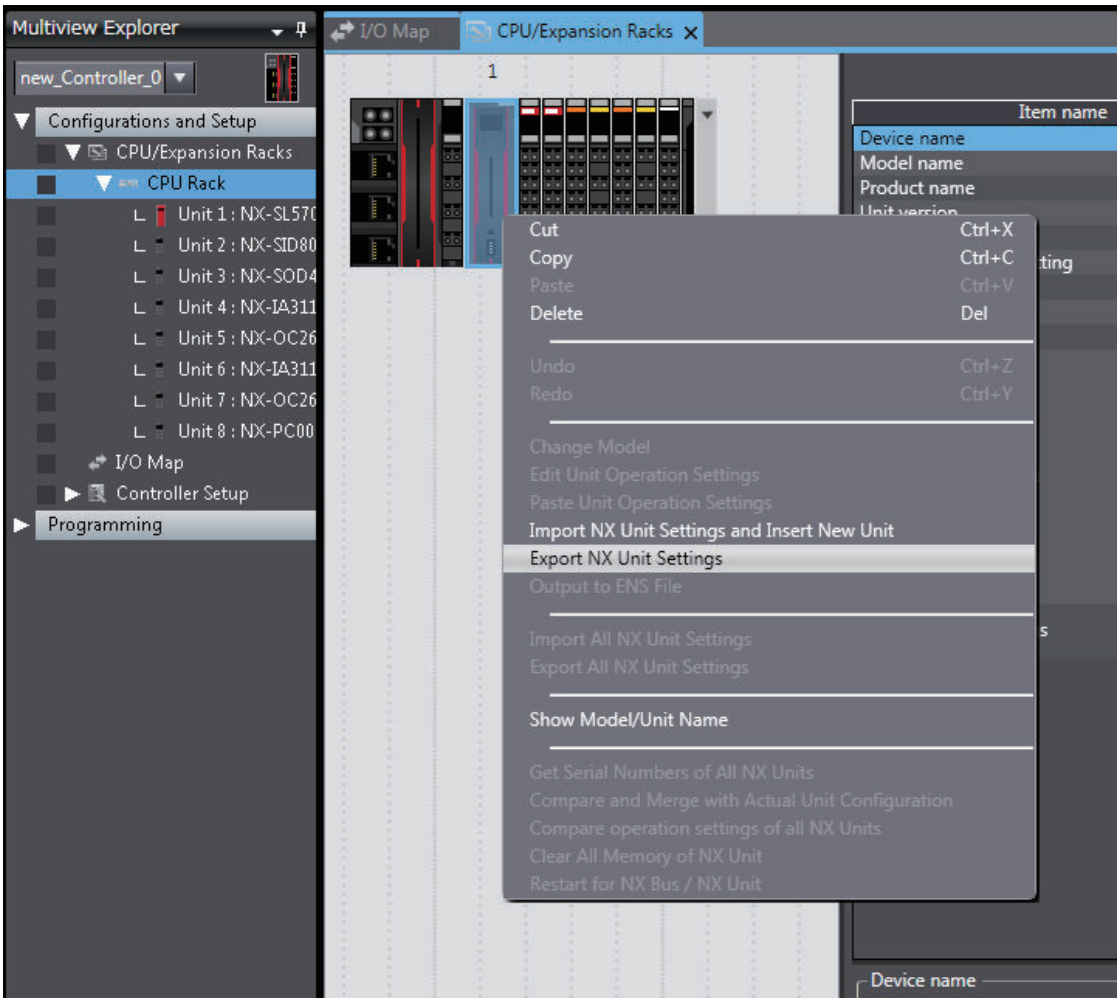
Precautions for Correct Use

- If even one NX Unit has been added to the CPU and Expansion Racks that is being imported, then the CPU and Expansion Racks cannot be imported. Delete all of the NX Units, and then execute the import.
- Settings data of communications between NX Units cannot be restored.

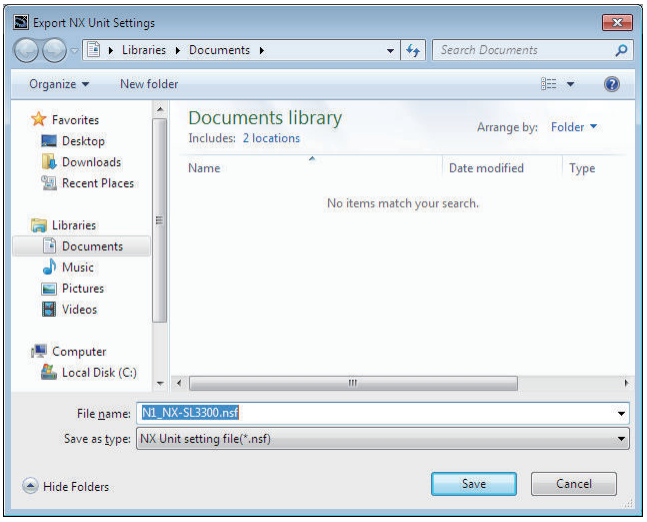
7-9-2 Exporting/Importing Data for Individual Safety CPU Unit

You can export and import the safety application data of each Safety CPU Unit as a single file (extension .nsf).
The exported Safety CPU Unit settings file can be imported to reuse the safety application data for a Safety CPU Unit with the same settings. To do this, go into the CPU and Expansion Racks Tab Page in a different project on the Sysmac Studio, or a project for which a Safety CPU Unit has not been registered.

1 Display the CPU and Expansion Racks Tab Page where the Safety CPU Unit to export is configured.



2 Right-click the Safety CPU Unit to export and select **Export NX Unit Settings** from the menu.
The **Export NX Unit Settings** Dialog Box is displayed.



3 Enter a file name, and then click the **Save** Button.
An NX Unit configuration file with an .nsf extension is saved.

4 To import a file, select the Unit to the left of the point where you wish to add the slave on the CPU and Expansion Racks Tab Page, and then right-click and select **Import Slave Settings and Insert New Slave** from the menu.
The Safety CPU Unit to import is added to the CPU and Expansion Racks Tab Page.

Precautions for Correct Use

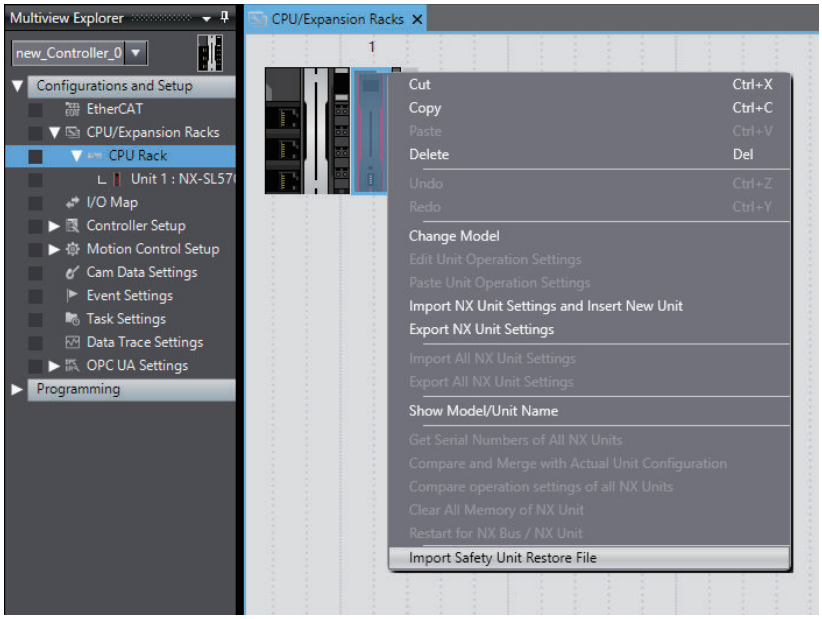
- When you import the data to the Safety CPU Unit, first configure all of the Safety I/O Units.
- If importing data results in two or more Safety CPU Units, an error will occur. Delete the Safety CPU Units that are not used.

7-9-3 Importing the Safety Unit Restore File

You can import safety application data stored in the Safety Unit Restore File into the Safety CPU Unit in the project.
For details on the Safety Unit Restore File, refer to *Section 12 Safety Unit Restore* on page 12-1.

1 Open the CPU and Expansion Racks Tab Page where the Safety CPU Unit is placed.

2 Right-click the Safety CPU Unit and select **Import Safety Unit Restore File** from the menu.



3 Select a Safety Unit Restore File to import and click the **Open** button.
The safety application data of the Safety CPU Unit is replaced with the safety application data stored in the Safety Unit Restore File.

Precautions for Correct Use

- You cannot import the file if the format and the unit version of the Safety CPU Unit in the Safety Unit Restore File are not consistent with those for the project.
- If the safety application data having the identical name as the safety application data in the Safety Unit Restore File exists in another Safety CPU Unit in the project, you cannot import the file.

7-10 Offline Comparison

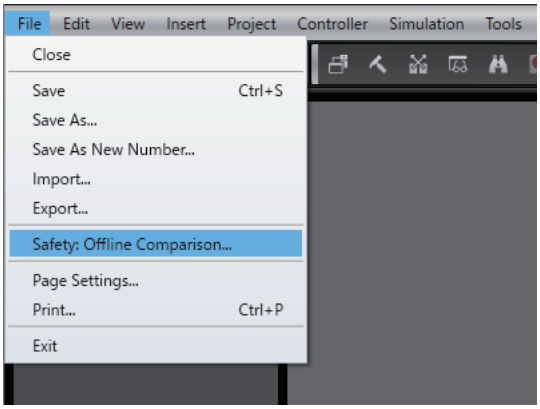
This section describes the function for comparing the safety application data between the currently opened project and another project file.
This function can be used for managing changes in safety application data. In addition, target data can be reflected in the current project if the data supports detailed comparison.

7-10-1 Procedure for Offline Comparison

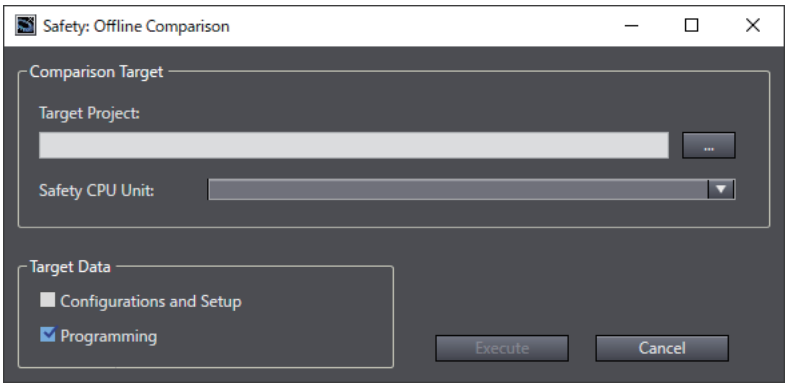
1 Start Sysmac Studio and open the source project file.

2 Select Safety CPU Unit from the Controller Selection Box in the Multiview Explorer and switch to the **Safety CPU Unit Setup and Programming** View.

3 From the Controller Menu, select **File** – **Safety: Offline Comparison**.



The comparison target setting window for offline safety comparison is displayed.

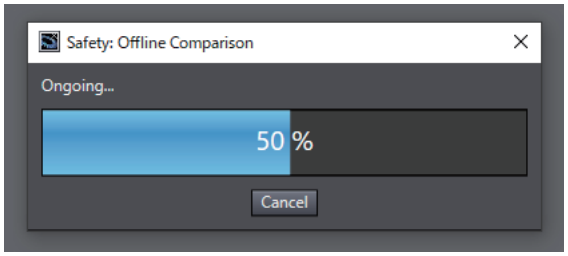


The contents of the setting window are as follows.

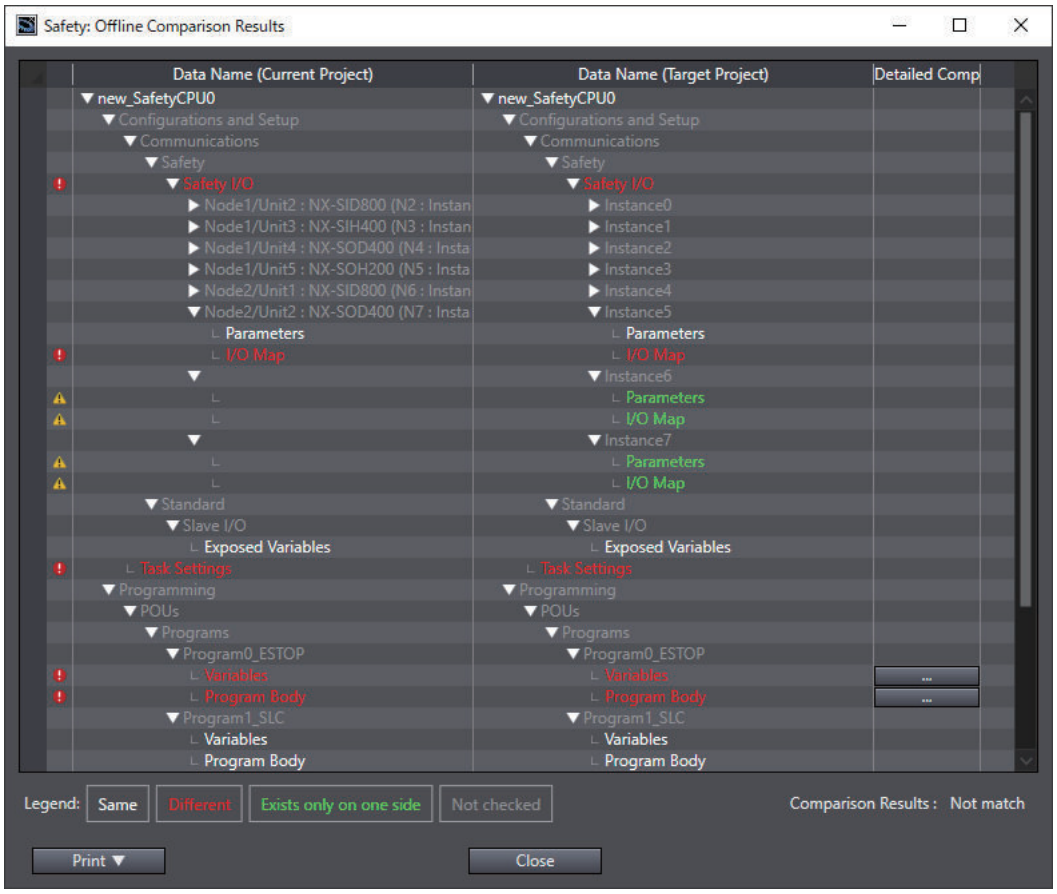
Item	Description
Target Project	A project file to compare with the currently opened project. Select a previously exported project file (smc2, csm2, smc, or csm).
Safety CPU Unit	Select Safety CPU Unit to compare.

Item	Description
Target Data	As data to compare, you can select *Configurations and Setup* or *Programming*. By default, *Programming* is selected. Refer to *7-10-4 Target Data of Offline Comparison* on page 7-69 for details of target data.

4 Select the target project, Safety CPU Unit to be compared, and target data, and then click the **Execute** Button.
The target data is loaded. The following progress dialog appears during offline comparison.
Depending on the project size, it may take time until the comparison results window appears.

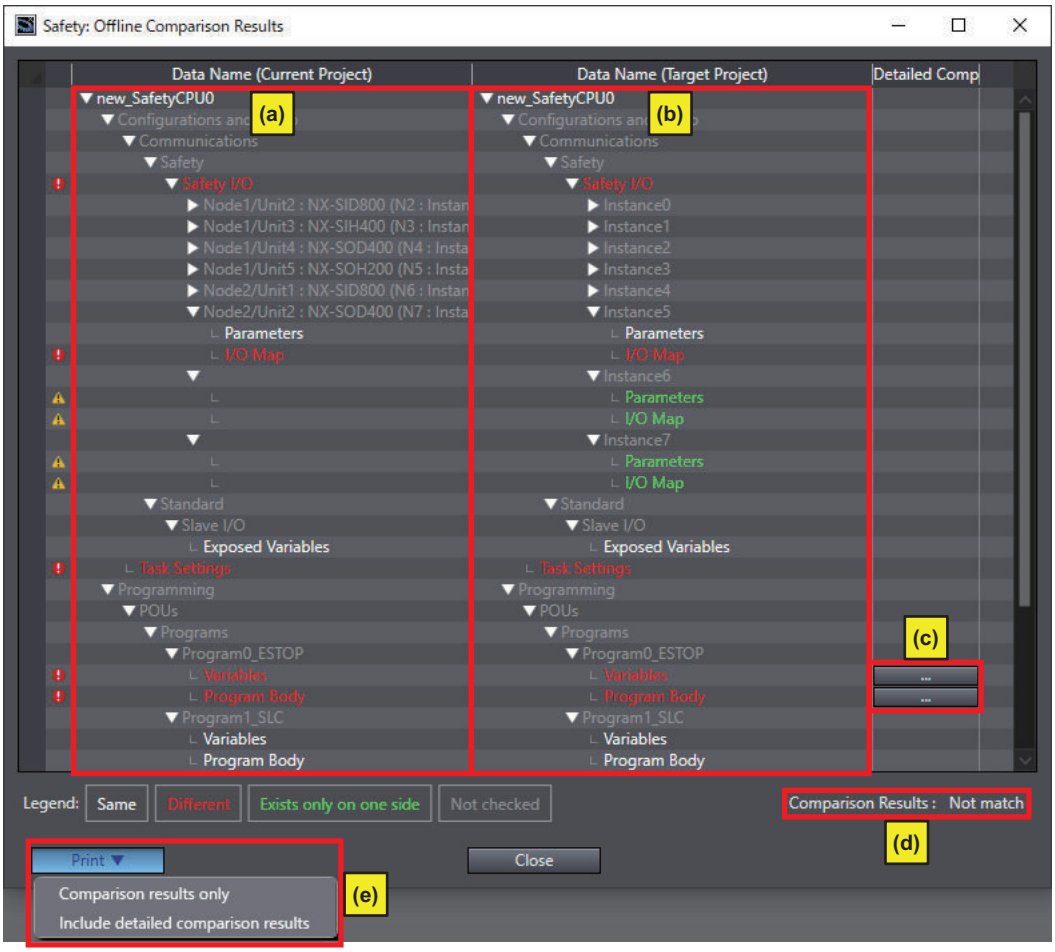


The offline comparison results are displayed.



7-10-2 Checking the Comparison Results

This section describes the displayed contents of the offline comparison results.



The contents of this window are as follows.

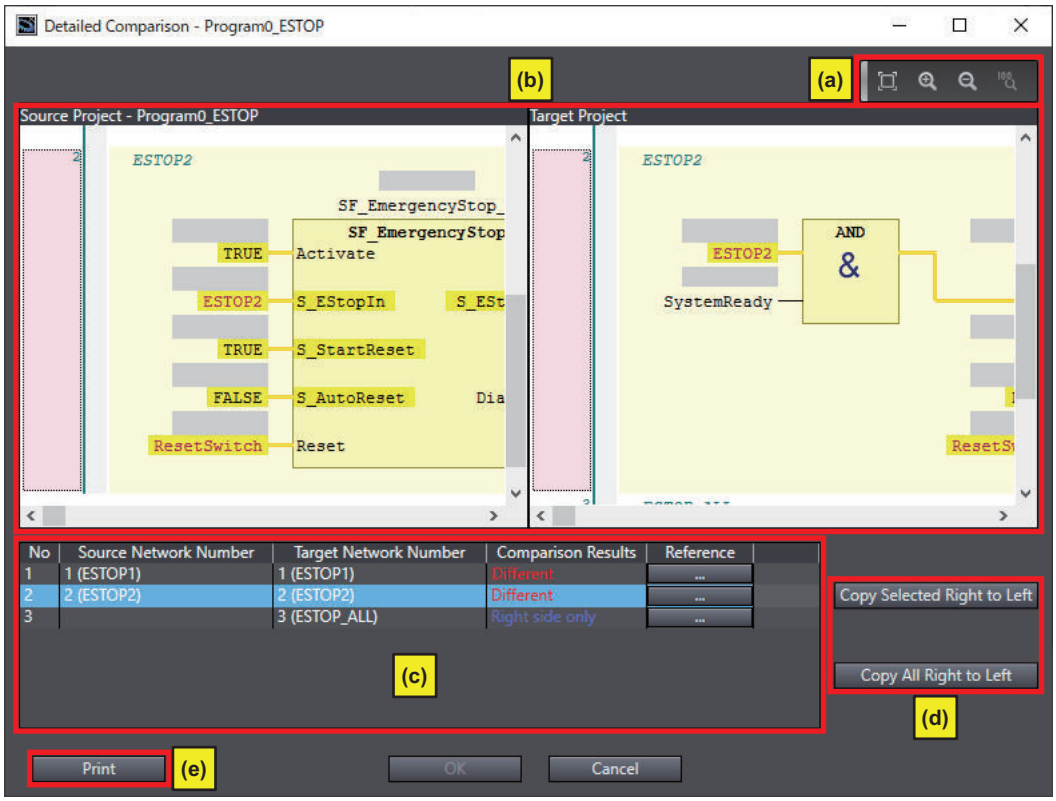
Letter	Name	Description
(a)	Current Project	Displays the source project in a tree format.
(b)	Target Project	Displays the target project in a tree format.
(c)	Detailed Comparison Button	Displays the detailed comparison window for data that has any differences in the comparison results AND that supports detailed comparison. Refer to *7-10-3 Detailed Comparison* on page 7-67 for details.
(d)	Comparison Results	Displays the comparison results for safety application data.
(e)	Print Button	Prints the comparison results. The operations of each button are as follows. Comparison results only: Only prints the results of comparison between source and target project trees. Include detailed comparison results In addition to the comparison results, prints the detailed comparison results for data that includes detailed comparison.

Refer to *7-10-4 Target Data of Offline Comparison* on page 7-69 for details of target data.

7-10-3 Detailed Comparison

Clicking the **Detailed Comparison** button on Offline Comparison Results displays the following detailed comparison window. From the detailed comparison window, you can reflect differences in the source project.

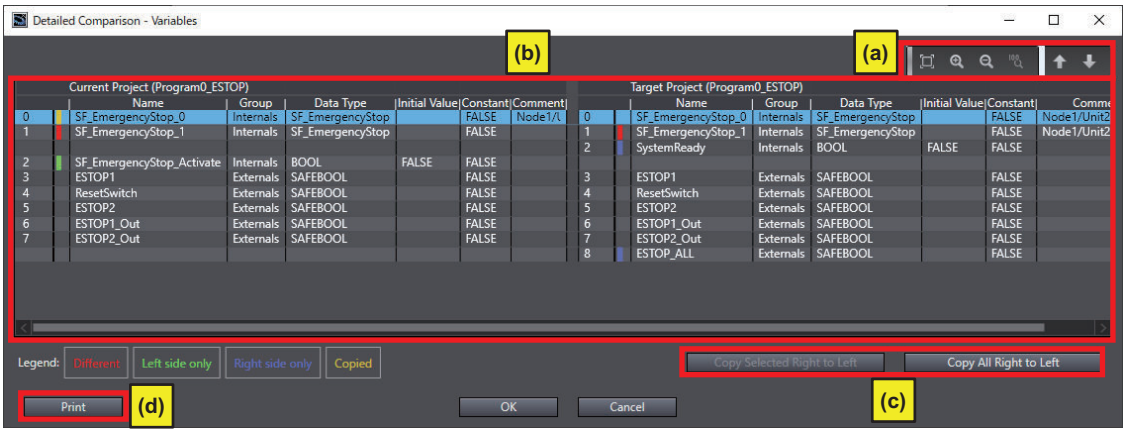
Safety Programs



The contents of this window are as follows.

Letter	Name	Description
(a)	Zoom in/out Button	Zooms in/out on the program comparison window.
(b)	Program Comparison Window	Displays the source and target programs.
(c)	Program Comparison Results List	Displays differences against each program network. Click the **Reference** button to display differences on the program comparison window.
(d)	Difference Copy Button	Copies the differences selected on the program comparison results window to the source project. After **OK** is clicked on the Detailed Comparison window, it will be reflected in the project.
(e)	Print Button	Prints the window of the detailed comparison results.

Variable Table



The contents of this window are as follows.

Letter	Name	Description
(a)	Zoom in/out and Jumping to Differences Button	Used to zoom in/out on the variable table comparison window and to jump to differences.
(b)	Variable Table Comparison Window	Displays the results of variable table comparison between the source and target projects.
(c)	Difference Copy Button	Copies the differences selected on the variable table comparison display to the source project. After **OK** is clicked on the Detailed Comparison window, it will be reflected in the project.
(d)	Print Button	Prints the window of the detailed comparison results.

Precautions for Correct Use

- After a program or variable is reflected in the current project using Offline Comparison's detailed comparison function, the safety program in the project will be in an unvalidated state. Before you perform safety validation of the safety programs, complete debugging of the safety programs.
- If a safety program that exists only in the target project is reflected in the source project, the program assignment setting (execution order) will be registered at the end. Make sure that the program execution order is correct in the task settings.
- Detailed Comparison does not compare safety programs that exist only in the source program.

7-10-4 Target Data of Offline Comparison

The following data is compared by Offline Comparison. Data not included in the safety application is not compared.

Displayed name	Target data	Detailed Comparison
SafetyCPU Device Name	• Safety Signature • Project options, etc.	Not applicable

Displayed name	Target data	Detailed Comparison
Configurations and Setup **Communications** **Safety** Safety I/O	• Whether FSoE communications settings are enabled or disabled • Whether FSoE Watchdog Timer is set to auto setting or not • Slot comment settings for safety slave unit parameters	Not applicable
Configurations and Setup **Communications** **Safety** **Safety I/O** **Node/Unit** Safety Slave Unit Parameters	• Safety slave unit parameter settings • Settings for FSoE Slave Address • Settings for FSoE Watchdog Timers	Not applicable
Configurations and Setup **Communications** **Safety** **Safety I/O** **Node/Unit** SRA Parameters	• SRA parameter settings for the R88D-1SA series • Settings for FSoE Slave Address • Settings for FSoE Watchdog Timers	Not applicable
Configurations and Setup **Communications** **Safety** **Safety I/O** **Node/Unit** I/O Map	• I/O map settings of an FSoE slave	Not applicable
Configurations and Setup **Communications** **Safety** **EtherNet/IP Safety Connection Settings** Safety Network Number	• Safety network number settings for CIP Safety	Not applicable
Configurations and Setup **Communications** **Safety** **EtherNet/IP Safety Connection Settings** **Connection Settings (Originator)** **CIP Safety Device** CIP Safety Parameters	• Connection settings for CIP Safety	Not applicable
Configurations and Setup **Communications** **Safety** **EtherNet/IP Safety Connection Settings** **Connection Settings (Originator)** **CIP Safety Device** I/O Map	• I/O map settings for a CIP Safety device	Not applicable
Configurations and Setup **Communications** **Safety** **EtherNet/IP Safety Connection Settings** **Connection Settings (Originator)** I/O Assembly Settings (Target)	• I/O assembly settings for CIP Safety	Not applicable

Displayed name	Target data	Detailed Comparison
Configurations and Setup **Communications** **Safety** **EtherNet/IP Safety Connection Settings** **Connection Settings (Originator)** **I/O Assembly Settings (Target)** I/O Map	• I/O assembly settings for a CIP Safety I/O assembly	Not applicable
Configurations and Setup **Communications** **standard** Standard I/O	• Assignment settings for standard I/O and exposed variables	Not applicable
Configurations and Setup **Communications** **standard** **Slave I/O** Exposed Variables	• Settings for exposed variables	Applicable
Configurations and Setup **Task Setup**	• Safety task period • Program assignment settings	Not applicable
Programming **POU** **Programs** **Program names** Variable tables	• Program local variables (internal variables, external variables)	Applicable
Programming **POU** **Programs** **Program names** Program Body	• Program body (algorithm)	Applicable
Programming **POU** **Function blocks** **Function block names** Variable tables	• Function block local variables (internal variables, I/O variables)	Applicable
Programming **POU** **Function blocks** **Function block names** Program Body	• Function block program body (algorithm)	Applicable
Programming **Data** Global variable	• Global variables (including exposed variables)	Applicable

8

Programming

This section describes variables, instructions, and other elements that are used to create safety programs. It also describes the programming operations that are used on the Sysmac Studio.

8-1 POUs (Program Organization Units) 8-3
8-1-1 POU 8-3
8-1-2 Overview of the Three Types of POUs 8-3
8-1-3 Differences between Programs, Functions, and Function Blocks 8-4
8-1-4 Details on Programs 8-5
8-1-5 Details on Function Blocks 8-6
8-1-6 Details on Functions 8-10
8-1-7 Instructions 8-11

8-2 Variables 8-12
8-2-1 Variables 8-12
8-2-2 Types of Variables 8-12
8-2-3 Type of User-defined Variable 8-12
8-2-4 Attributes of Variables 8-13
8-2-5 Data Type 8-14
8-2-6 Variable Attributes Other Than Data Type 8-16
8-2-7 Function Block Instances 8-17
8-2-8 Restrictions on Variable Names and Other Safety Program-related Names 8-17

8-3 Constants (Literals) 8-20
8-3-1 Constants 8-20
8-3-2 Types of Constants 8-20

8-4 Programming Languages 8-22
8-4-1 Programming Languages 8-22
8-4-2 FBD Language 8-22

8-5 Programming Operations 8-27
8-5-1 Programming Layer on the Sysmac Studio 8-27
8-5-2 Registering POUs 8-28
8-5-3 Registering Variables 8-38
8-5-4 FBD Programming 8-46
8-5-5 Program Pattern Copy 8-67
8-5-6 Function Block Conversion for Programs 8-70
8-5-7 Building 8-71
8-5-8 Searching and Replacing 8-73
8-5-9 Safety Task Settings 8-76
8-5-10 Variable Comment Switching Function 8-78

8-6 Automatic Programming 8-87

8-6-1 Generation Algorithms for Automatic Programming 8-87
8-6-2 Automatic Programming Settings 8-90
8-6-3 Automatic Programming Execution Procedure 8-93

8-7 Monitoring Memory Usage for Communication Control Unit 8-97

8-8 Monitoring Memory Usage for Safety Control Unit 8-98

8-9 Offline Debugging 8-100
8-9-1 Offline Safety Program Debugging 8-100
8-9-2 Monitoring 8-103
8-9-3 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing 8-103
8-9-4 Cross References 8-103
8-9-5 Setting the Initial Values of Variables 8-103
8-9-6 Feedback Settings 8-104
8-9-7 Simple Automatic Test 8-105

8-1 POUs (Program Organization Units)

The safety program that runs on an NX-series Safety CPU Unit is made from a combination of POUs (program organization units).
This section describes the configuration and specifications of POUs.
Refer to *8-5 Programming Operations* on page 8-27 for the procedures to create POUs on the Sysmac Studio.

8-1-1 POU

A POU (program organization unit) is a unit that is defined in the IEC 61131-3 user program execution model. A POU includes a local variable table and an algorithm (i.e., a series of code or logic). It is the basic unit used to build the safety program.
You combine POUs to build a complete safety program.
There are three types of POUs, as described below.

- Programs
  A program corresponds to a main routine. It is the main type of POU that is used for algorithms. You can place any instruction, function, or function block in the algorithm of a program.
- Function Blocks ("FBs")
  A function block can output different values even with the same inputs. Function blocks are executed when they are called from a program or another function block.
- Functions ("FUNs")
  A function always outputs the same values for the same inputs. Functions are executed when they are called from a program, another function, or a function block.

The POU consists of a combination of these three types of POUs. You can create many POUs.
You assign the created programs to a safety task to execute them. Only one safety task can be used by the Safety CPU Unit.

8-1-2 Overview of the Three Types of POUs

Program

● Executing Programs and Execution Conditions

- You execute a safety task to execute the programs that are assigned to that safety task.
- Programs are always executed.

● Notation

- The POUs must include at least one program. More than one program can be assigned to the safety task.

Function Blocks (FBs)

● Executing Function Blocks and Execution Conditions

- You can call function blocks from programs or other function blocks to execute them.
- Function blocks are always executed.
- To execute a function block for only specific conditions, pass a TRUE value to the *Activate* input variable of that function block. The function block is not executed if the value of the *Activate* input variable is FALSE.

● Notation

- There are both user-defined function blocks and system-defined function blocks.
  User-defined function blocks are sometimes called "user-defined FBs". System-defined function blocks are sometimes called "FB instructions".

For details on function blocks, refer to *8-1-5 Details on Function Blocks* on page 8-6.

Functions (FUNs)

● Executing Function and Execution Conditions

- You can call functions from programs or other function blocks to execute them.
- Functions are always executed.

● Notation

- You cannot create user-defined functions.
- System-defined functions are sometimes called "FUN instructions".
- The values of internal variables are not retained. The output value remains constant as long as input value is constant.

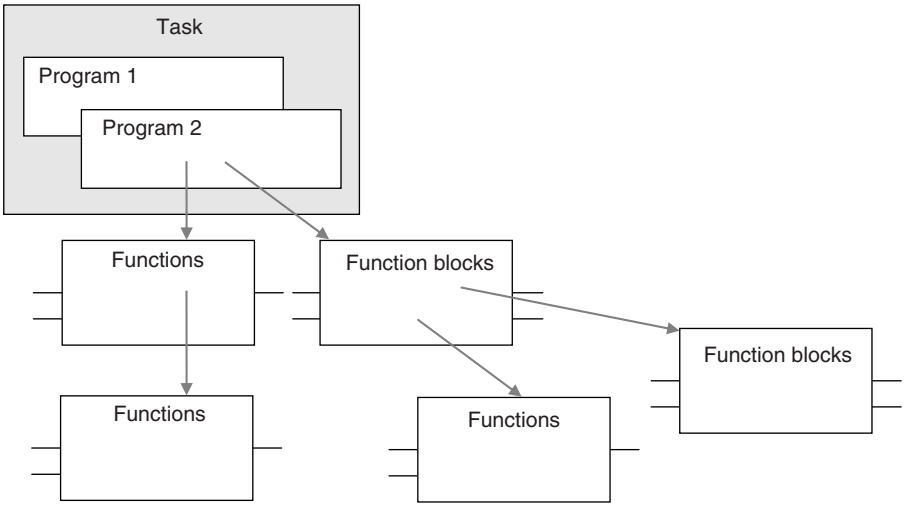
For details on functions, refer to *8-1-6 Details on Functions* on page 8-10.

8-1-3 Differences between Programs, Functions, and Function Blocks

POU type / Item		Programs	Function blocks	Functions
Types		User-defined only	Instructions or user-defined	Instructions only (User-defined functions not supported.)
Execution method		Executed upon execution of the safety task.	Called from a program or another function block.	Called from a program or function block.
Algorithm	**Any instructions**	Supported.	Supported.	Not supported.
	User-defined function blocks	Supported.	Supported.	Not supported.

POU type / Item	Programs	Function blocks	Functions
Execution condition	Always executed.	Always executed. Specify the execution condition with an input variable.	Always executed.

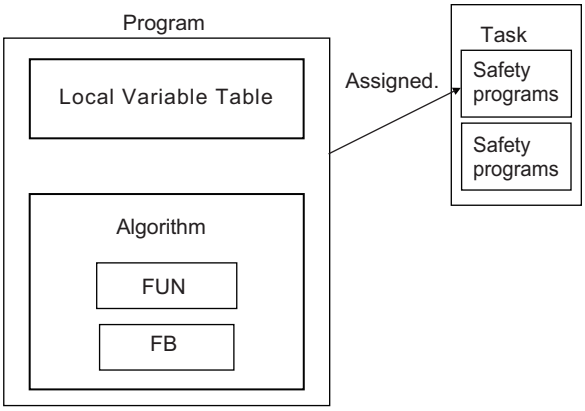
The hierarchical relationships between programs, functions, and function blocks are shown in the following figure.



8-1-4 Details on Programs

Program Structure

Programs consist of a local variable table and an algorithm.
The algorithm is programmed in the FBD language.
You can use any instructions or user-defined function blocks in the algorithm.



Program Execution Conditions

Programs are executed when the safety task they are assigned to is executed.

● Order of Execution

You can set the order of execution of all programs in a safety task.
You set this order in the **Program Assignment Settings** Display of the **Task Settings** Tab Page on the Safety CPU Unit Setup and Programming View on the Sysmac Studio. Refer to *8-5 Programming Operations* on page 8-27 for programming operations.

8-1-5 Details on Function Blocks

You can use system-defined function blocks (instructions) and user-defined function blocks in the Safety Control Unit.

Procedure to Create Function Blocks

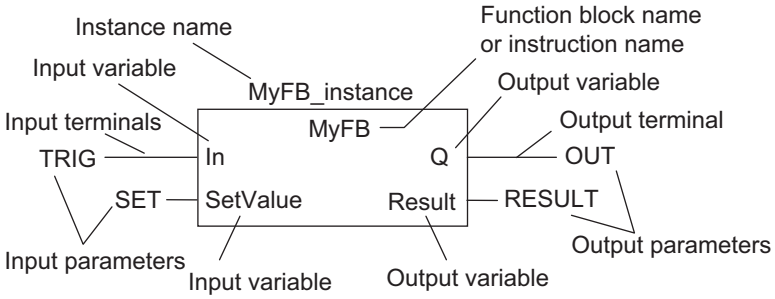
A function block consists of a "function block definition" that is made in advance and "instances" that are used in the actual programs.
Create function blocks in the following order.

1 Create the function block definition.
Create the algorithm.

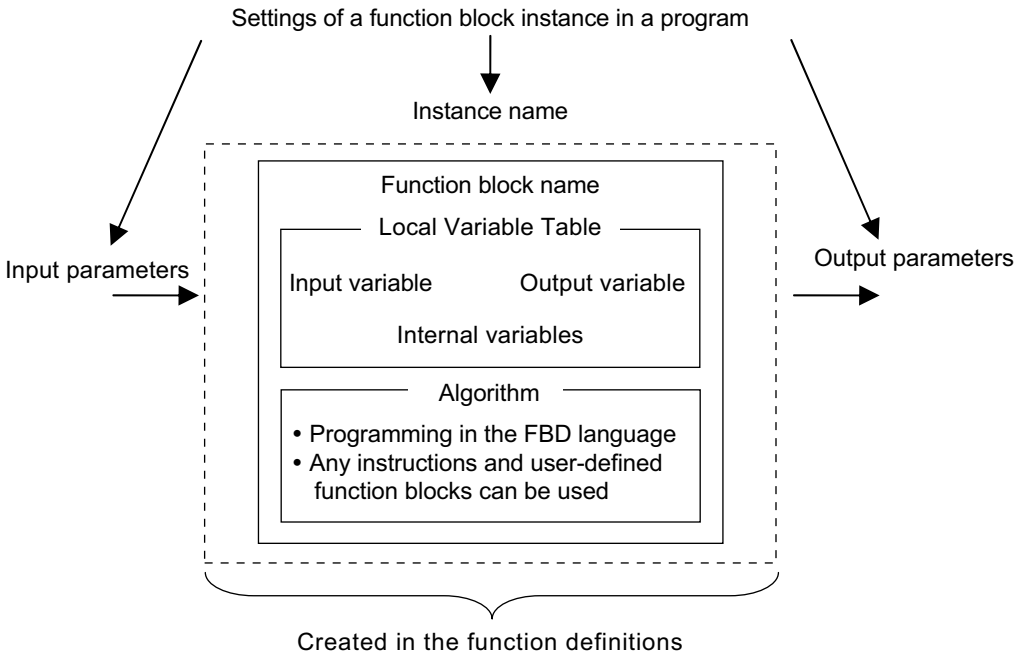
2 Place an instance of the function block definition in the program.
Call the function block definition from a program or another function block. You can call the same function block definition from more than one program or function block. After you place an instance of a function block definition in a program or in another function block, you can manipulate and execute it as an independent entity.

Structure of Function Blocks

With the FBD language, function blocks are represented as rectangular boxes as shown below.
Function blocks consist of the following parts.



- Function Block Settings
  When you create an instance of a function block definition, make the following settings.



● Function Block Name or Instruction Name

This is the name of the user-defined function block or the instruction.

● Instance Name

You give an instance name to a function block instance in a program to enable managing it.
You specify an instance name when you call a function block definition from a program or another function block.

● Algorithm

Algorithms are programmed in the FBD language.
You cannot use the ladder diagram language (LD) or the structured text language (ST).
You can use any instructions or user-defined function blocks in the algorithm.

● Local Variable Table

The local variable table contains the definitions for input variables, output variables, and internal variables.

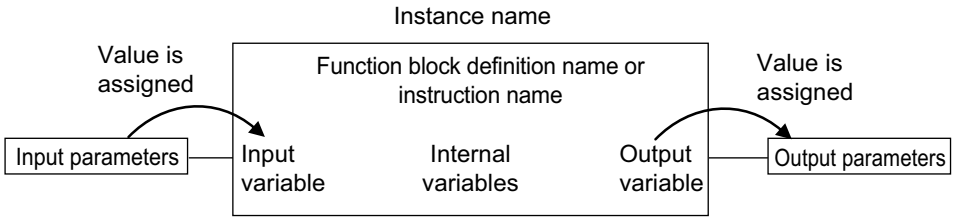
● Parameters

- Input Parameters to Input Variables
  An input parameter passes a value to an input variable in a function block when function block execution begins. An input parameter can be either a variable or a constant.
- Output Parameters from Output Variables
  An output parameter receives a value from an output variable in a function block when function block execution is completed. A variable is given as the parameter.

Additional Information

You can omit input and output parameters. For details on the operation, refer to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.

Variable Designations for Function Blocks



The specifications for variables in function blocks are given below.

Variables	Number*1	Specification
Input variables	1 to 64	Input variables are used as input arguments within the function block. They cannot be changed inside the function block.
		• When the function block is executed, the input variables are set to the values of the input parameters. • You can specify either constants or variables for input parameters. • Omitting Input Parameters: Refer to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.
Output variables	1 to 64	Output variables are used as output arguments from the function block.
		• The output parameters are set to the values of the output variables at the end of execution. • You cannot specify a constant for an output parameter. Only variables may be specified. • You can omit output parameter connections. If you omit an output parameter, the value of the output variable is not assigned to any parameter. • Omitting Output Parameters: Refer to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*. • You can access the values from outside of the function block. Access these values with the following format: *InstanceName.OutputVariableName*. However, you cannot write values directly to an output variable.
Internal variables	No limit	Internal variables are used for temporary storage within a function block.
		• The values of internal variables are retained regardless of whether the function block is executed. • The values cannot be referenced from outside of the function block.

*1. The individual restrictions are listed in the above table. The actual upper limits depend on the overall program capacity and internal memory capacity.

Refer to *8-2-4 Attributes of Variables* on page 8-13 for details on the variable attributes that can be set for each type of variable.

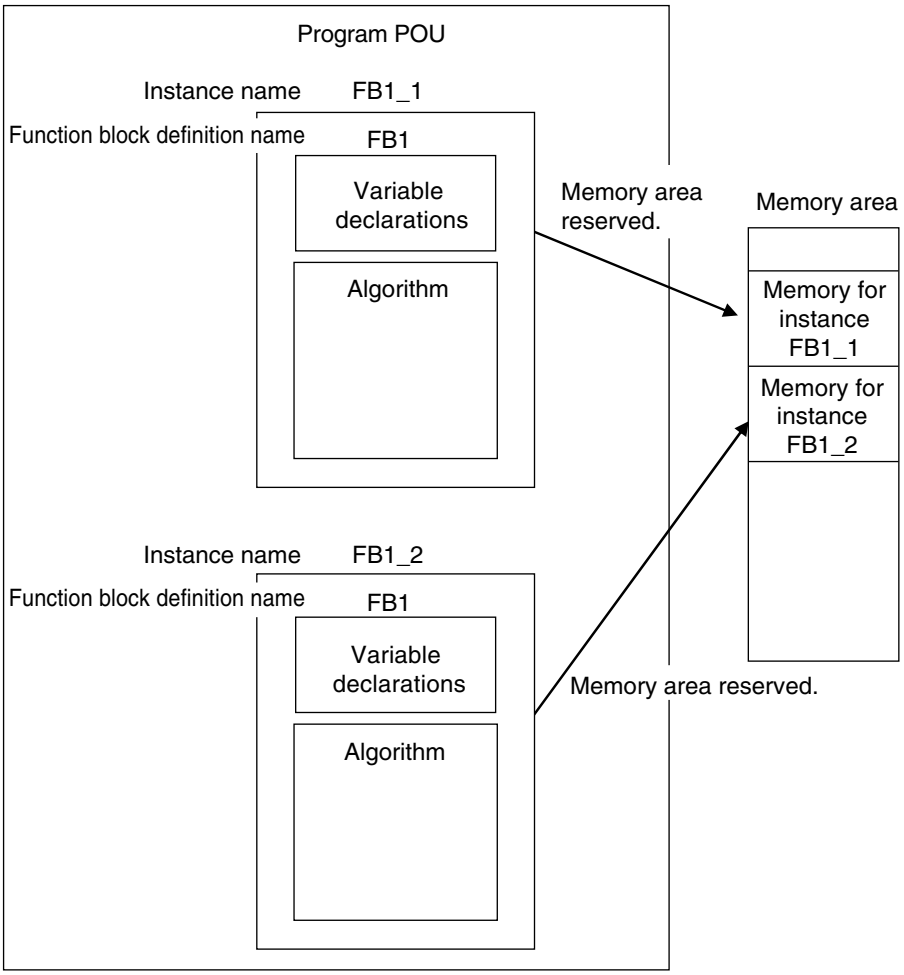
Function Block Definitions and Instances

A function block consists of a "function block definition" that is made in advance and "instances" that are used in the actual programs.
All instances of a function block are based on the "function block definition".
A "function block definition" consists of an algorithm and a local variable table.

Function Block Instance

When you place an instance of a function block definition in a program or another function block, the function block definition is treated as a part of that program or function block.
Function block definitions that are called from a program or another function block are called "instances".
Every instance of a function block has an identifier known as an instance name associated with it, and every instance uses memory.

You can use a single function block definition to create more than one "instance". This allows you to process different I/O data with the same function.



If you place instance names *FB1_1* and *FB1_2* for function block FB1 in the program, each instance requires its own space in memory.
"Instances" cannot be read from other programs or function blocks. If an instance with the same name as another instance is placed in a different program or another function block, that instance will operate as a completely separate instance.

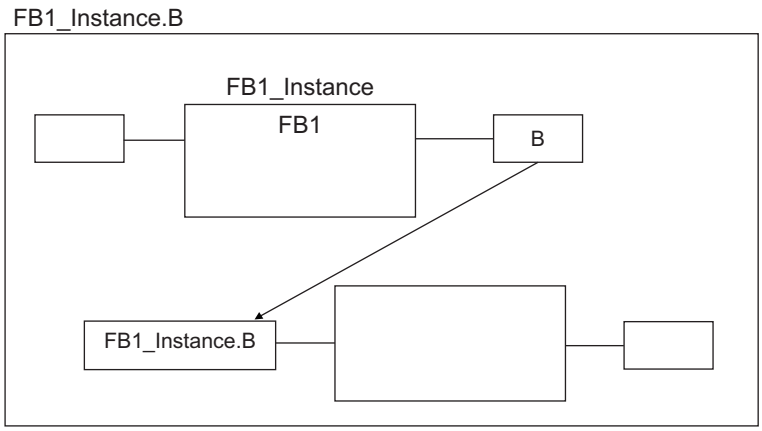
Precautions for Correct Use

In the following conditions, a user-defined function block will cause an error during the program check when the program is built.
- The same function block instance was called more than once in the POU.
- The instance of the function block was registered as a global variable.

Accessing Variables in a Function Block from Outside the Function Block

You can access the input and output variables of a function block from outside the function block. Variables are written as follows:
InstanceName.VariableName

Example: To Access Output Variable *B* of Function Block Instance *FB1_Instance*



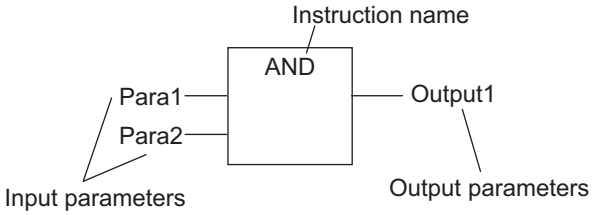
You can access the input and output variables for a function block only within the program that contains the function block.
However, you cannot access these variables from within other function block instances even if they are in the same program. You cannot access them from other programs.

8-1-6 Details on Functions

You cannot create user-defined functions for Safety Control Units. Only system-defined functions (instructions) are allowed.

Structure of Functions

With the FBD language, functions are represented as rectangular boxes as shown below.
A function consists of the following parts.
This function is expressed in the FBD language:



● Instruction Name

This is the instruction name.

● Instance Name

Functions do not have instance names.

8-1-7 Instructions

Instructions are the smallest unit of the processing elements that are provided by OMRON for use in POU algorithms.
There are FB instructions and FUN instructions.
Programs and user-defined function blocks consist of a combination of these instructions.

You can press a shortcut key to display help for an instruction.
Select an instruction that was previously entered in the FBD editor or select an instruction in the Instruction Navigator in the Toolbox, and then press the **F1** Key.



Additional Information

An instruction refers to a system-defined function or function block.
The following table shows the relationship between user-defined and system-designed functions and the FUN or FB.

	User-defined functions	System-defined = Instructions
FB	Supported	Supported
FUN	Not supported	Supported

For details on instructions, refer to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.

8-2 Variables

In the Safety CPU Unit, variables are used to exchange I/O information with external devices, to perform data calculations, and to perform other processes.
This section describes variable designations in detail.

8-2-1 Variables

Variables store I/O data for exchange with external devices or temporary data that is used for internal POU processing. In other words, a variable is a data container with attributes, such as the name and data type.

You do not need to assign a memory address to a variable. The Sysmac Studio automatically allocates memory addresses in the memory area for variables.

8-2-2 Types of Variables

Variables are broadly classified into the following two types.

- **User-defined Variables**

  The user defines all of the attributes of a user-defined variable.
  The rest of this section describes "user-defined variables".

- **Semi-user-defined Variables**

  For semi-user-defined variables, some attributes are designed by the system, while others are defined by the user.
  This includes variables that are used to access specific devices and data.
  This is the equivalent of a "device variable" in the Safety Control Unit.

8-2-3 Type of User-defined Variable

There are five types of user-defined variables as defined according to their function in a POU.

Type of user-defined variable		POU type	
		Programs	FB
Local variables	Internal variables	Provided	Provided
	Input variables	Not provided	Provided
	Output variables	Not provided	Provided
	External variables	Provided	Not provided
Global variables		Provided*1	Not provided

*1. You can define global variables as external variables to access the global variables through the external variables.

Local Variables

A local variable can be read and written only inside the POU (program or function block) in which it is defined.
“Local variables” is the generic term for internal variables, input variables, output variables, and external variables.

● Internal Variables

An internal variable can be used only within one POU.
An internal variable is declared in the local variable table of the POU.
You cannot access the values of internal variables from outside of the POU.
You can declare an internal variable with the same name in different POUs. In this case, memory is allocated separately for each variable.

● Input Variables

When a POU is called, the values of the input parameters are assigned to the input variables from the calling POU. An input variable is declared in the local variable table of the POU.

● Output Variables

Before processing a POU is completed, the output parameters returned to the calling POU are assigned to the output variables. An output variable is declared in the local variable table of the POU.

● External Variables

External variables are used to access global variables from a POU.

Global Variables

A global variable is declared in the global variable table.

Device variables that are automatically created are automatically registered as global variables.

8-2-4 Attributes of Variables

You can set the following attributes for variables.

Variable Attributes According to Variable Type

● Attributes of Variables

Attribute	Description	Specification	Default
Variable Name	The variable name is used to identify the variable.	UTF-8 format 127 bytes max.	Name
Data Type	The data type defines the format of the data that is stored in the variable.	---	BOOL

Attribute	Description	Specification	Default
Initial Value	Specify a value for the variable for one of the following situations: • When the power supply is turned ON • When the mode is changed to RUN mode or DEBUG mode.	This setting is required.	FALSE for BOOL and SAFEBOOL variables, and 0 for numeric variables.
Constant	If you set the Constant attribute, you can set the initial value of the variable when it is downloaded, but you cannot overwrite the value afterward.	Specify making the value a constant or not a constant.	Do not specify a constant.
Comment	You can add comments to variables.	UTF-8 format 127 bytes max.	None (empty).

● Attributes Supported by Each Type of Variable

Type of variable		Variable Name	Data Type	Initial Value	Constant	Comment
Global variables		Supported.	Supported.	Supported.	Supported.	Supported.
Programs	**Internal variables**	Supported.	Supported.	Supported.	Supported.	Supported.
	External variables	Not supported.	Not supported.	Not supported.	Supported.	Supported.
Function blocks	**Internal variables**	Supported.	Supported.	Supported.	Supported.	Supported.
	Input variables	Supported.	Supported.	Supported.	Not supported.	Supported.
	Output variables	Supported.	Supported.	Supported.	Not supported.	Supported.

Additional Information

The following comments are linked. If you change a comment, the comment for the corresponding parameter is also changed.
- Device variable comments in the I/O Map
- Global variable comments
- I/O terminal comments in the Parameters Tab Page

8-2-5 Data Type

The Data Type attribute defines the type of data and range of data that is expressed by a variable. The amount of memory that is allocated when you declare a variable depends on the data type of that variable. The more memory allocated, the larger the range of values that the variable can express.
The data types for the input and output variables of instructions depend on the instruction. Set the data types of input and output parameters for the instruction arguments according to the data types of the input and output variables for that instruction.
The Safety Control Unit allows the use of only pre-defined basic data types. You cannot use user-defined derivative data types, such as structures, unions, and enumerations, or array specifications.

Basic Data Types

The basic data types that you can use with the Safety Control Unit are listed below.

Type	Definition
Boolean	A data type with a value of either TRUE or FALSE.
Bit string	A data type that represents a value as a bit string.
Integers	A data type that represents an integer value.

Type	Definition
Duration	A data type that represents a time duration (days, hours, minutes, seconds, and milliseconds).

Safety Data Types and Standard Data Types

The Safety Control Unit classifies data types into the following two types to distinguish between safety data and standard data.

- Safety data types: These data types represent data related to safety control.
- Standard data types: These data types represent data related to standard control.

"SAFE" is prefixed to the names of the standard data types such as SAFEBOOL, to create the names of the safety data types.

You can input a signal for a safety data type variable to a standard data type variable.
You cannot input a signal for a standard data type variable to a safety data type variable. A building error will occur.

Basic Data Types

The basic data types are given below.

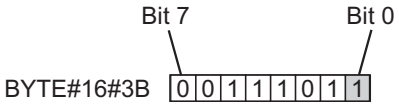
Classification	Data type	Safety/ standard data type	Range of values	Notation
Boolean	**BOOL**	Standard data type	FALSE or TRUE	bool#0 or bool#1 FALSE or TRUE
	SAFEBOOL	Safety data type		
Bit strings	**BYTE***1*2	Standard data type	byte#16#00 to byte#16#FF	byte#2#0101010 byte#2#0101_1010 byte#16#5A You can use the separator character "_".
	WORD*3	Standard data type	word#16#0000 to word#16#FFFF	
	SAFEWORD*4	Safety data type		
Integers	**INT**	Standard data type	int#-32768 to int#-32767	100 int#100 int#2#00000000_1100100 int#16#64 -100
	SAFEINT	Safety data type		
	DINT	Standard data type	dint#-2147483648 to dint#-2147483647	
	SAFEDINT	Safety data type		
Duration	**TIME***4	Standard data type	t#0ms(t#0d0h0m0s0ms) to t#4294967295ms (t#49d17h02m47s295ms)	t#3000ms
	SAFETIME*4	Safety data type		

*1. The BYTE data type cannot be used for an internal variable.
*2. If you use the BYTE data type for a global variable, you must define an exposed variable.
*3. If you use the WORD data type for a global variable, you must define an exposed variable or use a constant.

*4. If you use the SAFEWORD, TIME, or SAFETIME data type for a global variable, you must set a constant.

Bit String Data Format

This section describes the data format for bit string data.
"Bit 0" is the least significant bit of a bit string variable.
Bit values are expressed as 1 or 0.



8-2-6 Variable Attributes Other Than Data Type

This section describes the variable attributes other than the Data Type.

Variable Name Attribute

The variable name is used to identify the variable.
Each variable in a POU must have a unique name. However, you can declare local variables with the same variable name in different POUs. These are treated as two separate variables.
You cannot declare an internal variable with the same variable name as a global variable.

Initial Value Attribute

The variable is set to the initial value in the following situations.

- When the power supply is turned ON
- When the mode is changed to RUN mode
- When the mode is changed to DEBUG mode (STOPPED)

● Types of Variables That Can Have Initial Values

You can set initial values for only some types of variables. A list is provided below.

Variables	Initial Value Settings
Global variables	Yes (required)
Internal variables	
Input variables	
Output variables	
External variables	Not possible.

You must set initial values for all variables that allow them.

Constant Attribute

The Constant attribute prohibits instructions from writing values to a variable. Setting the Constant attribute will prevent any program from overwriting the variable.

The values of variables with a Constant attribute cannot be written from instructions after the initial value is set. If there is an instruction in a POU that attempts to write a value to a variable with the Constant attribute, an error will occur when the program is built.

8-2-7 Function Block Instances

Function block instances are added to and displayed in the local variable table or the global variable table as data types.



Additional Information

A function block instance is treated as a local variable of the program in which the instance is created. As such, the instance is added to and displayed in the local variable table of the program.

8-2-8 Restrictions on Variable Names and Other Safety Program-related Names

The following table lists the restrictions on variable names and other safety program-related names.

Character Restrictions

Safety program-related name	Applicable characters	Reserved words	Multi-byte character compatibility	Case sensitivity	Maximum size *1 (not including NULL)	Character code
Variable names (including POU instance names)	**Usable characters** • 0 to 9, A to Z, and a to z • Single-byte kana • _ (underlines) Refer to *Reserved Words* below for a list of the reserved words. **Characters that cannot be used together** • A text string that starts with a number (0 to 9) • A text string that starts with “P_” • A text string that starts in an underline (_) character • A text string that contains two or more consecutive underline (_) character • A text string that ends in an underline (_) character • Identifiers formed from a string of characters that is prefixed or suffixed with one or more expansion characters or spaces	Refer to *Reserved Words* below.	Not supported	Not case sensitive.	127 bytes	ASCII
POU definition names						
Full path of variable names (Example: This includes the number of characters for the instance name and period, which is InstanceName.OutputVariableName when accessing the output variable of a function block.)					511 bytes	
Device names					127 bytes	
Variable comments		None	Supported	---	127 bytes	UTF-8

*1. The individual restrictions are as listed in the table. The actual upper limits depend on the overall program capacity and memory capacity for variables.

Reserved Words

An error is detected during the program check for the following names.

- Use of the same name as any of the instructions that are described in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*
- Words that are reserved by the system

Names that Must Be Unique

The following names must be unique. Otherwise, errors will be detected in a program check.

- Global variable names in the same Safety CPU Unit
- Variable names in the same POU

- Local variable names and global variable names

8-3 Constants (Literals)

This section describes constants.

8-3-1 Constants

The value of a variable changes depending on the data that is assigned to that variable. The value of a constant never changes.
Unlike variables, constants are not stored in memory. You can use constants in the algorithm of a POU without the need to declare them.
Constants have a "data type" in the same way as variables.

8-3-2 Types of Constants

The following types of constants can be used with Safety Control Units.

- Bits
- Numbers
- Bit strings
- Times

The following tables show the notation to define different constants for the Safety Control Unit. The constant is normalized after it is entered.

Bits

Notation	Example	Remarks
TRUE or FALSE	FALSE or TRUE	
{data_type}#{numeric_value}	bool#0 or bool#1	Data type: BOOL

Numbers

● Integers

Notation	Example	Remarks
{data_type}#{base}#{numeric_value}	int#10#1	• Data type: int or dint • Base: 2, 8, 10, or 16 The editor on the Sysmac Studio does not show the base of 10. Values entered as the base of 8 are converted to decimal numbers. • Numeric values cannot be signed (+ or −).
{data_type}#{numeric_value}	int#1	This is interpreted as decimal data.
{numeric_value}	-100	This is interpreted as SAFEINT or SAFEDINT data.

Bit Strings

● Bit String Data

Notation	Example	Example
{data_type}#{base}#{numeric_value}	word#16#0064	• Data type: BYTE or WORD • Base: 2, 8, 10, or 16 The normalizing processing omits the base of 10 and converts values entered as base of 8 to decimal numbers.
{data_type}#{numeric_value}	word#100	This is interpreted as decimal data.

Times

● Durations

Notation	Example	Remarks
{Data type}#{days}d{hours}h{minutes}m{seconds}s{milliseconds}ms	t#61m5s	Data Type: t

8-4 Programming Languages

This section describes the programming languages in detail.
Refer to *8-5 Programming Operations* on page 8-27 to learn how to enter the programming languages on the Sysmac Studio.

8-4-1 Programming Languages

The languages used to express the algorithms in a POU (program or function block) are called the programming languages.
FBD is the only programming language that can be used with the Safety Control Unit.

8-4-2 FBD Language

The FBD language is a graphical programming language that is used for programmable controllers and is defined by IEC 61131-3.
You use connecting lines to show the data flow, and rectangular boxes to represent functions and function blocks to write algorithms.

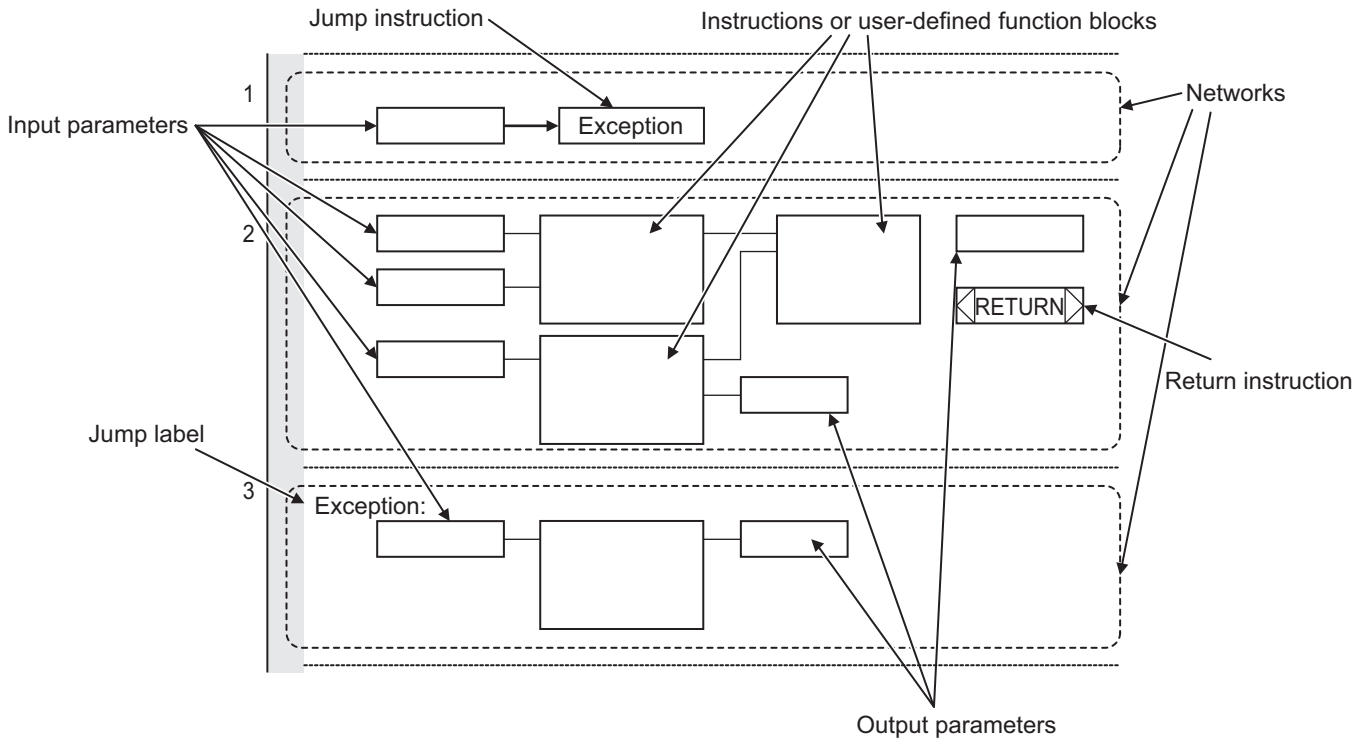
Elements of the FBD Language

An algorithm in the FBD language is a unit made up of a series of elements, called "networks", that connect the inputs to the outputs. The networks consist of the following elements.

- Input parameters
- Connecting lines
- Instructions (FUN or FB instructions) or user-defined function blocks
- Output parameters

In a network, signals flow from the inputs on the left to the outputs on the right.

- Input parameters and output parameters are arguments that are written with variables or constants. These arguments are written in the areas that are connected to the terminals of input variables or output variables inside the instructions or user-defined function blocks with connecting lines.
- The connecting lines show the flow of the following three types of signals.
  a) Flow between input and output parameters and instructions
  b) Flow between terminals on user-defined function blocks
  c) Horizontal and vertical flow between instructions or between user-defined function blocks
- Instructions and user-defined function blocks are represented by rectangular boxes. You can use connecting lines to connect input variables or output variables. Some terminals do not need to be connected with a connecting line.



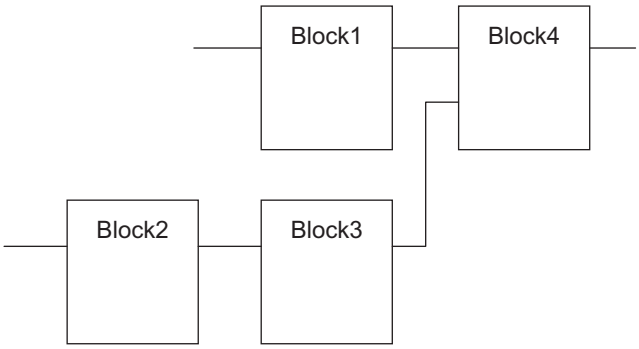
The networks shown above include a Jump instruction that changes the top-to-bottom flow of execution between networks, a label that shows the network to jump to, and a Return instruction.
Refer to *Execution Order of Safety Programs Written in the FBD Language* on page 8-23 and *Execution Control* on page 8-24 later in this manual, and also to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)* for details.

Additional Information

- Unlike the ladder diagram language, the FBD language does not have bus bars. The connecting lines do not indicate power flow. They indicate the flow of data. The FBD language does not have an END instruction. Execution for the task period ends when the last network is executed.
- In this manual, "FBD network" is sometimes used to differentiate programming networks from physical networks, such as EtherCAT networks.

Execution Order of Safety Programs Written in the FBD Language

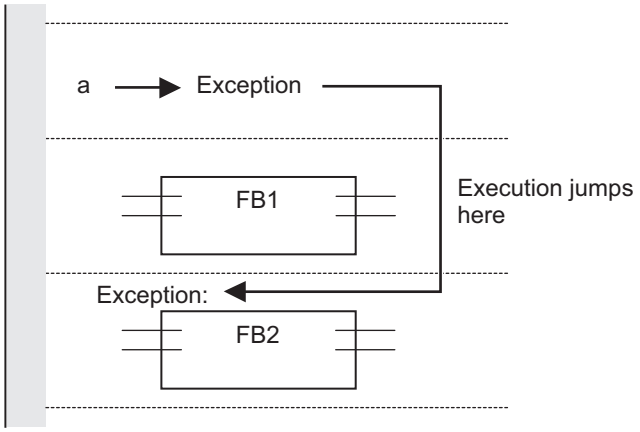
In POUs that are written in the FBD language, networks are executed in order from top to bottom. Processing ends when the network at the very bottom of the program is executed.
Elements in the same network are executed from top to bottom for FUN and FB inputs and left to right for blocks that are connected in series. In the following example, execution is in the following order: Block 1, Block 2, Block 3, and then Block 4.



However, if there is a Return instruction in the middle of a program and the execution condition is met, the POU is ended and a return is made to the source of the call. No processes after Return instruction are executed.

Execution Control

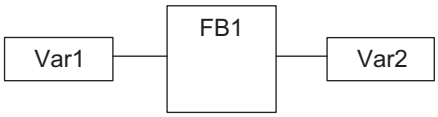
Safety programs that are written in the FBD language are generally executed from top to bottom, but you can use the Jump instruction to change the execution order.
For example, when the value of variable *a* changes to TRUE in the following example, execution will move to the network labeled "Exception".
You cannot jump to a network that is above the current network.



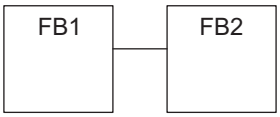
Connecting Instructions or User-defined Function Blocks

● Correct Connection Configurations

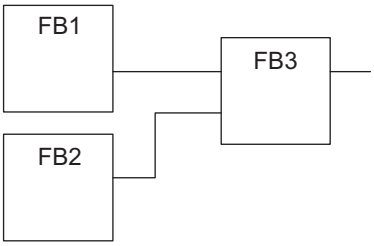
Parameters and commands, or user-defined function blocks can be connected with a connecting line.



The connecting line can connect two instructions or two user-defined function blocks.

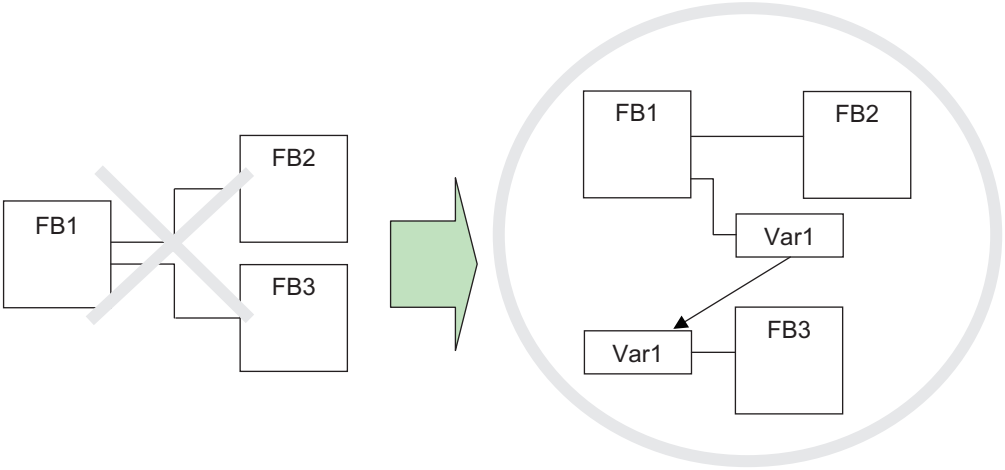


Multiple instructions or user-defined function blocks can be connected to a single instruction or user-defined function block.

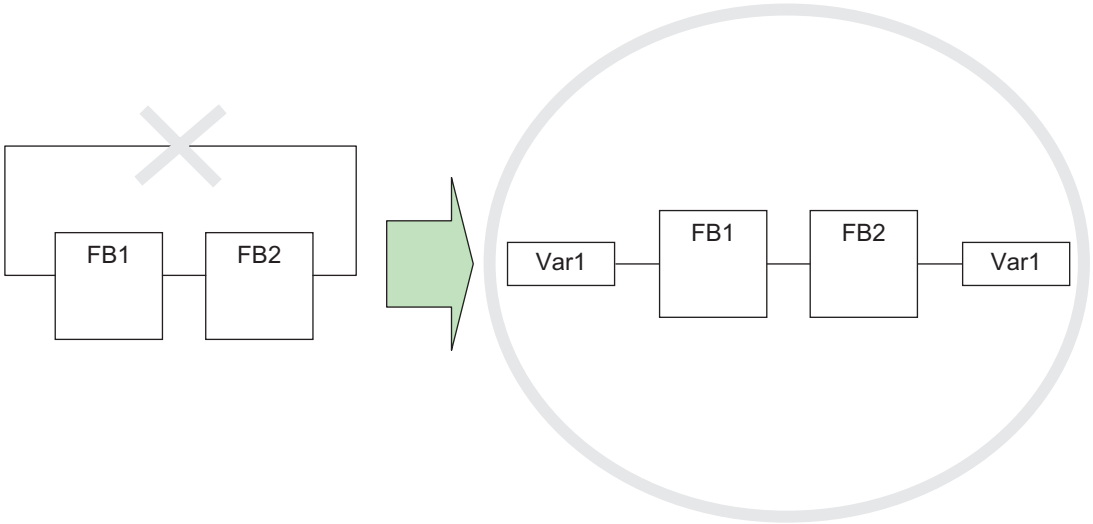


● Incorrect Connection Configurations

You cannot connect more than one instruction or user-defined function block to the right of another instruction or user-defined function block. In this case, you must pass the signal to a variable as shown in the following figure.



You cannot route a connecting line from the output to the input. In this case, you must pass the signal to a variable as shown in the following figure.

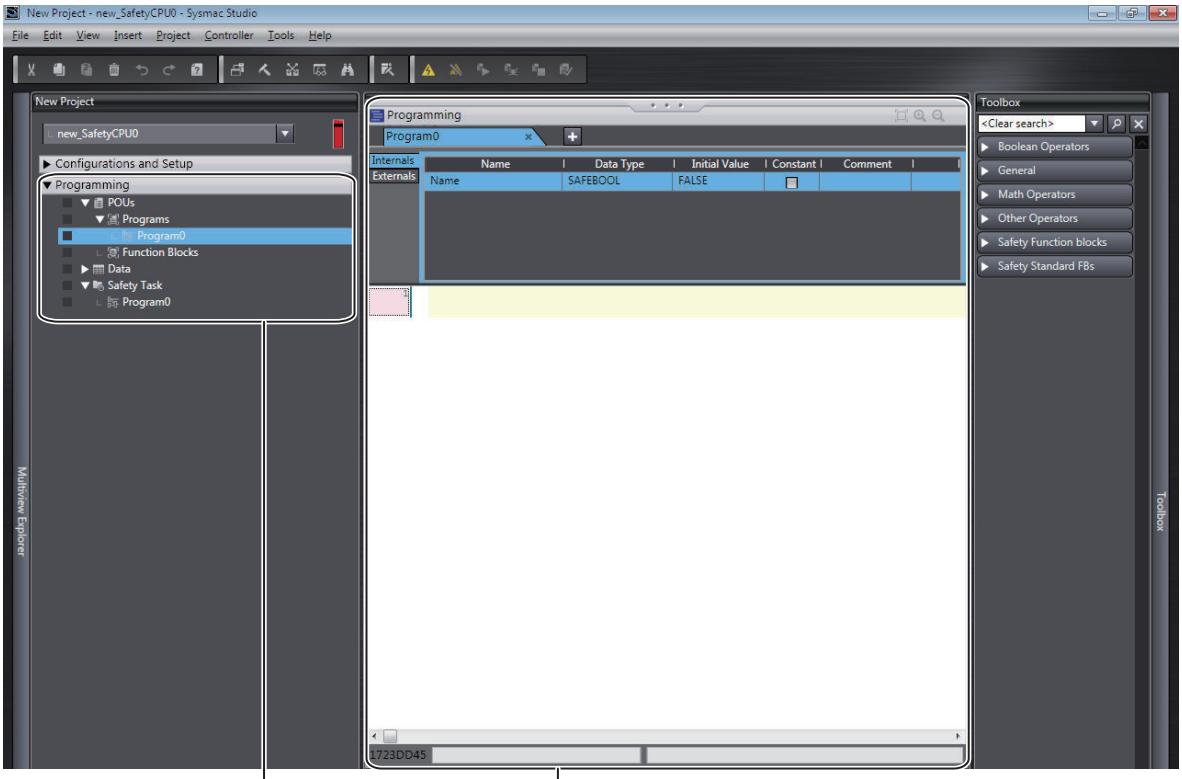

FB1
FB2
Var1
FB1
FB2
Var1

8-5 Programming Operations

This section describes the procedures on the Sysmac Studio that you use to create safety programs for the Safety CPU Unit.

8-5-1 Programming Layer on the Sysmac Studio

You use the Programming Layer with the Controller set to the Safety CPU Unit on the Sysmac Studio as shown below to create safety programs for the Safety CPU Unit.

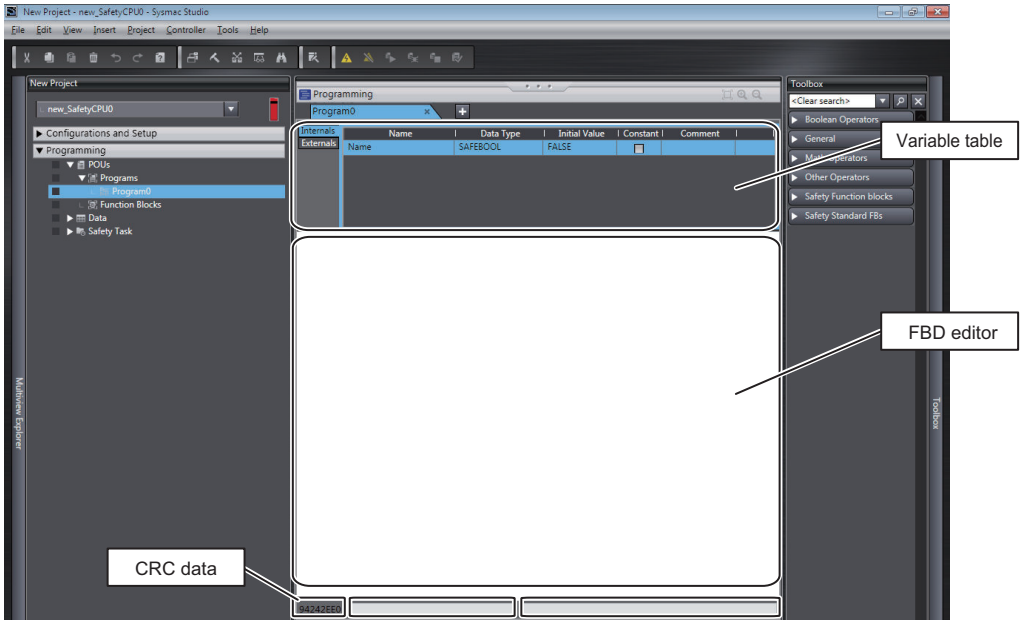


The Programming Headers of the Multiview Explorer are organized as shown below.

Programming Header	Description
POUs	
Programs	
Program0	The list of programs is displayed. "Program0" is created when a new project is created. Double-click a program to display it in the FBD editor and begin editing. In the Multiview Explorer, you can change the names of programs or delete, copy, paste, and cut programs.
Program1	
Function Blocks	

Programming Header			Description
		FunctionBlock0	A list of user-defined function blocks is displayed. There are no function blocks when you create a new project. Double-click a function block to display it in the FBD editor and begin editing. You can change the name, delete, copy, paste, and cut function blocks.
		FunctionBlock1	
Data			
	Global variables		Double-click Global Variables to display the Global Variable Table and begin editing.

The structure of the Edit Pane is shown below.



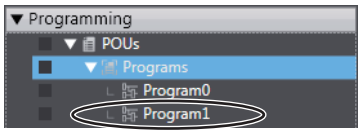
Item	Editing	Description
Variable table	Possible	Displays the local variables.
FBD editor	Possible	Displays the FBD network.
CRC data	Not possible	Displays the CRC data of the POU.

8-5-2 Registering POUs

This section shows how to register programs and function blocks.

Registering New Programs

1 Right-click **Programs** under **Programming** - **POUs** and select **Add** - **Program** from the menu. A new program is added under **Programs**.



2 Double-click the **Program1** that was added.

The variable table and FBD editor are displayed in the Edit Pane. From here you can edit programs.
Refer to *8-5-3 Registering Variables* on page 8-38 for information on how to register variables, and *8-5-4 FBD Programming* on page 8-46 for information on programming in the FBD editor.

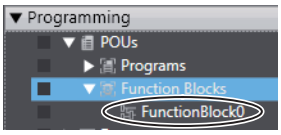
Registering Function Blocks

Function blocks are written in the FBD language. You can call them from safety programs as required. You can use functions inside function blocks.
Refer to *8-1-2 Overview of the Three Types of POUs* on page 8-3 for a detailed description of function blocks.

● Registering New Function Block

This section describes the procedures for registering a new user-defined function block.
Function block instructions are registered in the Sysmac Studio in advance. You do not need to register function block instructions to use them.

1 Right-click **Function Blocks** under **Programming** - **POUs** in the Multiview Explorer and select **Add** - **FunctionBlock** from the menu.
A new function block is added under **Function Blocks**.



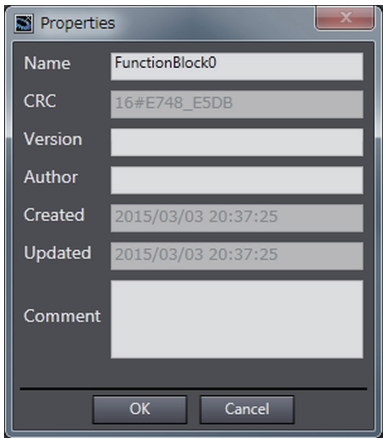
2 Double-click the new function block.
The variable table for the function block and the FBD editor are displayed in the Edit Pane.
From here you can create local variables and FBD networks.

Refer to *8-5-3 Registering Variables* on page 8-38 for information on how to register variables, and *8-5-4 FBD Programming* on page 8-46 for information on programming in the FBD editor.

Displaying Properties

This section describes how to display program and function block properties.

Right-click the registered program or function block and select **Properties** from the menu.
The Properties Dialog Box is displayed.



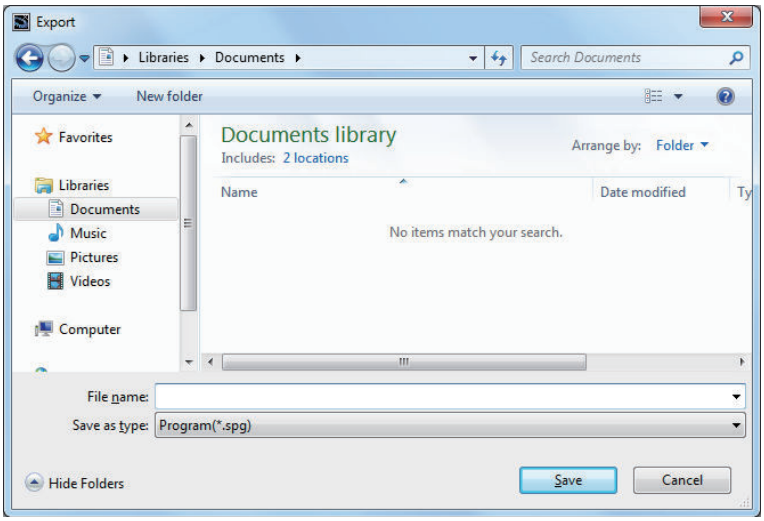
The following table describes the items in the Property Dialog Box.

Item	Editing	Description
Name	Possible	This is the name that is currently set for the POU.
CRC	Not possible	This is the CRC data of the POU. You can also check the CRC data on the **Change Tracking** Tab Page.
Version	Possible	This is the version information for the POU. You can also check the version information on the **Change Tracking** Tab Page.
Author	Possible	This is the person that created the POU.
Created	Not possible	This is the date that the POU was created.
Updated	Not possible	This is the date that the POU was updated.
Comment	Possible	This is a comment for the POU.

Exporting Programs

You can export a program to a file (extension .spg).
You can import an exported program to reuse it in another project.
Use the following procedure.

1 Right-click a program displayed under **Programming** - **POUs** - **Programs** in the Multiview Explorer, and then select **Export** from the menu.
The **Export** Dialog Box is displayed.



2 Enter a file name, and then click the **Save** Button.
A program file with an .spg extension is saved.

Precautions for Correct Use

- Do not delete the program CRC data that is displayed after the program is exported. It is used to check the data when importing the program.
  You can check the CRC data on the **Change Tracking** Tab Page or Properties Dialog Box.
- The spg program file includes information on global variables that are used as external variables.

Importing Programs

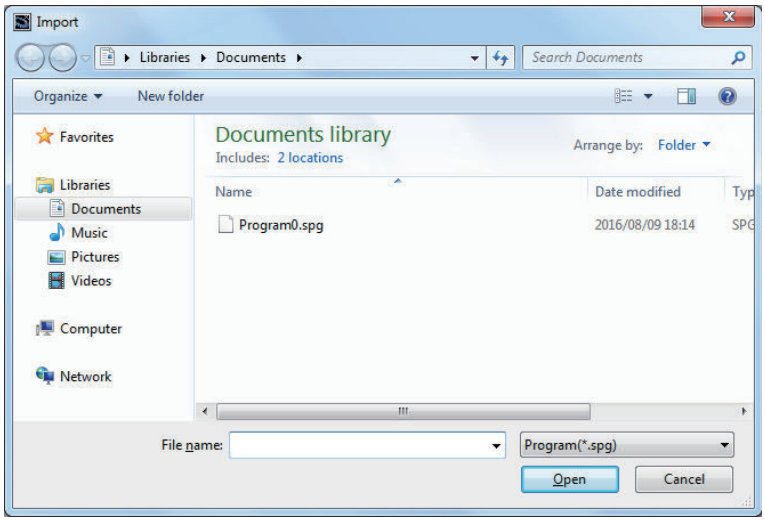
You can import an exported program to reuse it in another project.

⚠ WARNING

Check during the import of the program that the CRC of the program is correct. Serious injury may possibly occur due to loss of required safety functions.

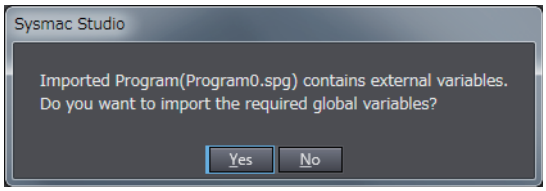
Use the following procedure to import a program that was previously exported.

1 Right-click **Programs** under **Programming-POUs** in the Multiview Explorer and select **Import** from the menu.
The **Import** Dialog Box is displayed.

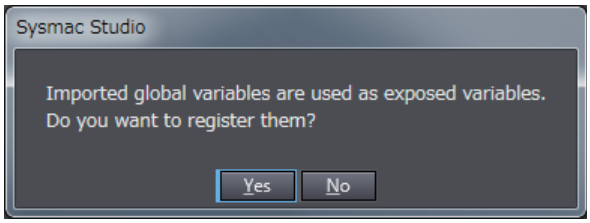


When you select the files to import, you can press the**Shift**Key or**Ctrl**Key to select more than one file.

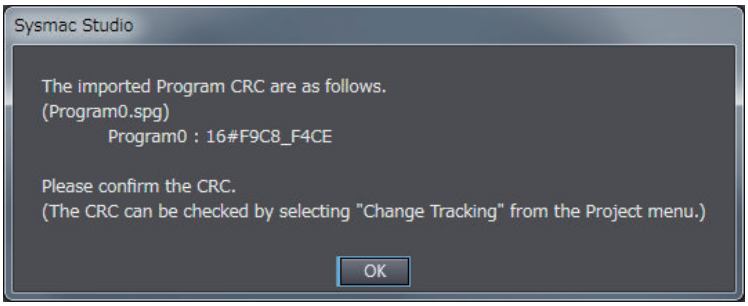
2 Select the .spg file to import, and then click the**Open**Button.
When external variables are used in the program to import, the following dialog box is displayed.
Select**Yes**to register the variables as global variables.



When the registered global variables are used as exposed variables, the following dialog box is displayed.
Select**Yes**to register the variables as exposed variables.



A dialog box to check the CRC data is displayed.



3 Check the CRC data, and click the **OK** Button.
The program is imported and added to the project.

Precautions for Correct Use

After a function block is imported, the safety program in the project will be in an unvalidated state. Always execute safety validation again.

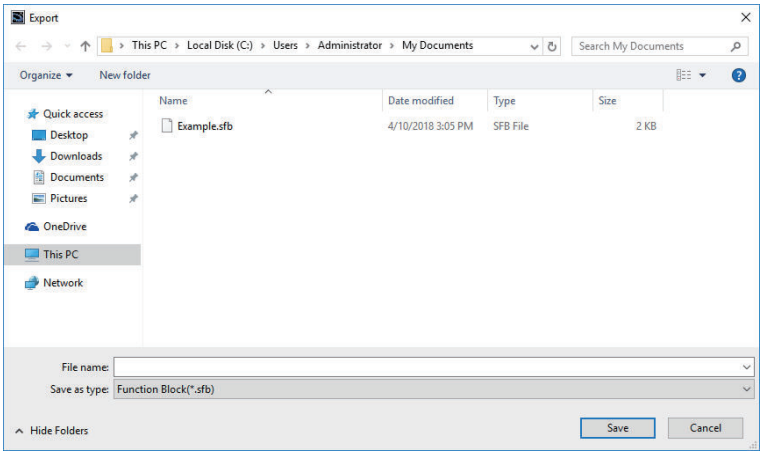
Additional Information

You can check the CRC data on the **Change Tracking** Tab Page or Properties Dialog Box.

Exporting User-defined Function Blocks

You can export a user-defined function block to a file (extension .sfb).
You can import the exported user-defined function block to reuse it in another project.
Use the following procedure.

1 Right-click the user-defined function block under **Programming** - **POUs** - **Function Blocks** in the Multiview Explorer and select **Export** from the menu.
The **Export** Dialog Box is displayed.



2 Enter a file name, and then click the **Save** Button.
A function block file with an .sfb extension is saved.

Precautions for Correct Use

- Do not delete the function block CRC data that is displayed after the function block is exported. It is used for data confirmation when the function block is imported.
  You can check the CRC data on the **Change Tracking** Tab Page or Properties Dialog Box.
- A help file is not included with the user-defined function block file (sfb).

Importing User-defined Function Blocks

You can import the exported user-defined function block to reuse it in another project.

⚠ WARNING

Check during the import of the user defined function that the CRC of the imported function block is correct. Serious injury may possibly occur due to loss of required safety functions.

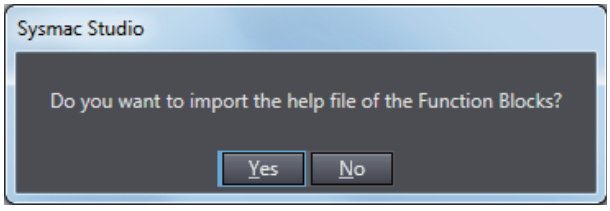
Use the following procedure to import a user-defined function block that was previously exported.

1 Right-click **Function Blocks** under **Programming** - **POUs** in the Multiview Explorer and select **Import** from the menu.
The **Import** Dialog Box is displayed.



When you select the files to import, you can press the **Shift** Key or **Ctrl** Key to select more than one file.

2 Select the .sfb file to import, and then click the **Open** Button.
The following dialog box is displayed. To import the function block help file, select **Yes**.

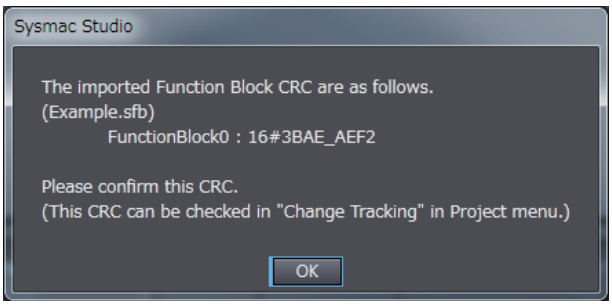


When a function block help file is imported, the following **Import** Dialog Box is displayed.



If you select a help file (.pdf extension) with the same name as the imported function block, the specified file is copied to the save location for the user-defined help file.

A dialog box to check the CRC data is displayed.



3 Check the CRC data, and click the **OK** Button.
The function block is imported and added to the project.

Precautions for Correct Use

After a function block is imported, the safety program in the project will be in an unvalidated state. Always execute safety validation again.

Additional Information

You can check the CRC data on the **Change Tracking** Tab Page or Properties Dialog Box.

Help for User-defined Function Blocks

In the FBD editor, select the user-defined function block and then press the **F1** Key to open the help file.

● Setting a Help File

Use the following procedure to set a help file for a user-defined function block.

1 Prepare a help file with the same name as the function block (extension .pdf).

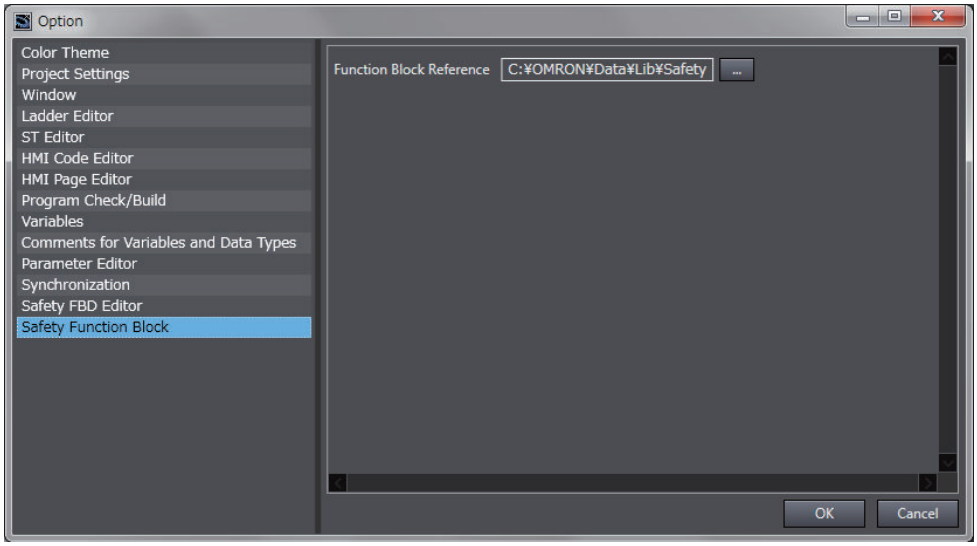
2 Save the help file in the specified folder.
The default folder is C:\OMRON\Data\Lib\Safety.

● Changing the Save Location for Help Files

You can change the folder in which help files are saved.
Use the following procedure.

1 Select **Option** from the **Tools** Menu.
The **Option** Dialog Box is displayed.

2 Click the **Safety Function Block**.
The help save location is displayed.



3 Select the folder in which to save the help files and click the **OK** Button.
The save location for help files for user-defined function blocks is changed.

Importing IEC 61131-10 XML Files

This function imports XML files that conform to IEC 61131-10. You can import global variables and POUs described in FBD language from the XML file.

An example of writing XML is installed by default in the following folder. To check the data supported by this function, refer to the XML schema in the same folder.

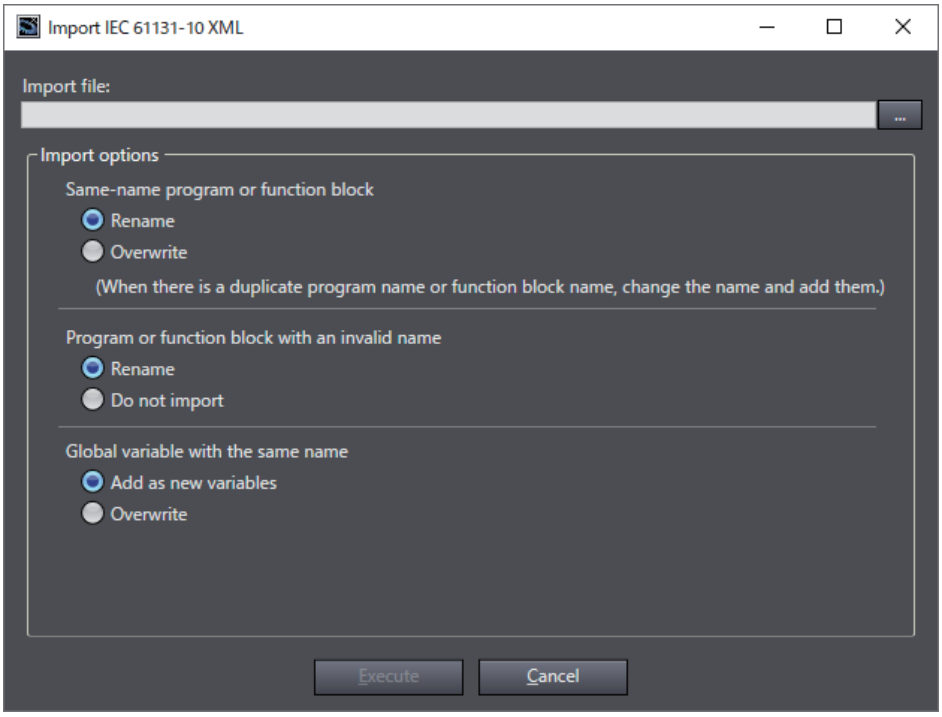
- **Sysmac Studio (32 bit)**
  For 32-bit OS:
  C:\Program Files\OMRON\Sysmac Studio\Sample\IEC 61131-10 XML\Safety

For 64-bit OS:
C:\Program Files (x86)\OMRON\Sysmac Studio\Sample\IEC 61131-10 XML\Safety

- **Sysmac Studio (64 bit)**
  C:\Program Files\OMRON\Sysmac Studio\Sample\IEC 61131-10 XML\Safety

The procedure to import the IEC 61131-10 XML files is as follows.

1 Select **IEC 61131-10 XML** - **Import** from the **Tools** Menu.
The Import IEC 61131-10 XML Dialog Box is displayed.



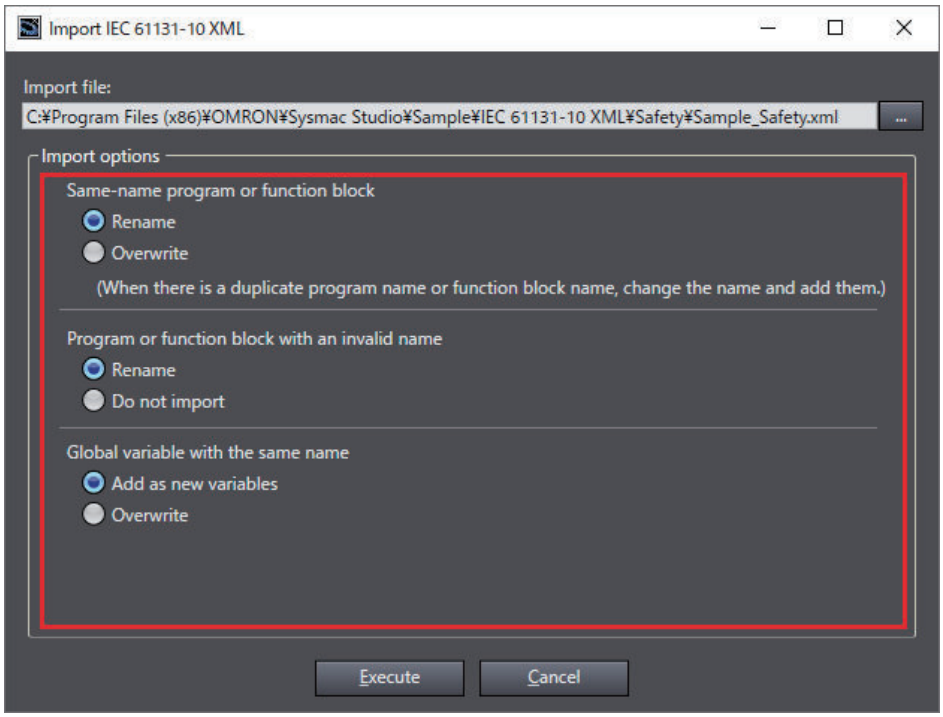
2 Click the **View File Selection Dialog Box** Button.



The Select File Dialog Box is displayed.

3 In the Select File Dialog Box, select the XML file to import, and then click the **Open** Button.
The screen returns to the Import IEC 61131-10 XML Dialog Box, in which the path to the file that you selected in the Select File Dialog Box is displayed as the import file.

4 Select the options before importing the file.



5 Click the **Execute** Button.
The data is imported and the global variables and POUs in the XML file are added to the project.
If the project already has any global variable or POU with the same name, data is imported as you configured in the import options. You can check the imported data on the Output Tab Page.

Precautions for Correct Use

The data integrity of the XML file is not checked by CRC when it is imported.
Always validate the correct logic under your responsibility after the import and assure proper execution before you use it for actual operation.

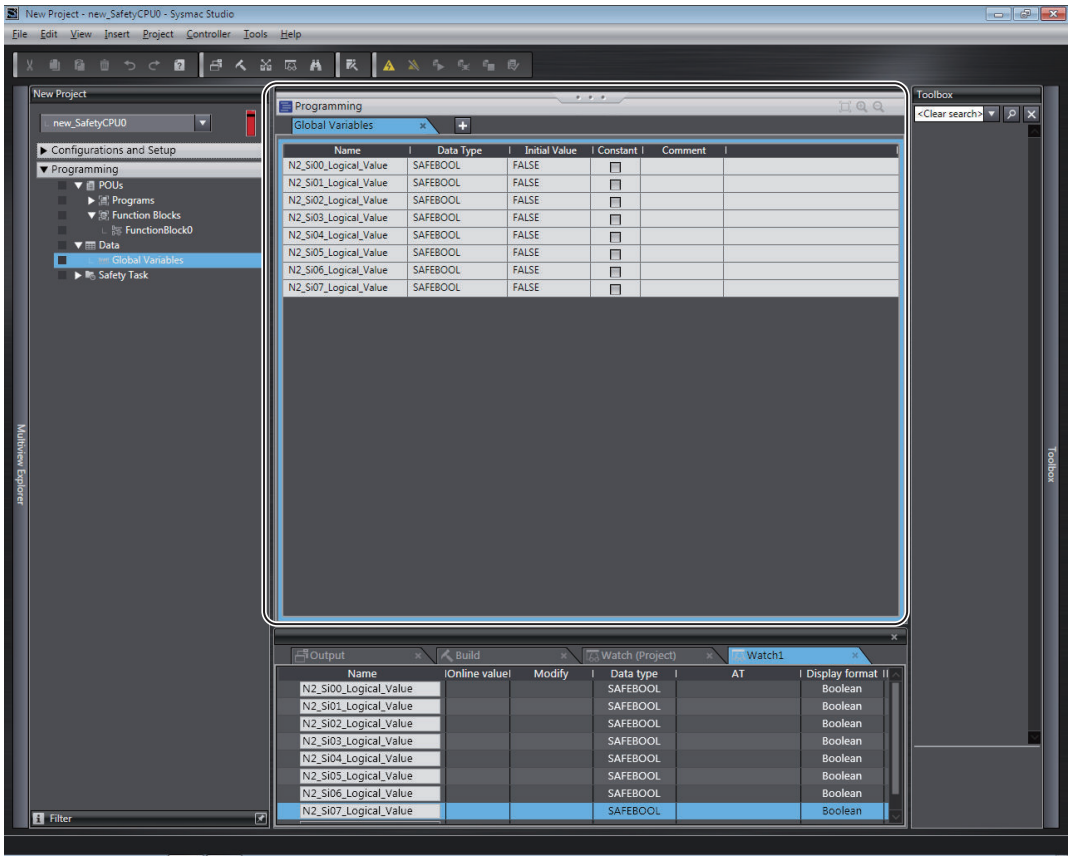
8-5-3 Registering Variables

This section describes how to register global variables and local variables.

Registering Global Variables

● Opening the Global Variable Table

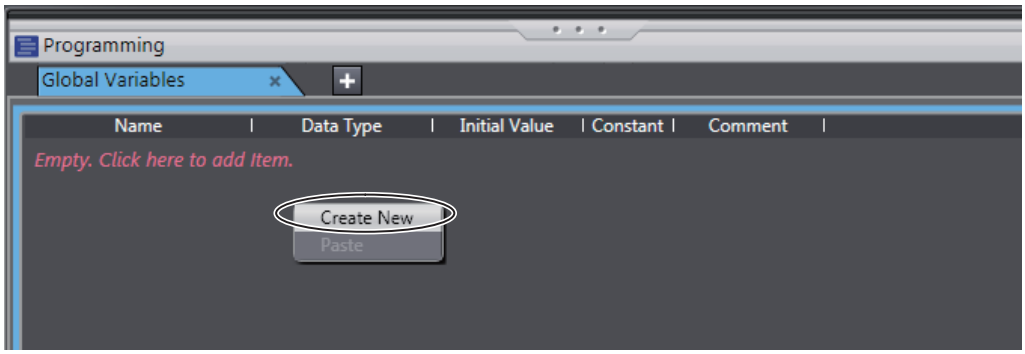
Double-click **Global Variables** under **Programming** - **Data** in the Multiview Explorer. Or, right-click **Global Variables** under **Programming** - **Data** and select **Edit** from the menu.
The global variable table is displayed.



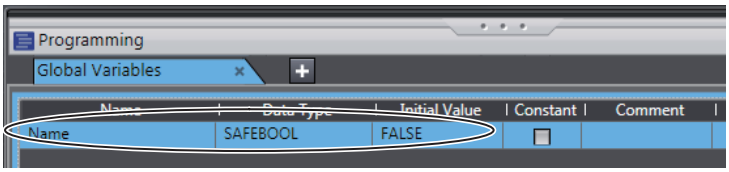
Field	Description	Restrictions
Name	Enter a name to use to identify the variable.	Only single-byte alphanumeric characters are allowed. Multi-byte characters, such as those used for Japanese, are not allowed. The maximum size is 127 bytes.
Data Type	Set the type of data that is stored in the variable. Refer to *8-2-5 Data Type* on page 8-14 for the data types that you can use.	---
Initial Value	Set the value to use when the power is turned ON, when the mode changes to RUN mode, or DEBUG mode (STOPPED). This parameter must be specified.	---
Constant	Select the check box in the Constant column to set the initial value of the variable when it is downloaded, but prevent it from being changed afterward. Select the check box or clear the selection (default).	---
Comment	Set any comments for the variable.	The maximum size is 127 bytes.

● Registering New Global Variables

1 Press the **Insert** Key in the global variable table, or right-click in the global variable table and select **Create New** from the menu.



2 Enter values for each item, and then press the **Enter** Key.



The variable is registered. Always set the variable name and the data type.

Additional Information

If there are no registered variables at all, the message *Empty. Click here to add Item* is displayed. Click to add a new variable.

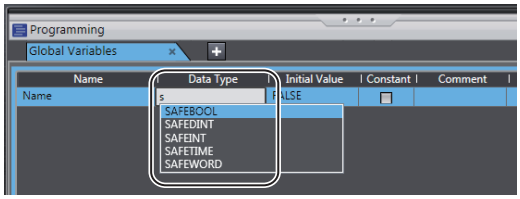
● Automatically Registering Global Variables

When you register device variables or exposed variables, any of the variables that are not already registered as global variables are automatically registered as global variables.

Refer to *7-7-1 Registering Device Variables* on page 7-46 for details on registering device variables.
Refer to *7-8 Exposing Variables to Standard Controllers* on page 7-53 for details on registering exposed variables.

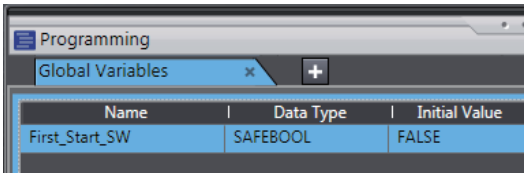
● Editing Global Variables

1 Click the cell to edit for the registered variable.



You can use the autocompletion to enter a data type in the Data Type cells. When you enter the first letter (example: S), a list of data types that begin with the letter is displayed. Select a data type from the list.

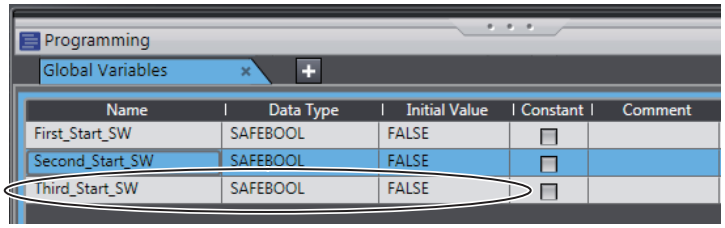
2 Change the value or the settings, and then press the **Enter** key.
The change is applied to the variable.



- Entry candidates you can select are displayed as follows:
  Entry candidates are displayed in the Name, Data Type, and Initial Value cells.
  Entry candidates that match the characters in the entered text string are displayed as you edit the text string.
- Entry candidates you can select by drag and drop are displayed as follows:
  You can move the position at which the selected variable is defined. You cannot select multiple variables.
  If you select multiple variables, the variable at the very bottom row will be the target of the drag and drop operation.

● Deleting Global Variables

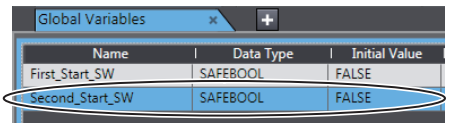
1 Click any cell on the line of the variable to delete to select the entire line.



2 Press the **Delete** Key. Or, right-click a row and select **Delete** from the menu.
The variable is deleted.

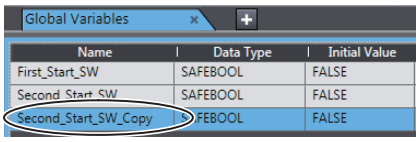
● Copying and Pasting Global Variables

1 Click any cell on the line of the variable to copy.



2 Press the **Ctrl** + **C** Keys. Or, right-click the row and select **Copy** from the menu.
The specified variable is copied.

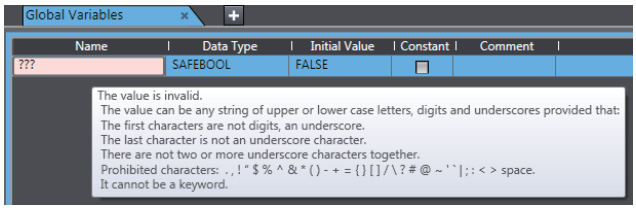
3 Press the **Ctrl** + **V** Keys. Or, right-click and select **Paste** from the menu.
A copy of the variable is registered with *_Copy* added to the name of the variable that was copied on the next row.



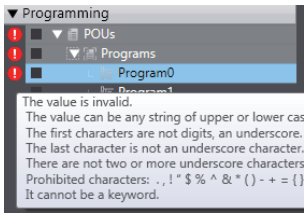
Precautions for Correct Use

If you enter any invalid characters or out of range values, the cell is highlighted in pink. An error will occur when the program is built. A red icon "!" is displayed in the Multiview Explorer.
The error message is displayed when the mouse cursor is moved over the cell where the error exists or over the exclamation icon.
Refer to *8-2-8 Restrictions on Variable Names and Other Safety Program-related Names* on page 8-17 for details on the restrictions on variable names.

- Variable Table



- POUs (when the mouse cursor is moved over a POU, including the local variable where the error exists)



Additional Information

- The global variable comments are linked to the device variable comments in the I/O Map and the I/O terminal comments on the Parameters Tab Page for the Safety Slave Unit.
- If the same variable names exist when variables are copied and pasted from other variable tables or spreadsheets, a dialog box that lists the source and destination variables is displayed. Select the variable to overwrite and execute the paste.

Registering Local Variables

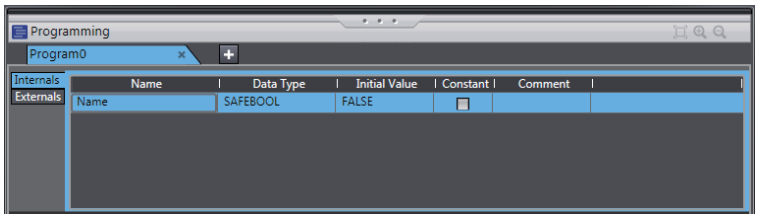
Registration of local variables refers to the registration of variables that can be used only inside POUs (programs and function blocks). Local variables include internal variables, input variables, output variables, and external variables.

● Registering and Editing Local Variables

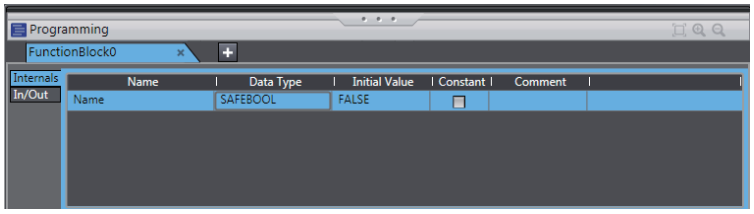
1 Double-click a program under **Programming** - **POUs** - **Programs** in the Multiview Explorer. Or, right-click the program and select **Edit** from the menu.

The local variable table for the program or the local variable table for the function block is displayed in the Edit Pane.

- The local variable table for programs is shown below.



- The local variable table for function blocks is shown below.



Field	Description	Restrictions
Name	Enter a name to use to identify the variable.	Only single-byte alphanumeric characters are allowed. Multi-byte characters, such as those used for Japanese, are not allowed. The maximum size is 127 bytes.
Data Type	Set the type of data that is stored in the variable. Refer to *8-2-5 Data Type* on page 8-14 for the data types that you can use.	---
Initial Value	Set the value to use when the power is turned ON, when the mode changes to RUN mode, or DEBUG mode (STOPPED). This parameter must be specified.	---
Constant	Select the check box in the Constant column to set the initial value of the variable when it is downloaded, but prevent it from being changed afterward. Select the check box or clear the selection (default).	---
Comment	Set any comments for the variable.	The maximum size is 127 bytes.

Note The items that can be set and viewed depend on the type of the local variable. Refer to *8-2-4 Attributes of Variables* on page 8-13 for details.

2 Select the tab for internal variables, in-out variables (function blocks only), or external variables, and then register and edit the local variables.
You can also register them directly in the FBD editor.

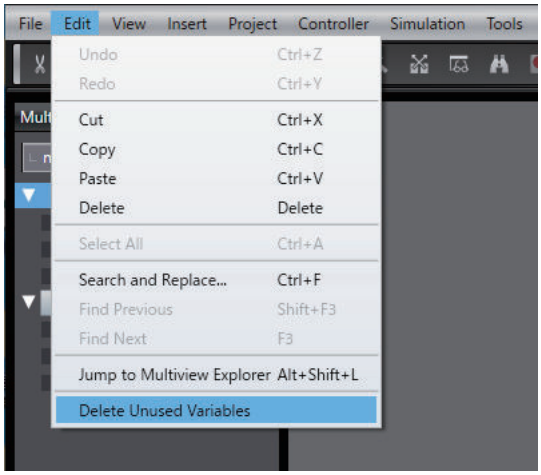
Additional Information

The operating procedures for local variables are the same as the procedures used for global variables.
Refer to *8-5-3 Registering Variables* on page 8-38.

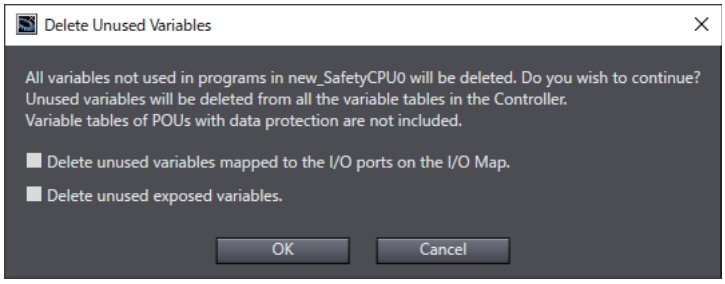
Deleting Unused Variables

You can delete unused variables in the Safety CPU Unit programs all at once.

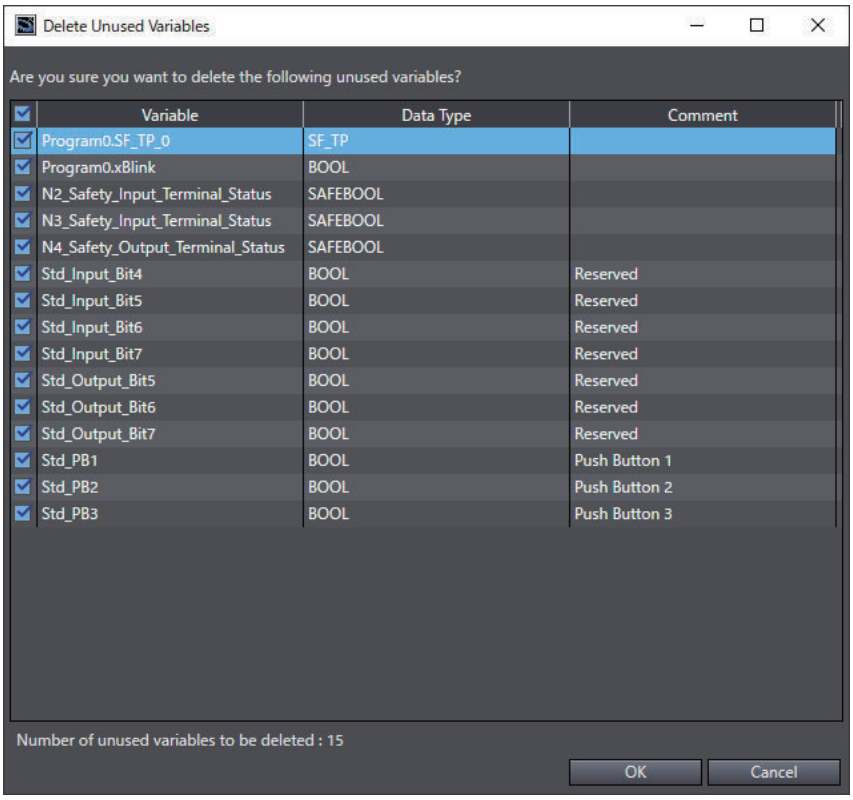
1 Select **Delete Unused Variables** from the **Edit** menu.



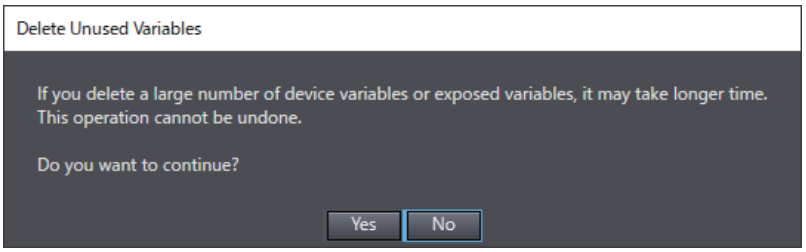
The confirmation message is displayed.



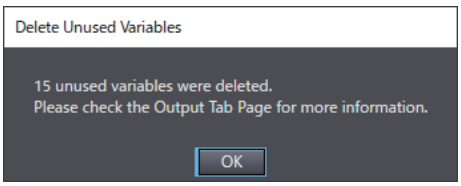
2 To include unused variables mapped to the I/O ports on the I/O Map and/or unused exposed variables to the deletion target, select the corresponding checkbox(es) and click the **OK** Button.
A list of unused variables is displayed.



3 Select the checkbox(es) of the variable(s) to delete and click the **OK** Button.
The following confirmation dialog is displayed.



4 Check the contents and click the **Yes** Button.
The unused variables are deleted. The window displays the number of deleted entries.



Precautions for Correct Use

- This deletion does not work for variables with data protection enabled and the I/O variables of function blocks.
- The deletion also does not work for the exposed variables with the device variables assigned by the standard controllers.

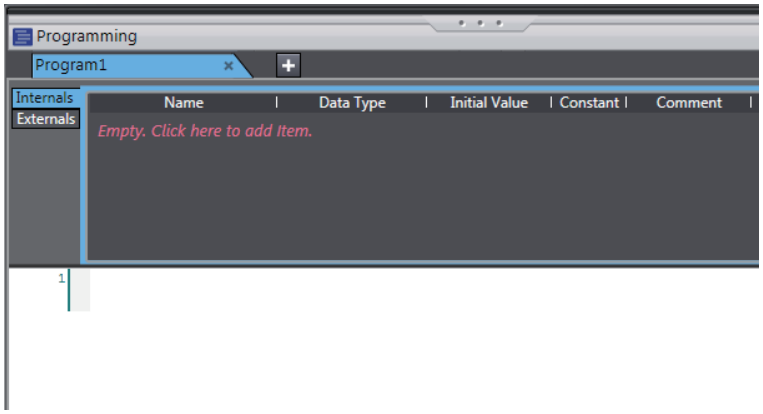
8-5-4 FBD Programming

With the Safety CPU Unit, you use the FBD language to express algorithms that are inside the POUs (programs and function blocks). You add and connect functions and function blocks in the FBD editor to build algorithms inside POUs (programs and function blocks).
This section describes how to use the FBD editor.

Opening and Using the FBD Editor

● Programs

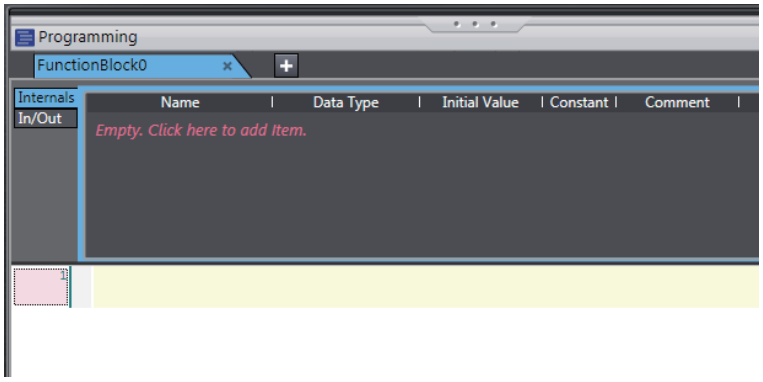
1 Double-click a program under **Programming** - **POUs** - **Programs** in the Multiview Explorer. Or, right-click the program and select **Edit** from the menu.
The FBD editor for the program is displayed.



Refer to *8-5-2 Registering POUs* on page 8-28 for the program registration procedure.

● Function Blocks

1 Double-click a registered function block under **Programming** − **POUs** − **Function Blocks** in the Multiview Explorer. Or, right-click the function block and select **Edit** from the menu.
The FBD editor for the function block is displayed.



Refer to *8-5-2 Registering POUs* on page 8-28 for the function block registration procedure.

Zooming In and Zooming Out of the FBD Editor

Use the icons that are displayed in the toolbar to zoom in or zoom out of the FBD editor.



Inserting FBD Networks

There are three ways to insert an FBD network.

● Method 1

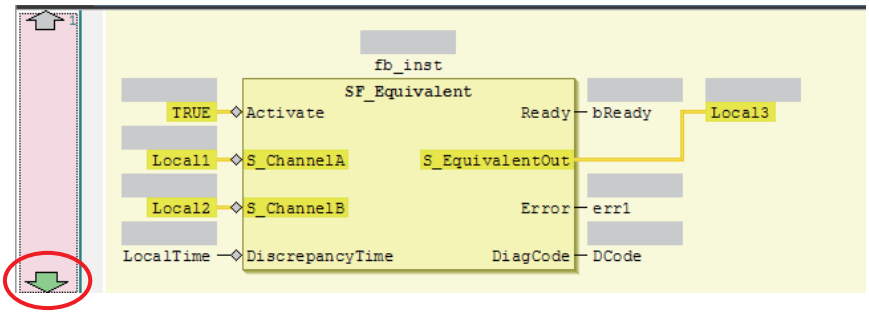
Right-click the FBD network and select **Insert Network Above** from the menu.
An empty FBD network is inserted before the selected FBD network.

● Method 2

Right-click the FBD network and select **Insert Network Below** from the menu.
An empty FBD network is inserted after the selected FBD network.

● Method 3

Drag a **Network** from **General** in the Toolbox to the FBD editor.
An empty network is inserted at one of the positions given in the following table, and the focus moves to the inserted network.



Drop point	Position where network is added
Upward arrow on the network number	An empty network is inserted before the FBD network where the network was dropped.
Downward arrow on the network number	An empty network is inserted after the FBD network where the network was dropped.

Deleting FBD Networks

There are two methods to delete an FBD network.

● Method 1

Right-click the FBD network and select **Delete** from the menu.
The selected FBD network is deleted and the focus moves to the next network.

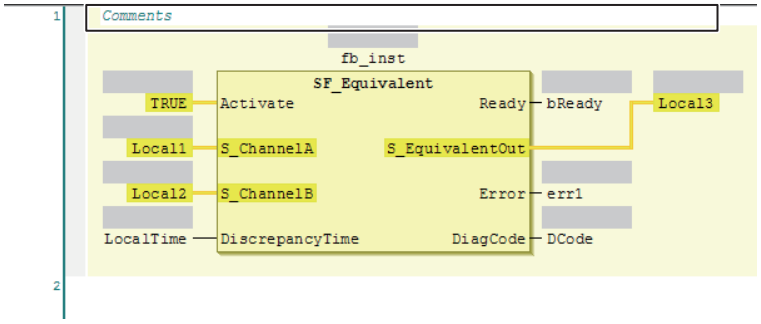
● Method 2

Select the FBD network and press the **Delete** Key.
The selected FBD network is deleted and the focus moves to the next network.

Editing Comments for FBD Networks

Use the following procedure to edit the comment for an FBD network.

- Select the comment portion of the FBD network and edit it.



Commenting Out FBD Networks and Restoring Them

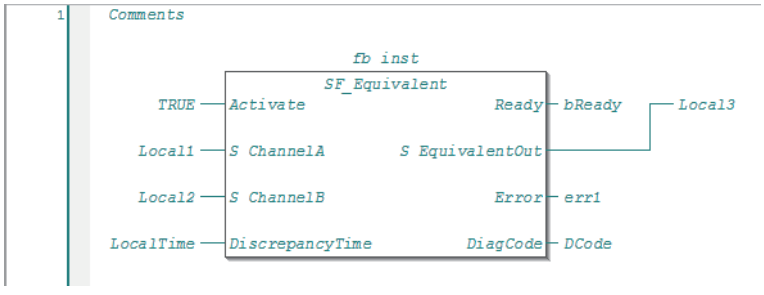
The following operation allows you to comment out an FBD network and then restore it. When a network is commented out, it is no longer executed.

Right-click the FBD network and select **Toggle Network Comment State** from the menu.

Precautions for Correct Use

You cannot select more than one network. If you select more than one network, the comment status of last network that you select will change.

Networks that are commented out are displayed in blue italic letters as shown below.



If you select a commented network, the network is changed to an uncommented network.

Inserting a FUN or FB

There are following two ways to insert a FUN or FB.

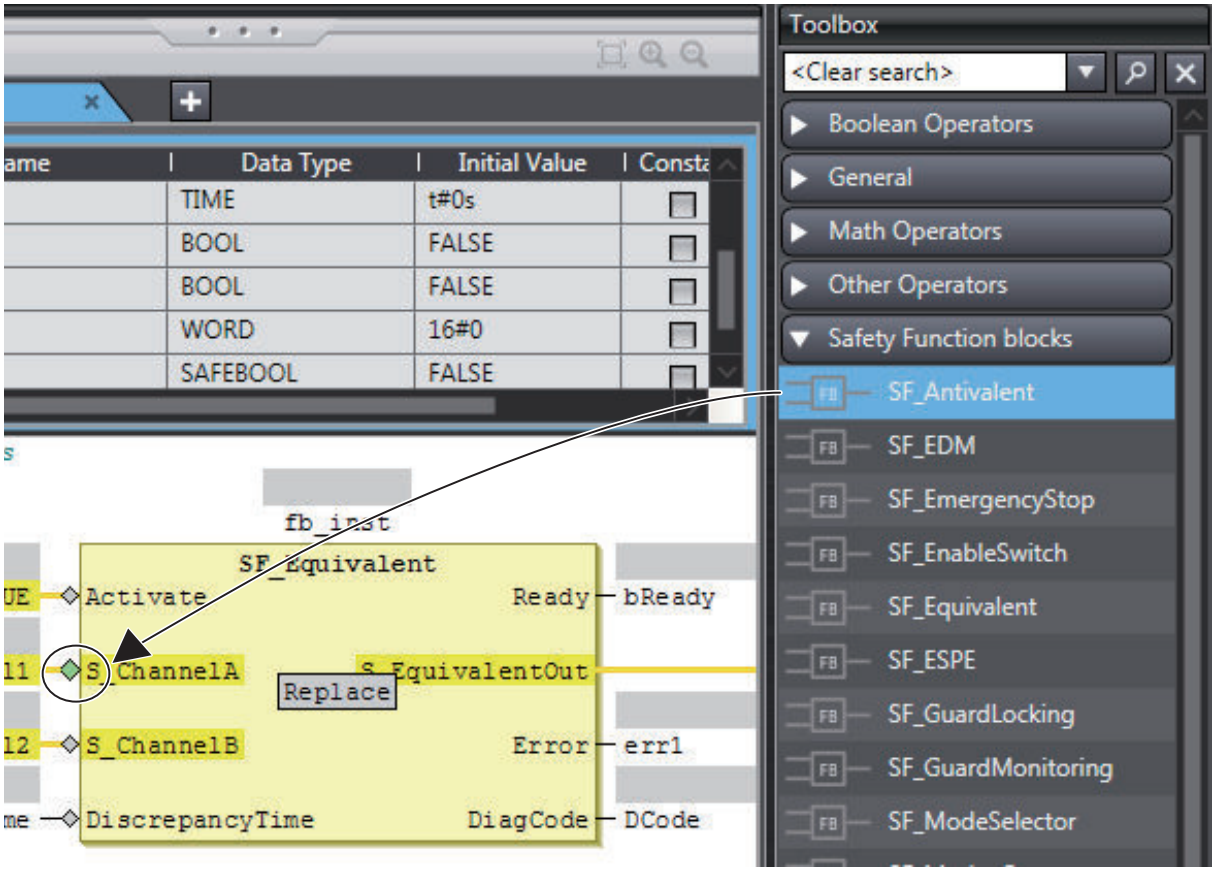
Method	Operation
Method 1	Drag a FUN or FB from the Toolbox to an I/O terminal on the FUN or FB in the FBD editor, or to a new network where the words **Start Here** are displayed.
Method 2	Right-click the FBD network, select **Insert Function Block** from the menu, and specify FUN or FB.

Precautions for Correct Use

Not all of the FUNs and FBs that you can use are displayed in the Toolbox. To use a FUN or FB that is not shown in the Toolbox, use Method 2.

● Procedure for Method 1

1 Drag a FB or FUN from the Toolbox to an I/O terminal on the FUN or FB in the FBD editor, or to a new network where the words **Start Here** are displayed. Positions where you can drop the function block are indicated with gray rectangular or diamond-shape boxes. These boxes change to green when you move the cursor over them.

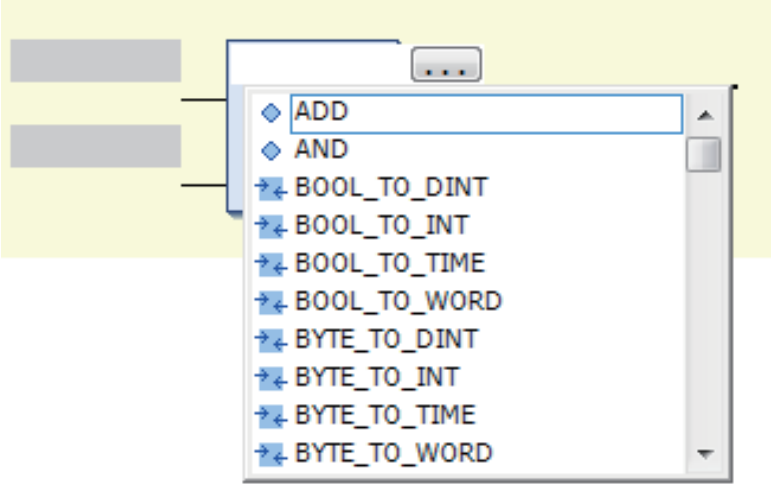


2 Drop the FUN or FB on a green diamond-shape box to insert it.

● Procedure for Method 2

1 Right-click the FBD network and select **Insert Function Block** from the menu.
An empty FB is inserted.

2 Click in the FB name text box and press the **Ctrl** + **Space** Keys to display a list of the FUNs and FBs that you can enter.



3 Select a FUN or FB from the list.

Additional Information

You can click the Input Assistance Button (...) to the right of the FB name text box to display the **Input Assistant** Dialog Box. You can select an FB from the **Items** in this dialog box to insert the selected FB.

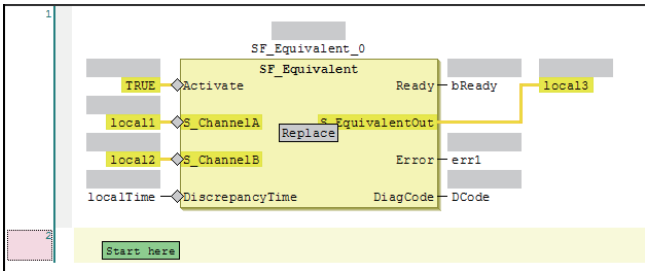
Area	Description
Categories	Displays the FB categories. The FBs that belong to the selected category are displayed in the **Items** Area.
Items	Displays a list of FBs.
Documentation	Any additional information that is available for the FB that you select in the **Items** Area is displayed.

The **Input Assistant** Dialog Box is also displayed when you right-click an FBD network and select **Insert Function Block** from the menu.

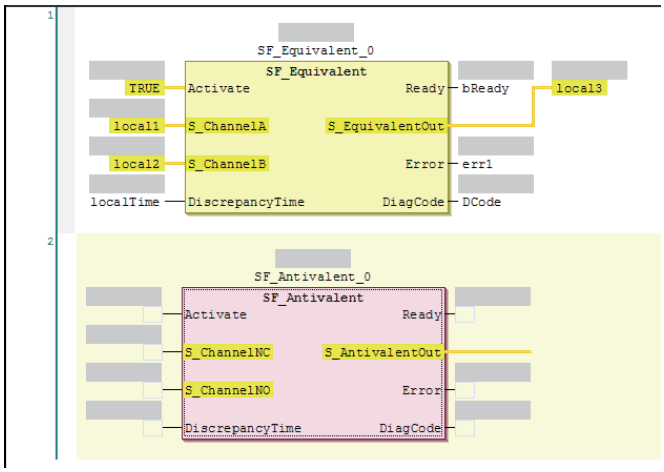
● Inserting Position of a FUN or FB

The position where the FUN or FB is inserted depends on the insertion method, as described below.

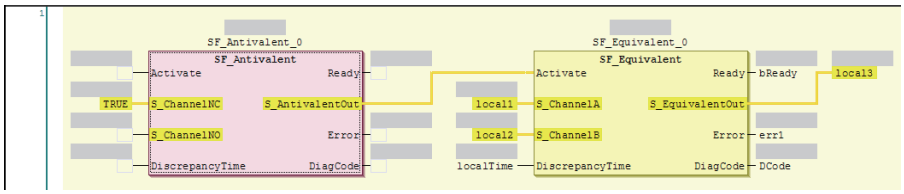
- If you drag a FB or FUN (SF_Antivalent in the example) from the Toolbox, the FB or FUN is inserted at the position shown below.



If you drop the SF_Antivalent FB on the network where the words **Start here** are displayed, the FB is inserted in the new network.

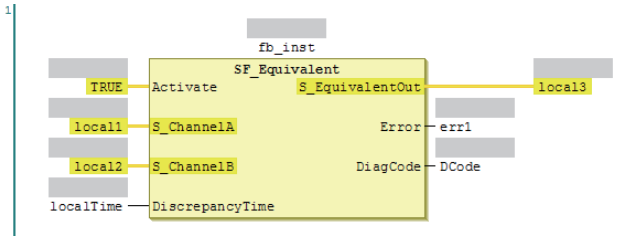


If you drop the SF_Antivalent FB on an input terminal, the FB is inserted before the input terminal.

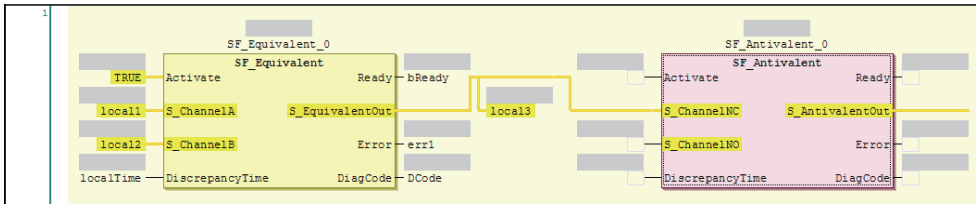


- If you select a FB or FUN (in this example, SF_Antivalent) from the right-click menu, the FUN or FB is inserted at the location shown below.

  a) Before the FB is inserted, the network is as shown below.



  b) When the SF_Antivalent is selected from the right-click menu, the network is as shown below.



Deleting a FUN or FB

Use one of the following procedures to delete a FUN or FB.

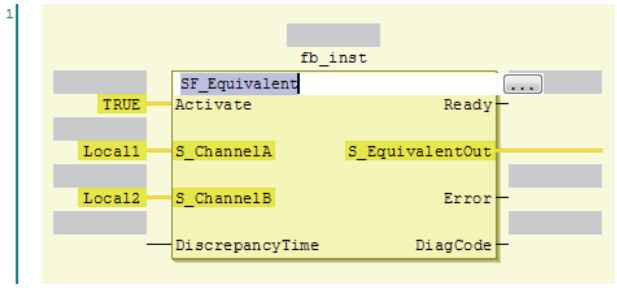
Method	Operation
Method 1	Right-click the FUN or FB on the FBD network and select **Delete** from the menu.
Method 2	Select the FUN or FB on the FBD network and press the **Delete** Key.

Replacing a FB or FUN

You can replace a FUN or FB with a different instruction without changing the input and output parameters. Use one of the following procedures.

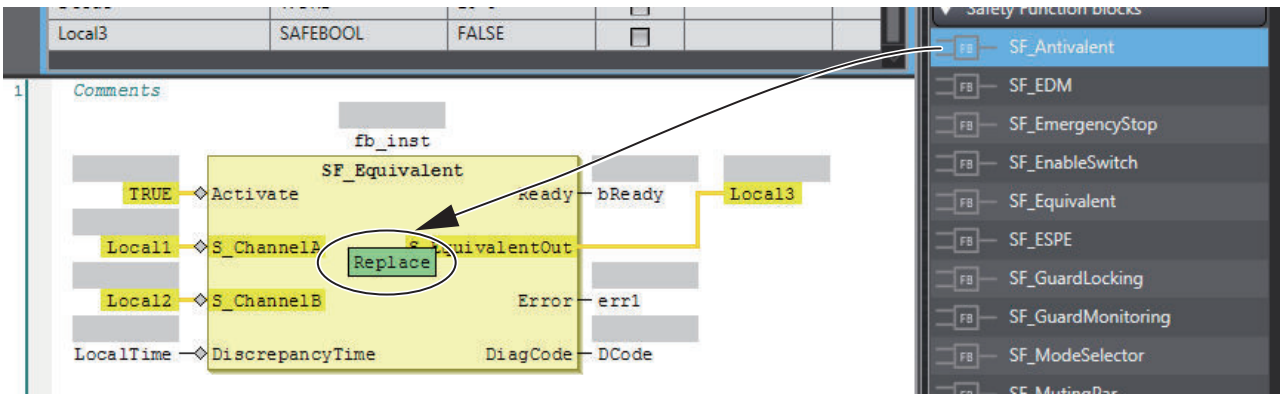
Method	Operation
Method 1	Drag the FUN or FB to change to in the Toolbox to the FUN or FB in the FBD editor.
Method 2	Select the FUN or FB name on the FBD network and directly enter the FUN or FB name.

- Before the FB is edited, the network is as shown below.



● Procedure for Method 1

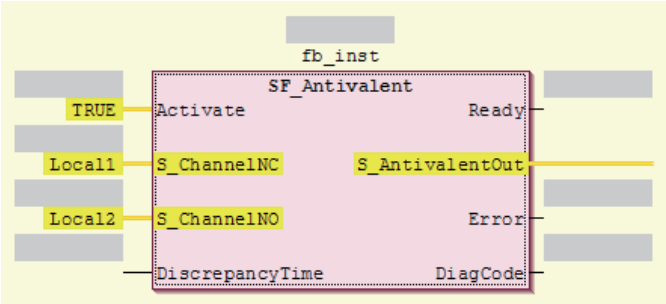
1 Drag a FUN or FB from the Toolbox to the FB to replace. A **Replace** area is displayed.



2 Drop the FUN or FB in the **Replace** area to replace the FUN or FB.

● Procedure for Method 2

If you directly enter the FB or FUN name, the FB or FUN is replaced when you press the **Enter** Key.

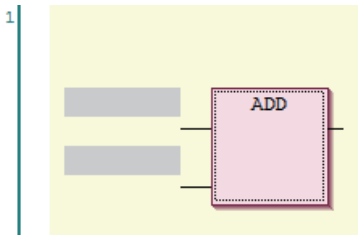


Adding Input Parameters to AND, OR, ADD, MUL, and MUX

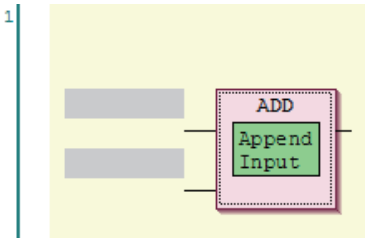
You can add input parameters to the AND, OR, ADD, MUL, and MUX instructions. Use one of the following procedures.

Method	Operation
Method 1	Drag **Input** from **General** in the Toolbox to the **Append Input** area in the instruction in the FBD editor.
Method 2	Right-click the FB on the FBD network and select **Add Input** from the menu.

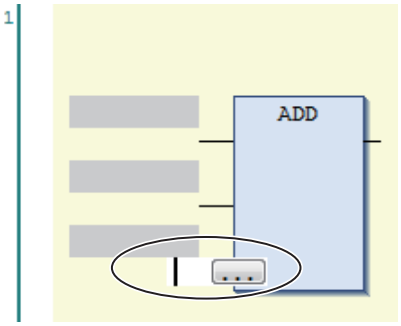
- Before the input parameter is added, the network is as shown below.



- When you drag an **Input Variable** from the toll box, the network is as shown below.



- After the input parameter is added, the network is as shown below.



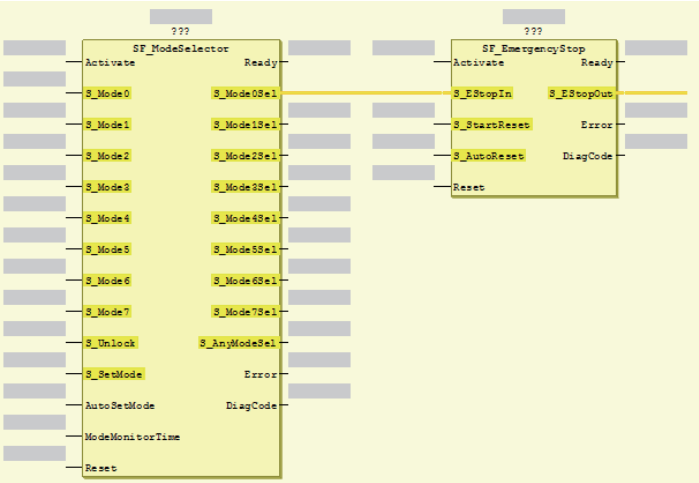
Changing the Output Terminals of a FUN or FB

Use the following procedure to change the output terminals of a FUN or FB.

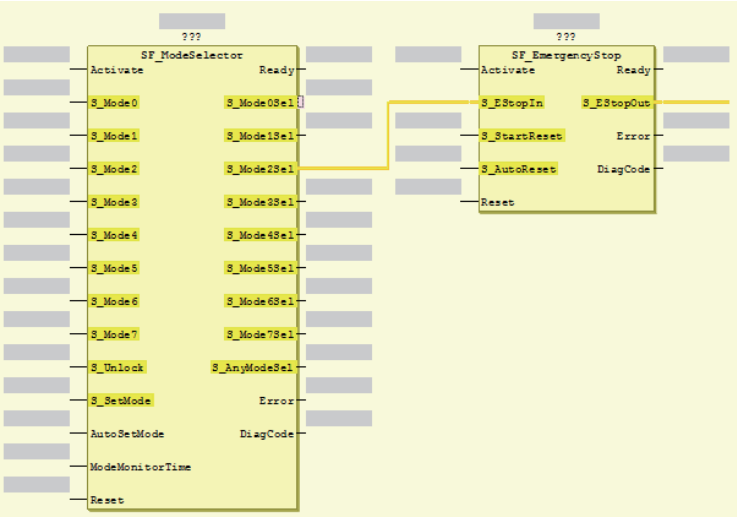
Right-click an output terminal on a FUN or FB on the FBD network and select **Set Output Connection** from the menu.

The selected output terminal is connected to the input terminal of the next FUN or FB.

- Before the output terminal is changed, the network is as shown below.



- When **S_Mode2Sel** is selected and **Set Output Connection** is executed, the network is as shown below.



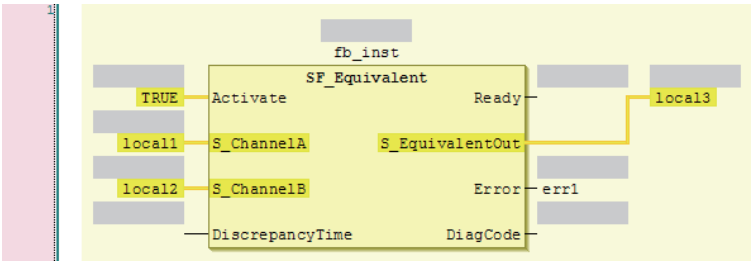
Deleting Unused Parameters from a FUN or FB

Use the following procedure to delete any unused parameters from a FUN or FB.

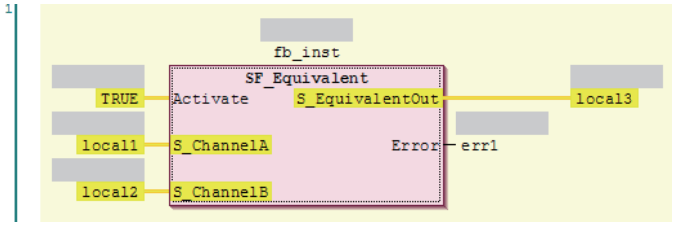
Right-click the FB or FUN on the FBD network and select **Remove unused FB call parameters** from the menu.

All of the unused parameters are deleted.

- Before the unused parameters of the FUN or FB are deleted, the network is as shown below.



- After the unused parameters of the FUN or FB are deleted, the network is as shown below.



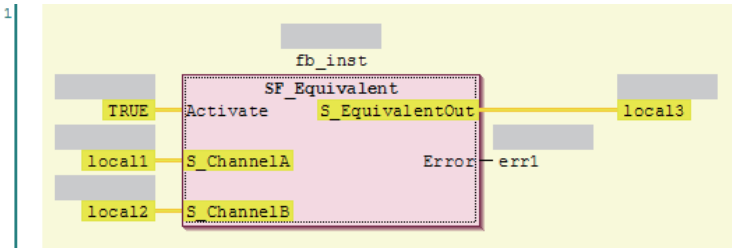
Updating the Input Parameters and Output Parameters of a FUN or FB

Use the following procedure to display the input parameters and output parameters of a FUN or FB.

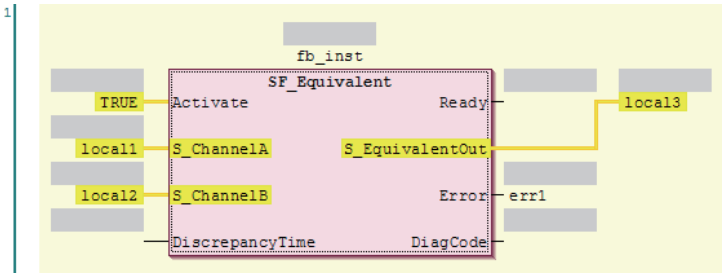
Right-click a FUN or FB on the FBD network and select **Update** from the menu.

The input parameters and output parameters for the FUN or FB are displayed along with any unused parameters.

- Before the input parameters and output parameters of the FUN or FB are updated, the network is as shown below.



- After the input parameters and output parameters of the FUN or FB are updated, the network is as shown below.

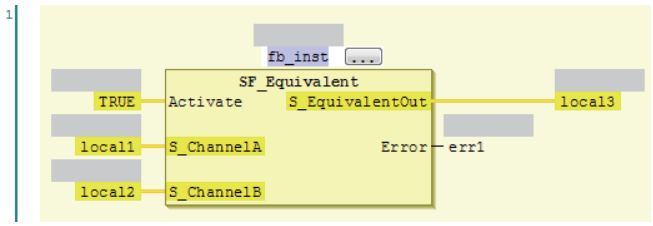


Editing Function Block Instance Variables

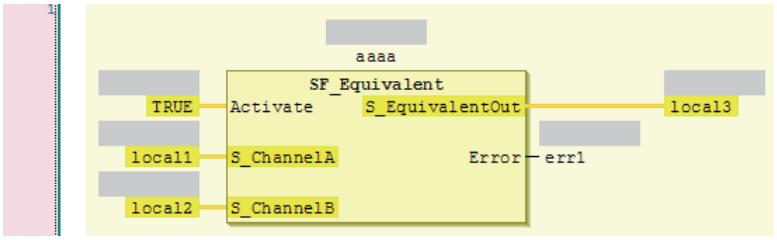
Use one of the following methods to edit existing function block instance variables.
If you specify a variable name that does not exist in the local variable table, that variable will be registered as a local variable.

Select an FB instance variable on the FBD network and directly enter the variable name.

- Before the function block instance variable is edited, the network is as shown below.



- After the function block instance variable is edited, the network is as shown below.



Additional Information

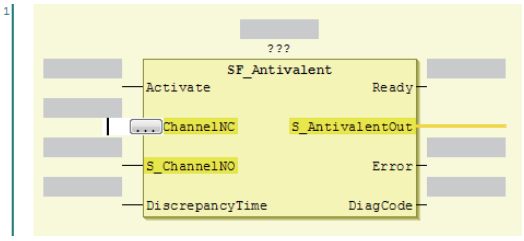
To create a new function block instance variable, enter the variable name and press the **Enter** key. The function block instance variable is registered as an instance of the FB, and it is also registered as a local variable in the local variable table.

Entering Parameters

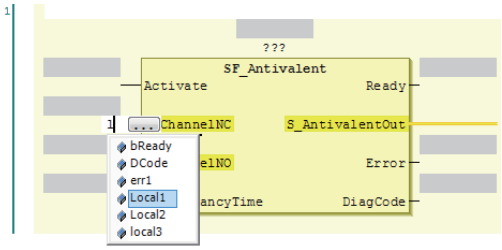
Use one of the following procedures to enter parameters.
If you specify a variable name that does not exist in the local variable table, that variable will be registered in the local variable table.

Select a parameter on the FBD network and directly enter the variable name.

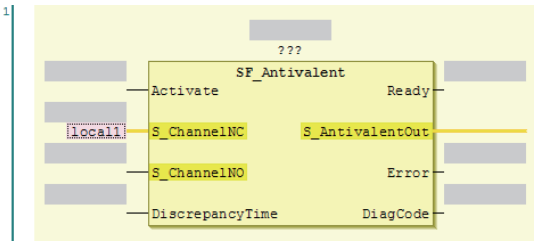
- Before the parameter is edited, the network is as shown below.



If you enter the variable name directly, a list of variable names that you can select from is displayed when you enter the first letter of the variable name. Use the **Up** and **Down** Keys to select the variable name from the list, and then press the **Enter** Key. The selected variable name is registered as an input parameter. If you press the **Ctrl** + **Space** Keys when nothing is displayed, list of variable name candidates is displayed.



- After the input parameter is edited, the network is as shown below.



To delete an input parameter assigned, select the parameter and press the **Delete** key.

Additional Information

- To create a new input variable, enter the variable name and press the **Enter** key. The input parameter is registered, and it is also registered as a local variable in the local variable table.
- You can click the Input Assistance Button (...) to the right of the text box to display the **Input Assistant** Dialog Box. You can select a variable from the **Items** in this dialog box to insert the selected variable.

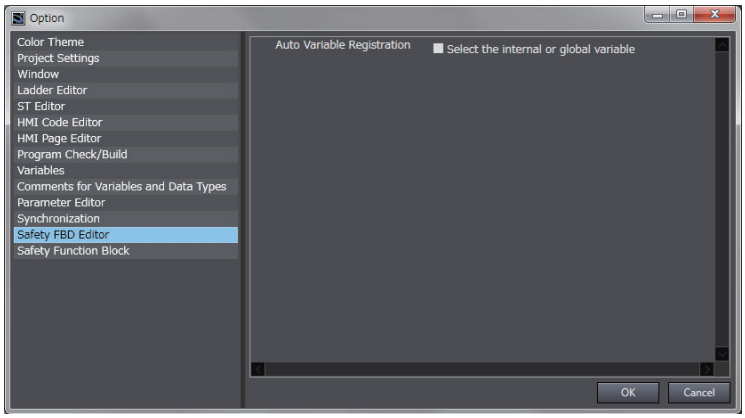
Area	Description
Categories	Displays the variable categories. The variables that belong to the selected category are displayed in the **Items** Area.
Items	Displays a list of variables.
Documentation	Any additional information that is available for the variable that is selected in the **Items** Area is displayed.

● Changing Variable Registration Locations

You can use the following option to enable the selection of the variable registration locations when you enter parameters.

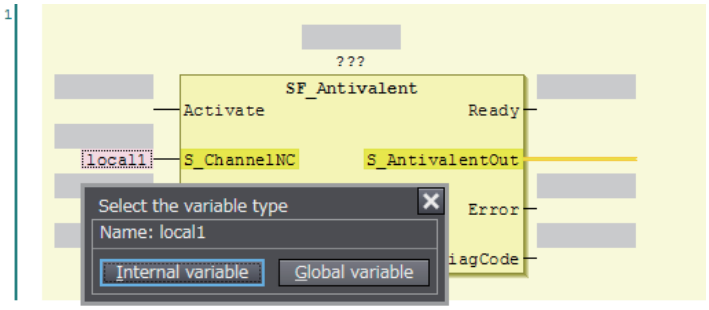
1 Select **Option** from the **Tools** Menu.
The **Option** Dialog Box is displayed.

2 Click **Safety FBD Editor**.
The Auto Variable Registration Option is displayed.



3 Select the **Select the internal or global variable** Check Box and click the **OK** Button.

If you select the above option, the following dialog box is displayed when a variable is registered automatically from the Safety FBD Editor.



If you click the **Internal variable** Button, the variable is registered as an internal variable in the local variable table.
If you click the **Global variable** Button, the variable is registered in the global variable table and as an external variable in the local variable table.

Assigning Output Parameters

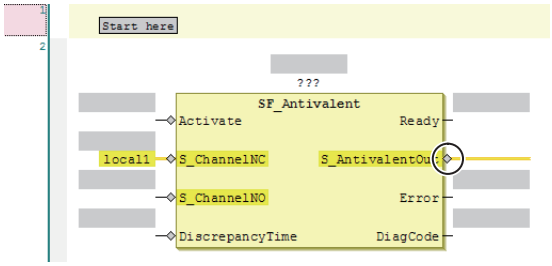
You can insert output variables at specified locations. Use one of the following procedures to assign an output parameter to an output variable of a FUN or FB.

Method	Operation
Method 1	Drag **Assignment** from **General** in the Toolbox to a terminal in the FBD editor, or to a new FBD network where the words **Start here** are displayed.
Method 2	Right-click the FBD network and select **Insert Assignment** from the menu.

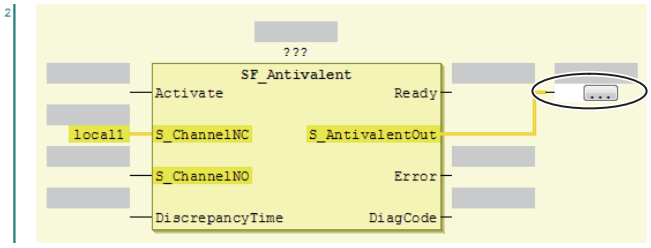
- If you select a network, the output variable is added to the last output area (before the output terminal or the output variable) on the network.
- If you drag **Assignment** from the Toolbox, the point of insertion depends on where you drop the output variable.

Drop point	Position where function block is added
“Start here” on the network	Input parameters and output parameters are added to the new network.
Input terminal	The output parameter is inserted on a branch that is created before the input terminal.
Output terminal	The output parameter is inserted after the output terminal.
Before the output parameter	The output parameter is inserted on a branch that is created before the output variable.

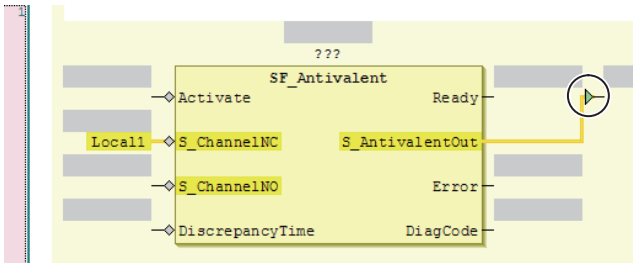
● Example 1 of a Dragged Output Parameter Object



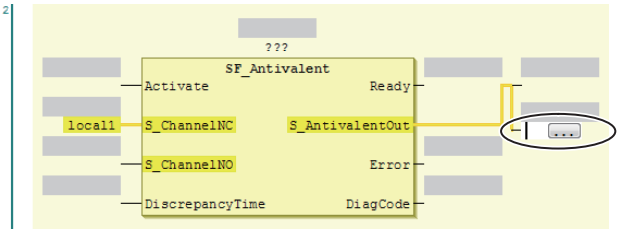
When an output parameter is added to the output terminal, the network is as shown below.



● Example 2 of a Dragged Output Parameter Object



When an output parameter is added before another output parameter, the network is as shown below.



The output parameter is inserted on a branch that is created before the output variable.

Deleting Output Parameters

Use the following procedure to delete output parameters.

Right-click the Output parameters on the FBD network and select **Delete** from the menu.

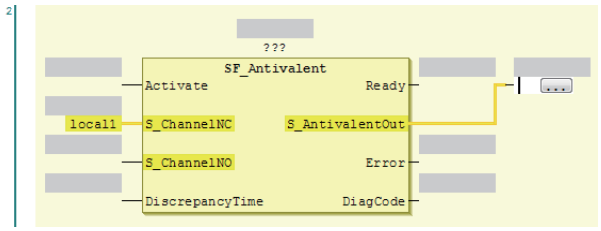
The selected output parameter is deleted. You cannot select multiple variables.

Editing Output Parameters

Use one of the following procedures to edit output parameters.
If you specify a variable name that does not exist in the local variable table, that variable will be registered as a local variable.

Select the output variable on the FBD network and directly enter the variable name.

Before the output variable is edited, the network is as shown below.



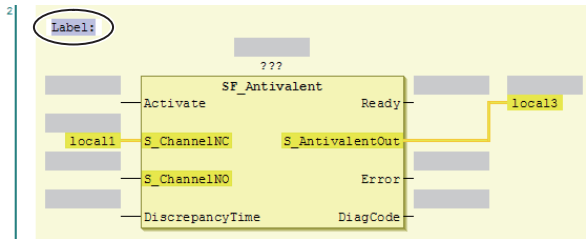
- If you prefer to enter the variable name directly, a list of variable names that you can select from is displayed when you begin entering the variable name.
- To create a new output variable, enter the variable name and press the **Enter** Key. The output variable is registered, and it is also registered as a local variable in the local variable table.

Inserting Jump Labels

Use the following procedure to insert jump labels into an FBD network.

Right-click the FBD network and select **Insert Jump Label** from the menu.

After the jump label is added, the network is as shown below.



You cannot add another jump label to a network if it already has one.

Deleting Jump Labels

Use one of the following procedure to delete jump labels.

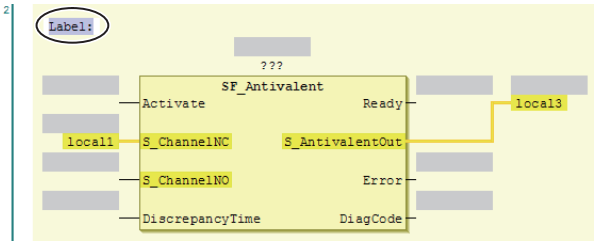
Method	Operation
Method 1	Right-click the Jump label and select **Delete** from the menu.
Method 2	Select the Jump label and press the **Delete** Key.

Editing Jump Labels

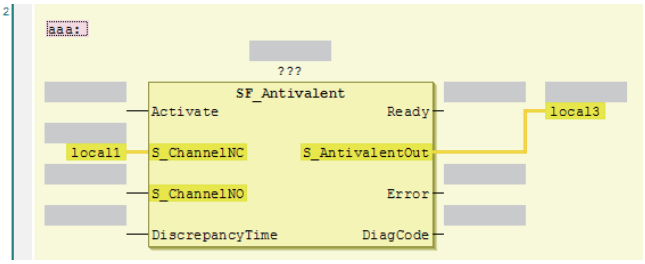
Use the following procedure to edit jump labels.

Select a jump label on the network and edit it.

- The jump label becomes editable when you click it. After you finish editing, press the **Enter** key.
  a) After the jump label is selected, the network is as shown below.



  b) After the jump label is edited, the network is as shown below.



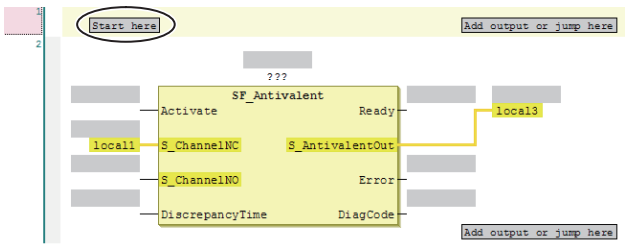
Inserting Jump Instructions

Use one of the following procedures to insert a Jump instruction in a network.

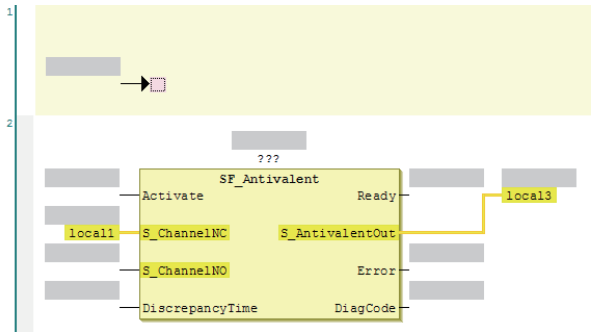
Method	Operation
Method 1	Drag **Jump** from **General** in the Toolbox to the words **Start here** on a new network.
Method 2	Right-click the FBD network and select **Insert Jump** from the menu.

The Jump instruction is inserted in the network.

- Before the Jump instruction is dropped, the network is as shown below.



- After the Jump instruction is inserted, the network is as shown below.



Deleting Jump Instructions

Use one of the following procedures to delete a Jump instruction.

Method	Operation
Method 1	Right-click the Jump Instruction select **Delete** from the menu.
Method 2	Select the Jump Instruction and press the **Delete** Key.

The selected Jump instruction is deleted.

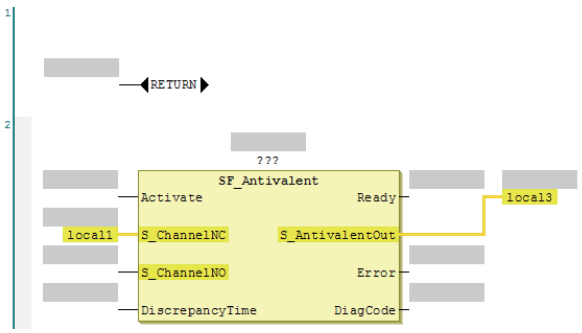
Inserting Return Instructions

Use one of the following procedures to insert a Return instruction in a network.

Method	Operation
Method 1	Drag **Return** from **General** in the Toolbox to a terminal in the FBD editor, or to a new FBD network where the words **Start here** are displayed.
Method 2	Right-click the FBD network and select **Insert Return** from the menu.

The Return instruction is inserted in the network.

- After you insert a return instruction, the network is laid out as shown below.



Deleting Return Instructions

Use one of the following procedures to delete a Return instruction.

Method	Operation
Method 1	Right-click the Return instruction and select **Delete** from the menu.

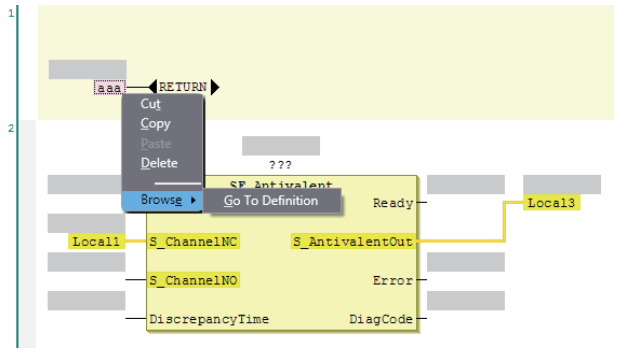
Method	Operation
Method 2	Select the Return instruction and press the **Delete** Key.

The selected Return instruction is deleted.

Viewing the Locations of Variable Definitions

You can view where variables are defined.
Use the following procedure.

Right-click the variable and click **Browse** − **Go To Definition** from the menu.

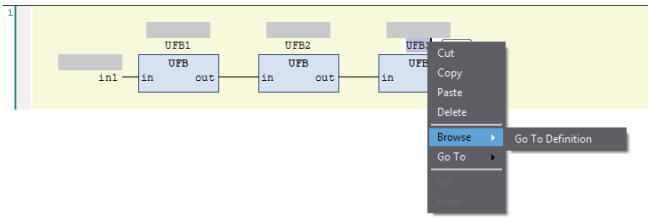


The focus moves to the location where the variable is defined (local variable).

Viewing the Locations of User-defined Function Block Definitions

You can view where user-defined function blocks are defined.
Use the following procedure.

Right-click the user-defined function block and click **Browse** − **Go To Definition** from the menu.

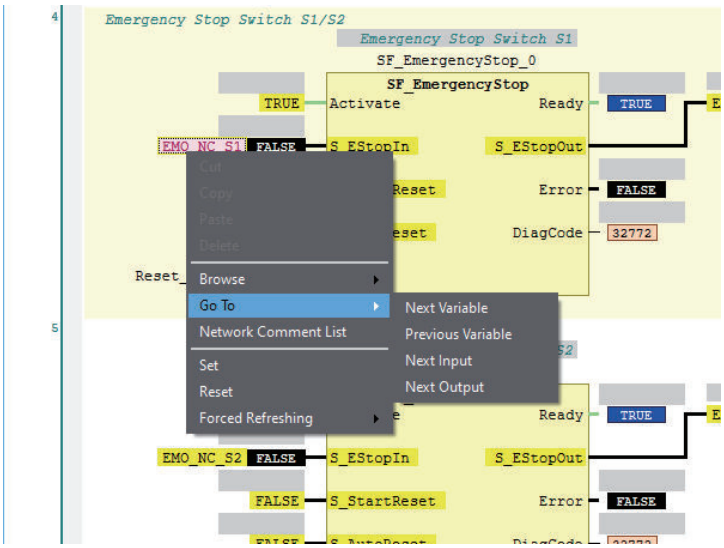


The focus moves to the location where the user-defined function block is defined.

Jumping to Variables in POUs

You can search sequentially for a variable used in the POUs (programs and function blocks) and then sequentially jump to the locations where the variable is used.
Use the following procedure.

Right-click a variable in the POU and select the destination to jump to from the menu.



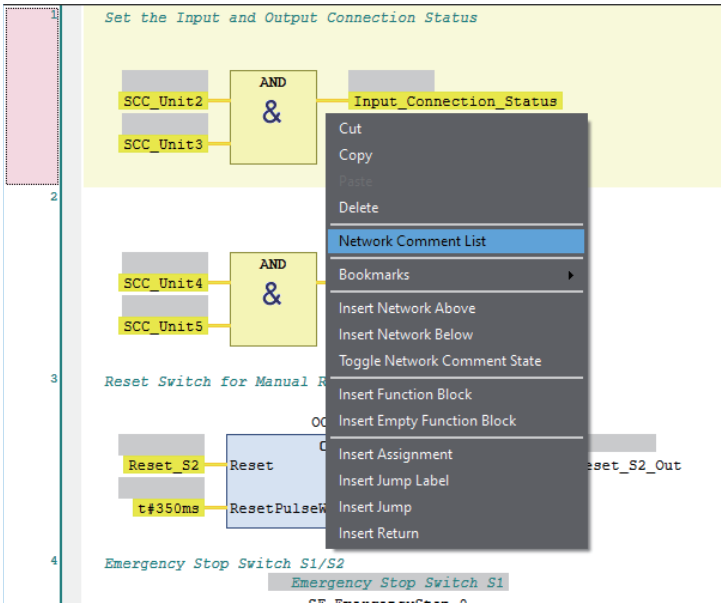
Menu command	Description
Next Variable	The display will jump to the next location where the selected variable is used.
Previous Variable	The display will jump to the previous location where the selected variable is used.
Next Input	The display will jump to the next location where the selected variable is used as a program input.
Next Output	The display will jump to the next location where the selected variable is used as a program output.
(Retrace Search*1)	If the selected variable is used as an output in the program, the search will start from the beginning of the program to look for a location where the selected variable is used as an input, and the display will jump to the location. If the selected variable is used as an input in the program, the display will jump to the location where the selected variable is used as a program output.

*1. This item is not displayed on the menu. Use the shortcut key **Space**.

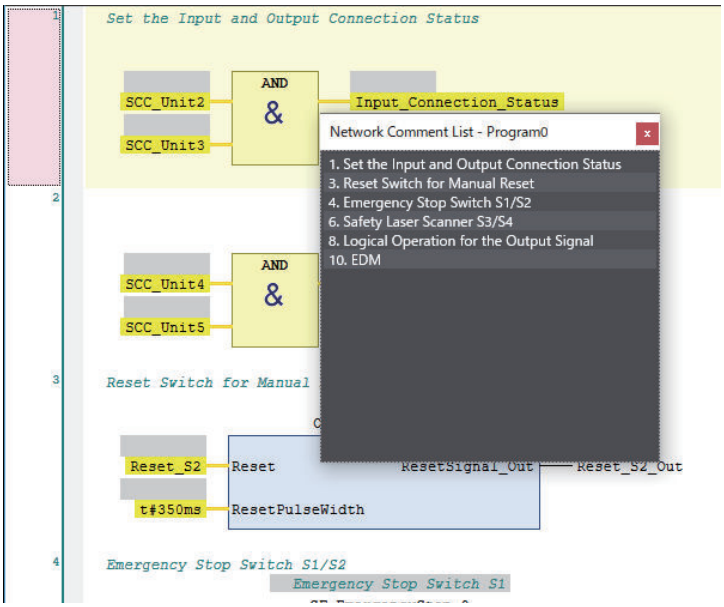
Displaying Network Comment List

You can display the list of network comments that are set in the POU (programs and function blocks), and then jump to a specific network comment.
You can use the following two methods to display the network comment list.

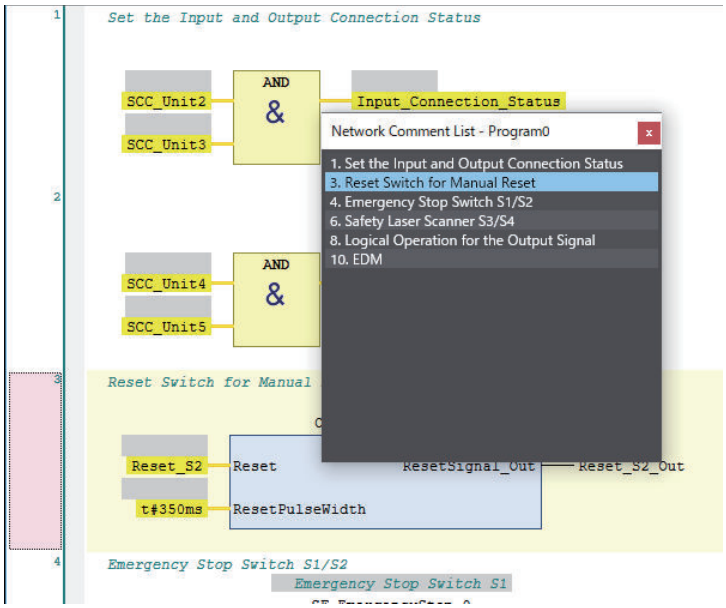
Method	Description
Method 1	Right-click on the FBD editor, and then select **Network Comment List** from the menu.
Method 2	On the FBD editor, press the **L** Key.



The list of network comment that are set in the current POU is displayed.



Select a network comment to jump to the location where the selected network comment is set.

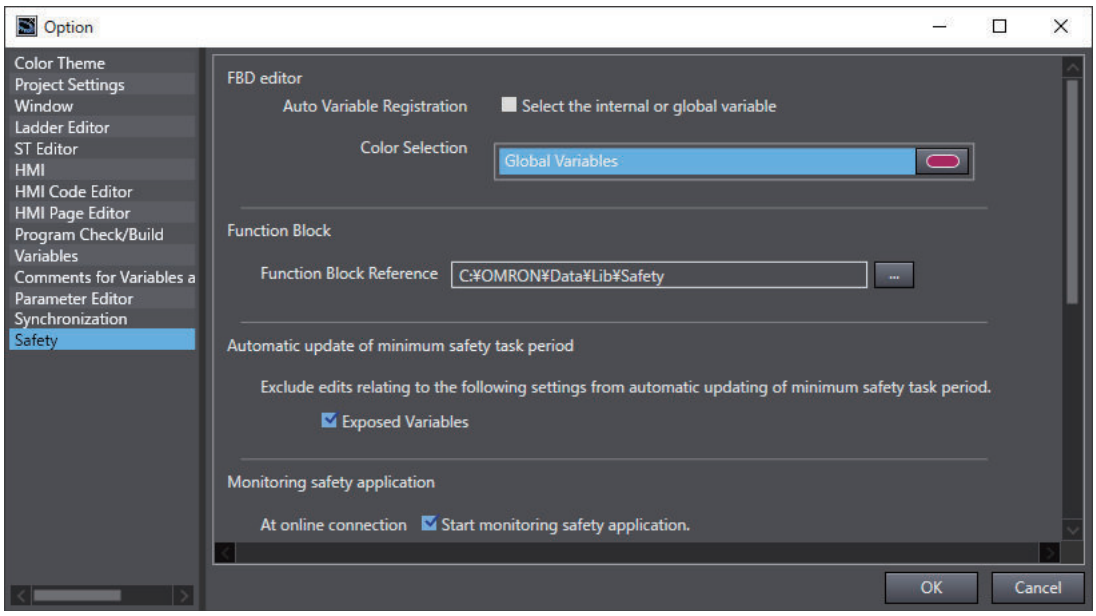


Color Selection for the FBD Editor

You can change the display color of global variables that are displayed in the FBD editor.

1 Select **Option** from the **Tools** menu.
The Option Dialog Box is displayed.

2 Select the **Safety** tab and click the button displayed at Color Selection.

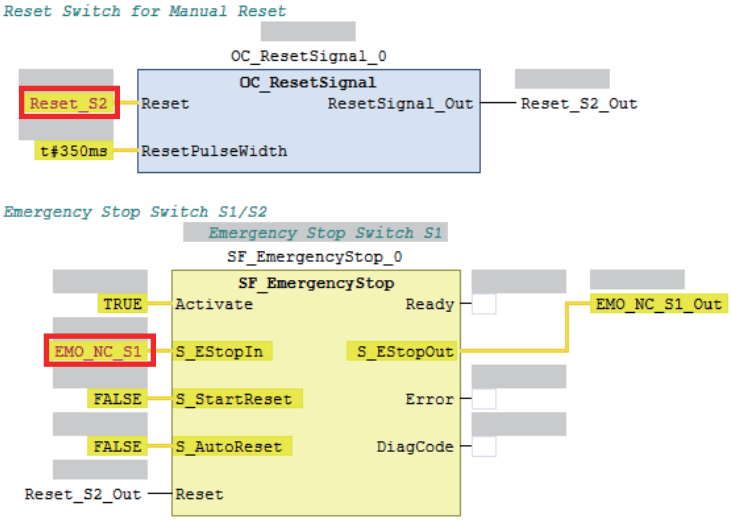


The Color Settings Dialog Box is displayed.



3 Select any color and click the **OK** button.

4 In the Option Dialog Box, click the **OK** button.
The color selection settings are applied.



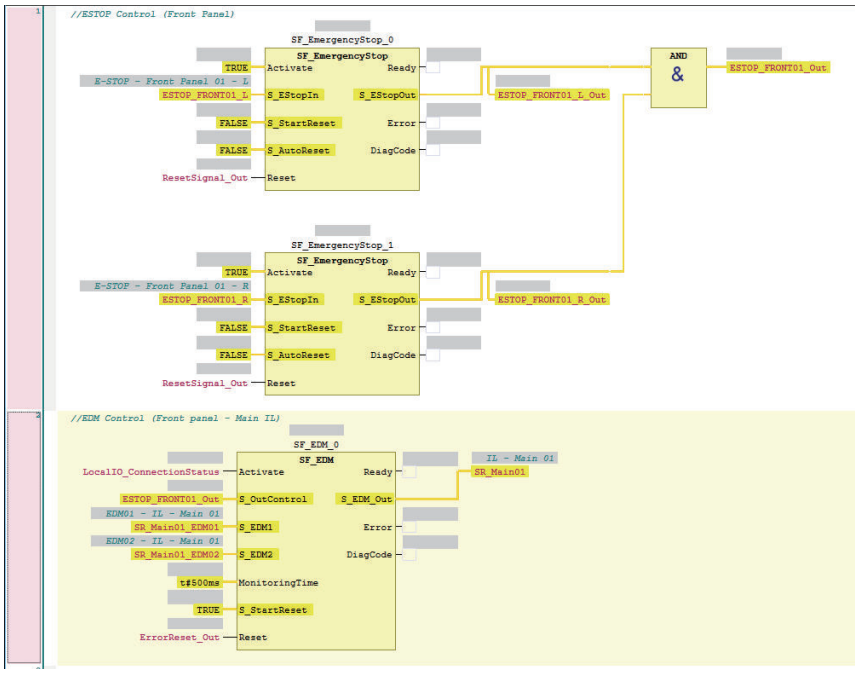
8-5-5 Program Pattern Copy

Program Pattern Copy is a function that allows you to easily replicate the FBD program having the same program pattern (logic part). The variable name of the replicated program can be automatically configured according to the variable name generation rules.

Operating Procedure

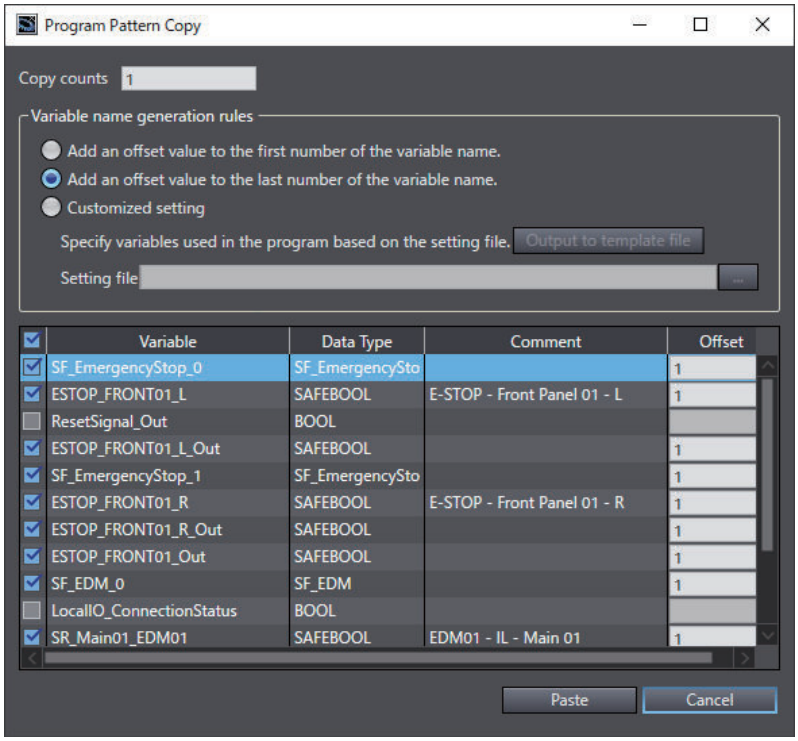
The procedure to copy a program pattern is explained below.

1 Select any FBD network.
You can select more than one FBD network by holding down the **Shift** or **Ctrl** Key.



2 Right-click a row and select **Program Pattern Copy** from the menu. Or, press the **Ctrl**+**Shift**+**V** Keys.

The following setting window is displayed.



3 Set the copy counts, variable name generation rules, variable name to be changed, and offset value.

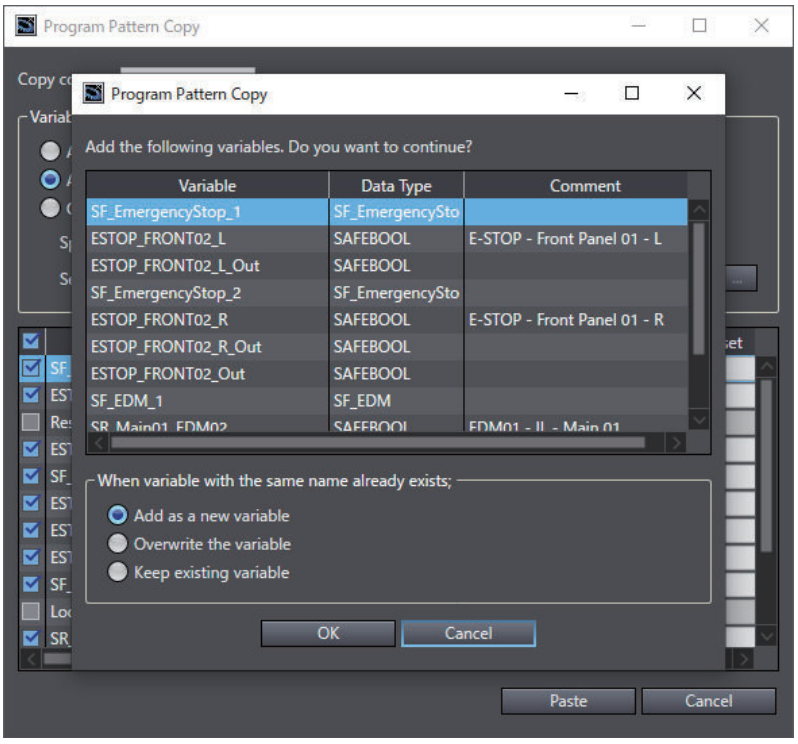
The setting items are given in the following table.

Item	Description
Copy counts	Set the number of times that the program can be replicated.

Item	Description
Variable name generation rules	Select a generation rule for the variable name. The rules you can select are as follows: • **Add an offset value to the first number of the variable name.** This rule generates another variable name by adding the offset value to the first number contained in the variable name. • **Add an offset value to the last number of the variable name.** This rule generates another variable name by adding the offset value to the last number contained in the variable name. • **Customized setting** This rule generates any variable name and comment by loading a setting file. Refer to *File Format for Customized Setting* on page 8-70 for details.
Variable name to be changed (Checkbox)	Select a variable to be renamed. Unchecked variables use the same variable names as those in the source program. Variables that do not include any number in the name are automatically excluded. Note that this setting is invalid when the variable name generation rules are set to **Customized setting**.
Offset	Set the offset value to be added to the variable name according to the variable name generation rules. Variables that do not include any number in the names are automatically excluded. Note that this setting is invalid when the variable name generation rules are set to **Customized setting**.

4 Click the **Paste** Button.

The following dialog is displayed when a variable is added by this function.

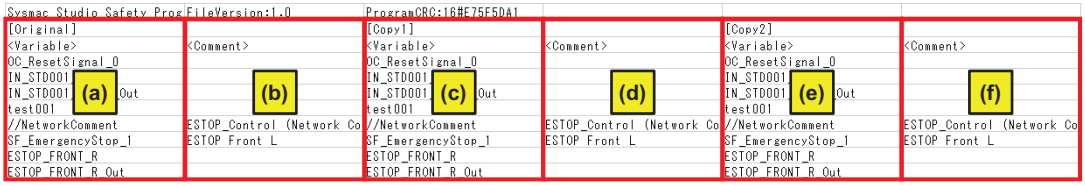


5 Select an option in **When variable with the same name already exists** and click the **OK** Button.

A replicated program is inserted under the selected FBD network. Check to see if the program and variables have been generated in the way you intended.

File Format for Customized Setting

The file format for the customized setting is shown below. Since the setting file contains the CRC of the selected FBD network, use the CSV file saved with **Output to template file**.



No.	Name	Description	Remarks
(a)	Source Variable Name	This is the variable name used in the source program to copy from.	Do not change this item.
(b)	Source Variable Comment	This is the variable comment used in the source program to copy from.	Do not change this item.
(c)	Copy 1 Variable Name	This is the variable name used for the first copy destination. You can set any variable name.	
(d)	Copy 1 Variable Comment	This is the comment for the variable used for the first copy destination. You can set any comment for the variable.	
(e)	Copy 2 Variable Name	This is the variable name used for the second copy destination. You can set any variable name.	
(f)	Copy 2 Variable Comment	This is the comment for the variable used for the second copy destination. You can set any comment for the variable.	

The **Variable Name** and **Variable Comment** columns will be repeated continuously.

Precautions for Correct Use

- After you edit the CSV file with a spreadsheet application, save the data in the CSV format (UTF-8).
- Network comments can be specified when the variable name generation rules are set to **Customized setting**. Since the identifier *//NetworkComment* is set in the variable name column of the setting file that is output as a template, set any text string for the variable comment.

8-5-6 Function Block Conversion for Programs

You can convert a generated program to a function block.

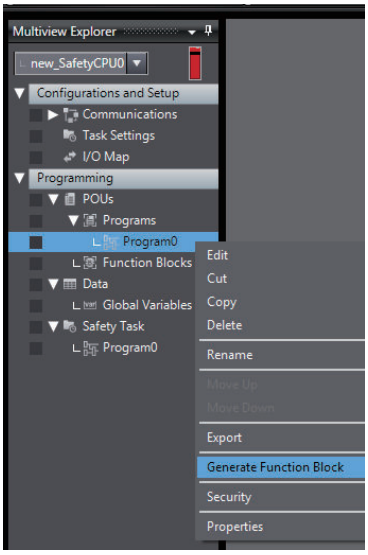
Conversion Method

Use the following conversion procedure.

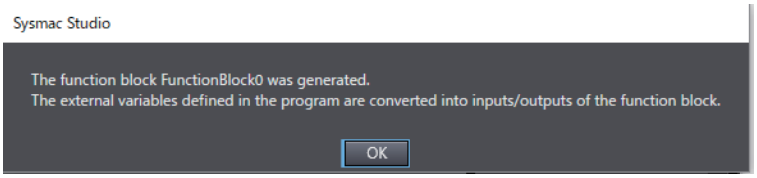
1 Select the Safety CPU Unit from the Controller Selection Box in the Multiview Explorer and open the Safety CPU Unit Setup and Programming View.

2 In the Multiview Explorer, select **Programming** – **POUs** – **Programs**. Then, select a program you want to convert into a function block.

3 Right-click the program and select **Generate Function Block** from the menu.



4 The following message appears and the converted function block is added under **Function Blocks**, which is located below **Programming** – **POUs** in the Multiview Explorer.



External variables defined in the program are automatically converted as shown below. Edit each item as necessary.

Item	Conversion method
Type of Variables	External variables are converted into input or output variables of the function block. If a value is written to an external variable in the POU, it is converted into an output variable. Otherwise, it is converted into an input variable.
Variable Name	It is converted into *FB_original variable name*.
Data Type	The data type of the external variable is applied to the input variable or output variable.
Initial Value	The initial value of the global variable referenced by the external variable is applied to the input variable or output variable.
Comment	The comments for the external variable are applied to the input variable or output variable. If the comments for the external variable are blank, the ones for the global variable are applied.

8-5-7 Building

Building is the process of converting the safety programs in your project into a format that is executable on the Safety CPU Unit.

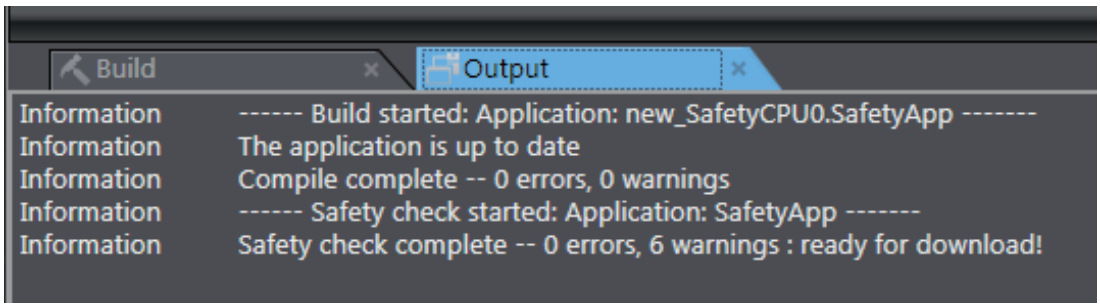
A check is performed on the programs and variables during this process. If there are any errors, the build is not performed and the errors are displayed in the Build Tab Page.

Executing the Build Process

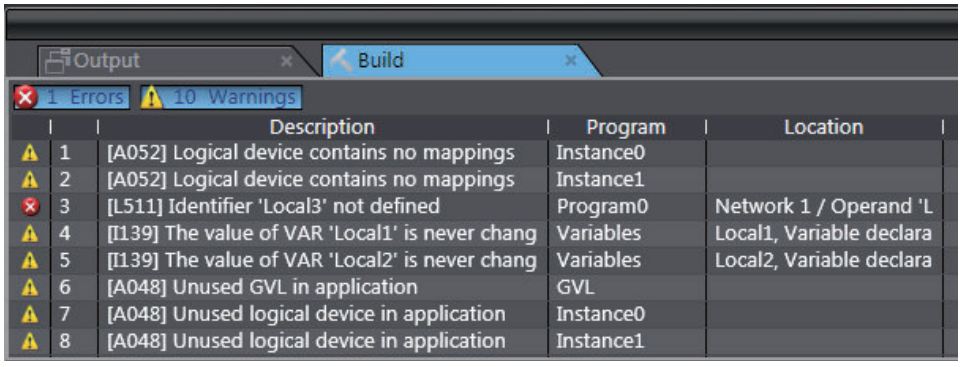
1 Use one of the following procedures to execute the build process.

Method	Operation
Method 1	Select **Build Controller** from the **Project** Menu.
Method 2	Press the **F8** Key.
Method 3	Click the **Build Controller** Button on the toolbar.

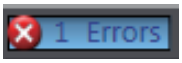
The build is started and the status during the build is displayed in the Output Tab Page.

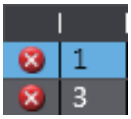
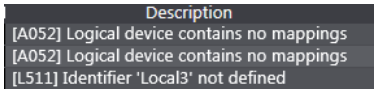
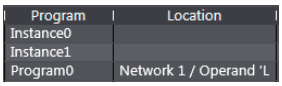


2 Click the **Build** Tab.
The Build Tab Page is displayed.
If there are any errors, a list of them is displayed.



The following items are displayed in the Build Tab Page.
If there is an error, double-click a line in the list to display the location of the error, and then correct the error.

Item	Example	Description
Number of errors		Displays the total number of errors.

Item	Example	Description
Number of warnings		Displays the total number of warnings.
Error or warning number		Displays the errors or warnings in the order in which they were found.
Description		Displays a description of the error or warning.
Location		Displays the location where the error or warning occurred. You can jump directly to the location of the error.

Additional Information

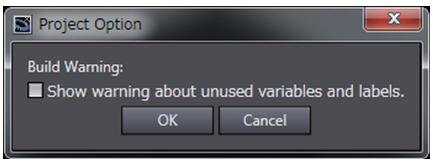
If the data size of the program exceeds the program capacity of the Safety CPU Unit, a Capacity Exceeded Error will occur when you change to DEBUG mode.
Reduce the number of FBs or variables that are used.

Changing Build Options

You can change the warning setting to change the build warning display settings for unused variables and jump labels.

Use the following procedure to change warning levels.

1 Select **Project Options** from the **Project** Menu.
The Project Option Dialog Box is displayed.



2 Select the check box and click the **OK** Button.
The specified warnings are shown or hidden accordingly.

8-5-8 Searching and Replacing

You can search for and replace strings in the data of a project.

Scope of Searching and Replacing

You can search for and replace text strings in the following items.

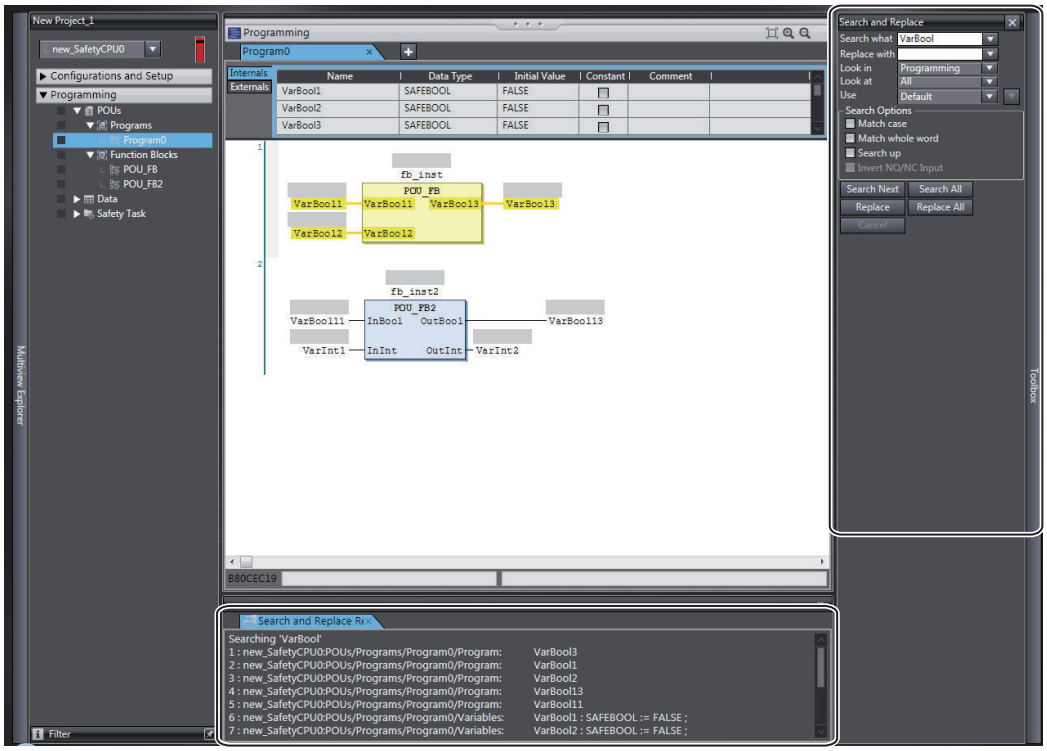
Selected item	Scope of Searching and Replacing
All items (text strings)	Variable names, variable comments, FBD network comments, jump labels, and Jump instructions.
Variable	Variable names
Instruction	Function block instance names

Search and Replace Pane

1 Use one of the following procedures to display the Search and Replace Pane in place of the Toolbox.

Method	Operation
Method 1	Select **Search and Replace** from the **Edit** Menu.
Method 2	Press the **Ctrl** + **F** Keys.
Method 3	Click the **Search and Replace** Button on the toolbar.

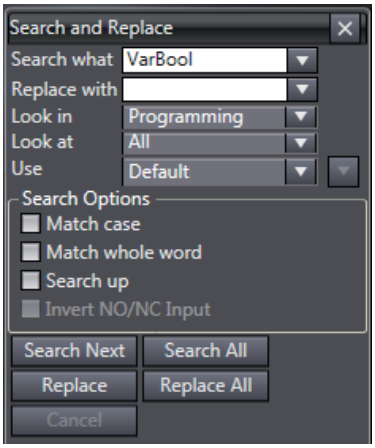
The Search and Replace Pane is displayed.

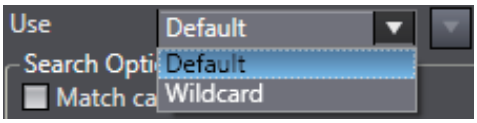


2 In the Search and Replace Pane, enter the text string and set the applicable search conditions, and then click one of the buttons for search or replace.
The results of the search and replace process are displayed on the **Search and Replace Results** Tab Page.
Double-click the line in the displayed results to move the focus to the corresponding location.

Setting Items

The setting items in the Search and Replace Pane are explained below.



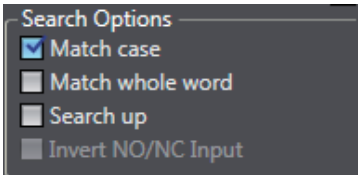
Setting Items	Description
Search what	• Enter a search string. • You can select from previous search strings in the list.
Replace with	• Enter the string to replace the search string with. • You can select from previous replacement strings in the list. You cannot use wildcard characters.
Look in	Specify the range to search. You can select from the following. Programming : The search is performed on the program to which the selected element belongs when the search is executed. If the search is made on the Safety CPU Unit Setup and Programming View, the search is performed only for the program in the Safety CPU Unit. Current view : The current view is searched.
Look at	Specify the items to search. You can perform a search on the following items. All : Variable tables (variable names in the table) and programs (jump labels, Jump instruction names, and variable names in the programs) Variable Name : Searches all variable names. Instruction : Function block instance names
Use	Specify if you want to use wildcard *1 characters. Default : Do not use wildcard characters. Wildcard : Use wildcard characters. If you select to use wildcard characters, you can click the  Button to the right to view a list of characters used for wildcard characters. Select any of these characters to enter them in the **Search** string. 

*1. The characters that you can use as wildcard characters are given on the next page.

● Wildcards

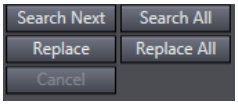
Character	Meaning	Description	Example
*	Zero or more characters	Searches for a text string that contains a variable text string.	“new*” matches “newfile.txt”.
?	Any single character	Searches for a text string with a variable character.	“A?C” matches “ABC”, “AdC”, and “AzC”.
#	Any single number	Searches for any single number.	“7#” matches “71”. “ABC#” matches “ABC5”.
[ ]	Character in a set	Searches for a single character in the set.	“ABC[xyz]” matches “ABCx” and “ABCy”. “ABC[x-z]” matches “ABCx” and “ABCy”.
[!]	Character not in a set	Searches for a single character that is not in the set.	“ABC[!xyz]” matches “ABCa” and “ABCd”. “ABC[!x-z]” matches “ABCa” and “ABCd”.

● Search Options



Item	Function
Match case	When this option is selected, searches are case sensitive.
Match whole word	When selected, only exact string matches are returned.
Search up	When selected, the search is performed backward from the cursor position.

● Button Functions



Item	Function
Search Next	Performs a search according to the selected options.
Search All	Searches all items and lists the results in the Output Tab Page.
Replace	Performs a replace according to the selected options.
Replace All	Replaces all items and lists the results in the Output Tab Page.
Cancel	Cancels the current search and replace operation.

8-5-9 Safety Task Settings

This section describes the procedures that are used to select the programs to execute in the safety task and the execution order of the selected programs. It also describes how to set the task period of the safety task.

Refer to *Section 10 Calculating Safety Reaction Times* on page 10-1 for details on safety tasks.

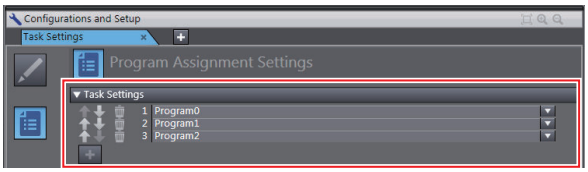
Program Assignments

The program assignment settings are used to assign the programs to the safety task and set the program execution order.
The programs that are assigned to the task are executed in the specified order.

1 Double-click **Task Settings** under **Configurations and Setup** in the Multiview Explorer.

2 Click the **Program Assignment Settings** Button ( ) in Safety Task Settings Tab Page in the Edit Pane.

3 The buttons shown within the red frame below allow you to change the program assignments and their execution order.



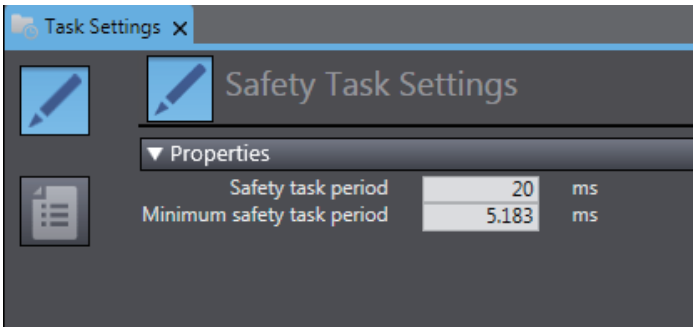
Precautions for Correct Use

Any program you assign must already be registered under **Programming** - **POUs**.

Setting the Task Period

1 Double-click **Task Settings** under **Configurations and Setup** in the Multiview Explorer.
The Safety Task Settings Tab Page is displayed.

2 If the **Safety Task Settings** Display does not appear on the Safety Task Settings Tab Page in the Edit Pane, click the **Safety Task Settings** Button ( ).



The minimum safety task period is automatically calculated and displayed based on the program and settings information.

3 Set the task period for the safety task.
Set the safety task period to a value that is within 100 ms of the minimum safety task period.

8-5-10 Variable Comment Switching Function

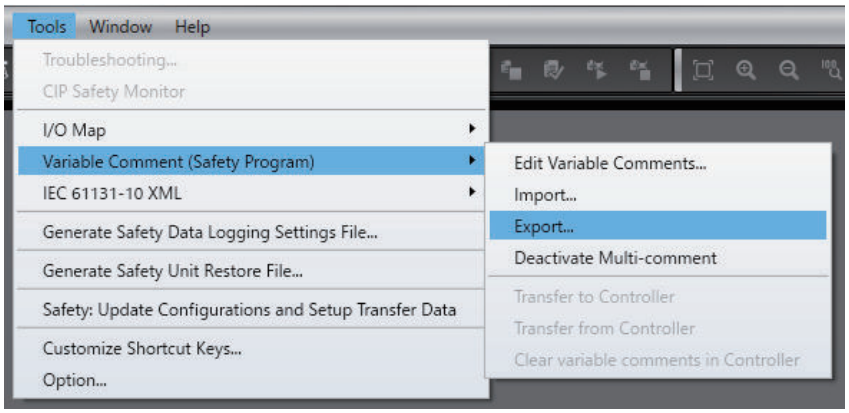
The variable comment switching function is designed to switch the variable comment displayed in the safety program or on the variable table to another comment.
To use this function, add any variable comment by using one of the following methods.

- **Importing a Comment File**
  Export the original variable comment file, add the variable comments used in the comment switching destination and import the comment file.
- **Editing with the Edit Variable Comments Function**
  Use the Edit Variable Comments function to edit displayed comments used for the variable comment switching function.

The operation procedure of this function is explained below.

Exporting Variable Comments

1 Select a Safety CPU Unit from which the variable comment is exported. On the **Tools** Menu, select **Variable Comment (Safety Program)** - **Export**.



The Save File Dialog Box is displayed.

2 Enter a file name, and then click the **Save** Button.
The comments for variables are saved in the CSV format.

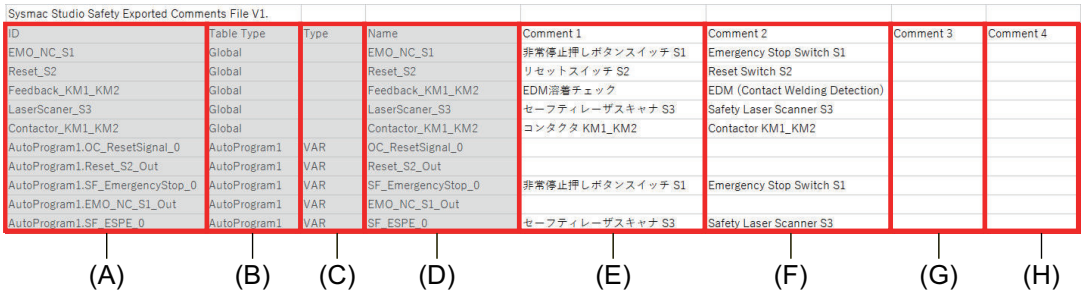
Additional Information

The variable comments of which displaying is disabled by the data protection feature will not be exported. Before you export such comments, temporarily disable the data protection that is being applied.

Editing a Variable Comment File

Edit comments for variables in the exported CSV file.

1 Open the CSV file on a spreadsheet application.



Sysmac Studio Safety Exported Comments File V1.							
ID	Table Type	Type	Name	Comment 1	Comment 2	Comment 3	Comment 4
EMO_NC_S1	Global		EMO_NC_S1	非常停止押しボタンスイッチ S1	Emergency Stop Switch S1		
Reset_S2	Global		Reset_S2	リセットスイッチ S2	Reset Switch S2		
Feedback_KM1_KM2	Global		Feedback_KM1_KM2	EDM溶着チェック	EDM (Contact Welding Detection)		
LaserScaner_S3	Global		LaserScaner_S3	セーフティレーザスキャナ S3	Safety Laser Scanner S3		
Contactor_KM1_KM2	Global		Contactor_KM1_KM2	コンタクタ KM1_KM2	Contactor KM1_KM2		
AutoProgram1.OC_ResetSignal_0	AutoProgram1	VAR	OC_ResetSignal_0				
AutoProgram1.Reset_S2_Out	AutoProgram1	VAR	Reset_S2_Out				
AutoProgram1.SF_EmergencyStop_0	AutoProgram1	VAR	SF_EmergencyStop_0	非常停止押しボタンスイッチ S1	Emergency Stop Switch S1		
AutoProgram1.EMO_NC_S1_Out	AutoProgram1	VAR	EMO_NC_S1_Out				
AutoProgram1.SF_ESPE_0	AutoProgram1	VAR	SF_ESPE_0	セーフティレーザスキャナ S3	Safety Laser Scanner S3		

(A) (B) (C) (D) (E) (F) (G) (H)

No.	Name	Description	Remarks
(A)	ID	Unique ID automatically assigned to a variable.	Do not change this item.
(B)	Table Type	The type of the variable table is displayed. • Global: Global variable • POU name: Local variable	Do not change this item.
(C)	Type	The type of the local variable table is displayed. • VAR: Internal variable • VAR_EXTERNAL: External variable • VAR_INPUT: Input variable • VAR_OUTPUT: Output variable	Do not change this item.
(D)	Name	The variable name is displayed.	Do not change this item.
(E)	Comment 1	This is a comment for the registered variable.	
(F)	Comment 2	This is a comment for the variable registered at Comment 2.	
(G)	Comment 3	This is a comment for the variable registered at Comment 3.	
(H)	Comment 4	This is a comment for the variable registered at Comment 4.	

2 For **Comment 2**, **Comment 3** or **Comment 4**, enter a variable comment to be switched.

3 Save the CSV file.

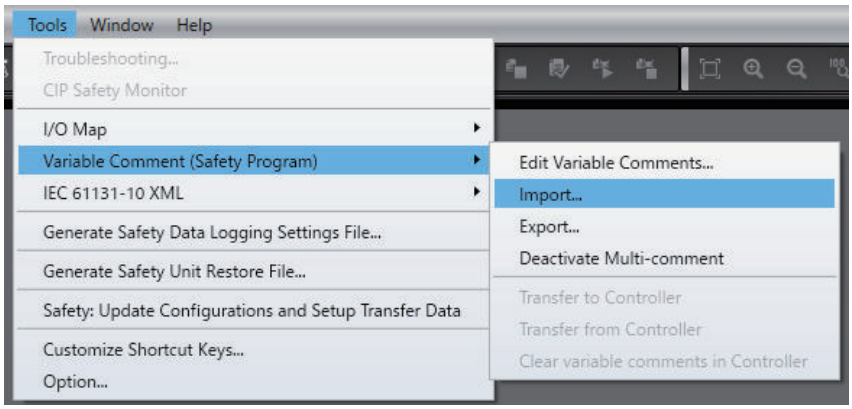
Precautions for Correct Use

- Do not change the contents of the variable comment file except for **Comment 1** through **Comment 4**.
- If you leave the comment field of **Comment 2** through **Comment 4** blank, the target variable comment becomes empty.

Importing a Variable Comment File

Import the edited CSV file to the original project.

1 Select a Safety CPU Unit to which the variable comment is imported. On the **Tools** Menu, select **Variable Comment (Safety Program)** - **Import**.



The File Selection Dialog Box is displayed.

2 Select an CSV file to import, and then click the **Open** Button.
The Confirmation Dialog Box for the import is displayed.
When you click the **OK** Button, the import function executes and replaces the comments in the project with the comments in the CSV file.
If an error occurs during the import processing, the error details are displayed in the Output Tab Page.

Precautions for Correct Use

- When you import a variable comment file, the comments in the target Safety CPU Unit inside the project are replaced with the comments in the variable comment file. Please remember that the original comments cannot be restored.
- After importing a variable comment file for project data, the project data cannot be imported using Sysmac Studio Ver.1.28 and earlier.
- If the content of **Comment 1** was modified by the import function of the variable comment file, the safety validation status becomes unvalidated. Changing the contents of **Comment 2** through **Comment 4** will not change the validated status.
- If **Comment 1** in the variable comment file is empty, the contents of **Comment 2** through **Comment 4** will not be imported.
- If there is no corresponding variable in the import destination of the variable comment file, the comment for the variable is excluded from the import target.
- If there are duplicated entries in **Comment 1**, the first found entry in **Comment 2** through **Comment 4** in CSV will be imported.

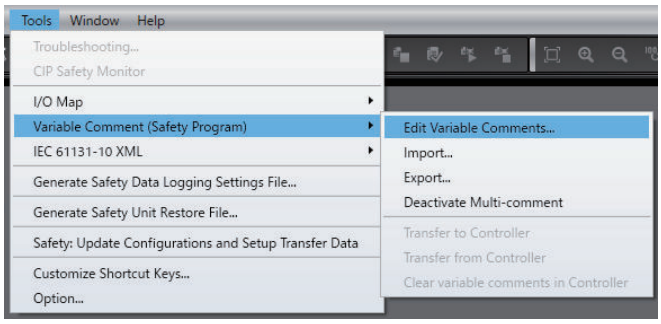
Additional Information

The variable comments of POUs of which editing is disabled by the data protection feature will not be imported. Before you import such comments, temporarily disable the data protection that is being applied.

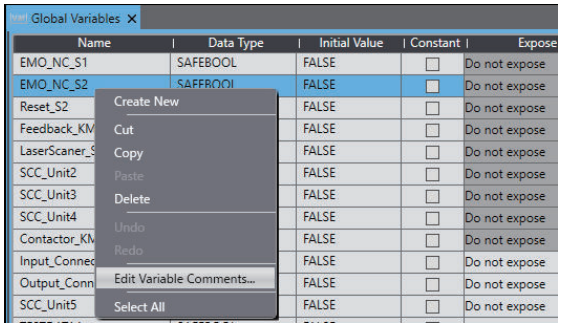
Edit Variable Comments Function

This function edits variable comments used for the variable comment switching function.
Use the following procedure to display the Edit Variable Comments Window, and add or edit any variable comment.

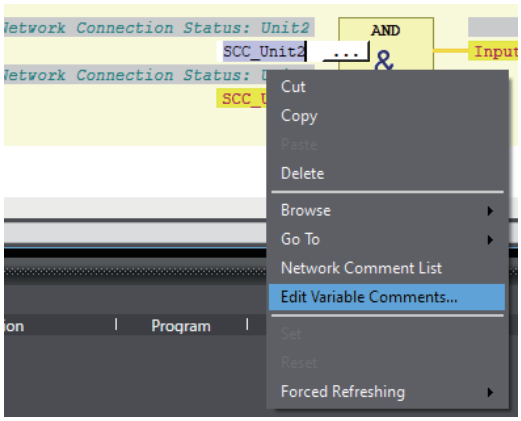
- **Method 1: How to start the Edit Variable Comments Window from the Tools menu**
  Select **Variable Comment (Safety Program)** - **Edit Variable Comments** from the **Tools** menu.



- **Method 2: How to start the Edit Variable Comments Window from the variable table**
  Select any variable in the variable table, and right-click the variable and select **Edit Variable Comments**.

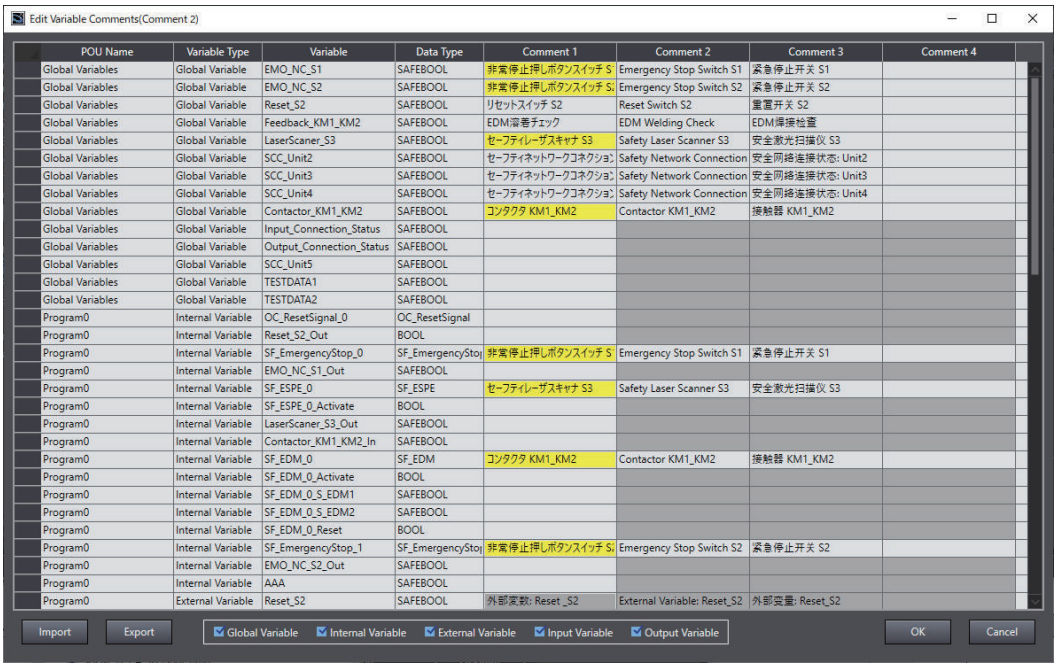


- **Method 3: How to start the Edit Variable Comments Window from the FBD editor**
  Select any variable in the FBD editor, and right-click the variable and select **Edit Variable Comments**.



When the Edit Variable Comments Window is started by method 2 or 3, it is displayed with the variable selected.

- **The Edit Variable Comments Window**
  When the Edit Variable Comments function is executed, the following screen is displayed.



The display contents of the Edit Variable Comments Window are as follows.

Item	Description	Remarks
POU Name	This is the name of POUs (programs and function blocks) in which variables are defined. The variables defined in the global variable table are displayed as *Global Variables*.	(Cannot be edited.)
Variable Type	Displays the type of variable table in which the variable is defined.	(Cannot be edited.)
Variable	Displays the variable name.	(Cannot be edited.)
Data type	Displays the data type of the variable.	(Cannot be edited.)
Comment 1	Displays the comment registered at the variable.	
Comment 2	Displays the comment for the variable registered at Comment 2.	
Comment 3	Displays the comment for the variable registered at Comment 3.	
Comment 4	Displays the comment for the variable registered at Comment 4.	
The **Import** button	Import the variable comments to the Edit Variable Comments Window. Refer to *Editing a Variable Comment File* on page 8-79 for the format of a variable comment file.	
The **Export** button	Export the variable comments from the Edit Variable Comments Window. Refer to *Editing a Variable Comment File* on page 8-79 for the format of a variable comment file.	
Variable Type Filtering check box	Displays only variable types for which the check boxes are selected.	

Note If the content of **Comment 1** is duplicated with other variable comments, the background of it is yellow. The variable comment switching function reflects the contents of **Comment 2** to **Comment 4** of the variable first found in the Edit Variable Comments Window, if the contents of **Comment 1** are duplicated.

Edit the contents of **Comment 1** to **Comment 4** of any variable. When you click the **OK** button, the contents of **Comment 1** to **Comment 4** are reflected in the project.

Precautions for Correct Use

- Project data, for which **Comment 2** to **Comment 4** are set by the Edit Variable Comments function, cannot be imported by using the Sysmac Studio Ver.1.28 and earlier.
- If the content of **Comment 1** was modified by the Edit Variable Comments function, the safety validation status becomes unvalidated. Changing the contents of **Comment 2** through **Comment 4** will not change the validated status.
- If **Comment 1**is empty, the comments from **Comment 2** to **Comment 4** will not be set.

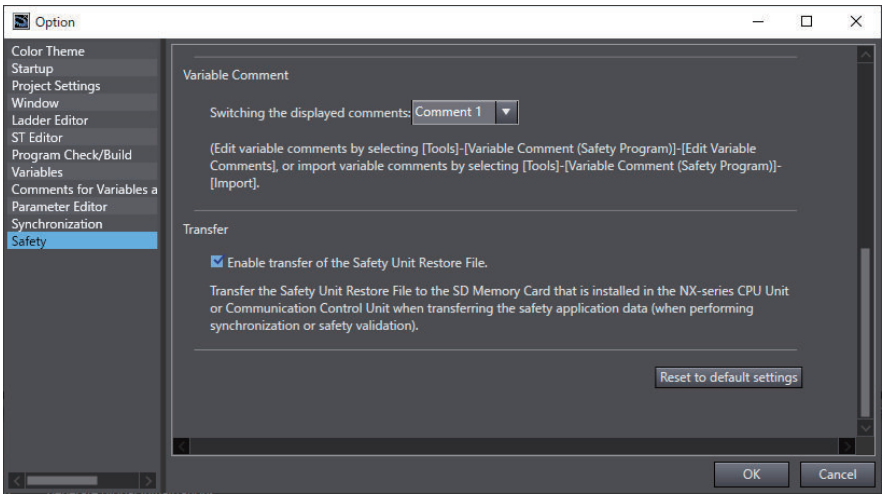
Additional Information

Variable comments of POUs of which editing is disabled by the data protection feature cannot be edited. Before you edit such comments, temporarily disable the data protection that is being applied.

Switching the Displayed Comments

The procedure below switches display to the comment in the imported variable comment file.

1. On the **Tools** Menu, select **Option** and open the Option Settings Dialog Box.
2. Select the **Safety** Tab. Go to **Variable Comment** - **Switching the displayed comments**. From the dropdown list, select a comment to show and click the **OK** Button.



The switched comment appears when you display the variable table or open the FBD editor.

Precautions for Correct Use

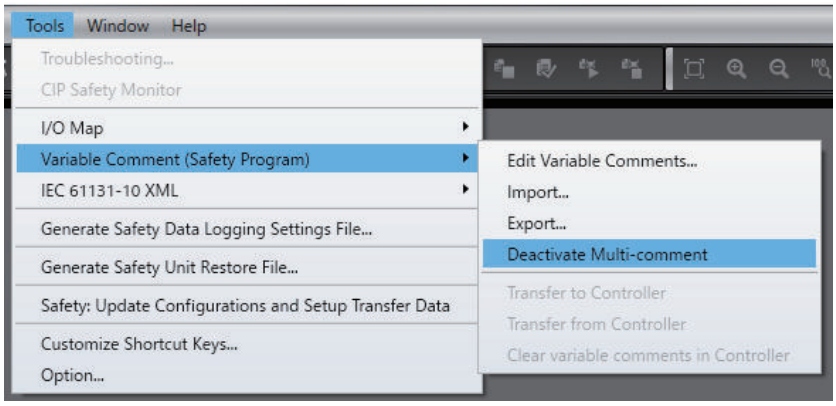
If the display comment is set to other than **Comment 1**, the variable comment cannot be edited except by using the Edit Variable Comments Function.

Deactivating Multi-comment

This section describes the procedure to delete variable comments entered in **Comment 2** through **Comment 4** that are used for the switching variable comment function.

The project containing the imported variable comment file cannot be opened on Sysmac Studio Ver.1.28 and earlier because the switching variable comment function is not supported. When you delete variable comments in **Comment 2** through **Comment 4** in the following procedure, the project can be opened on Sysmac Studio Ver.1.28 and earlier.

1 On the **Tools** Menu, select **Variable Comment (Safety Program)** - **Deactivate Multi-comment**.



If **Deactivate Multi-comment** is executed, the content of **Comment 1** is always displayed as the variable comment regardless of the option settings configured in **Safety** - **Variable Comment** - **Switching the displayed comments**.

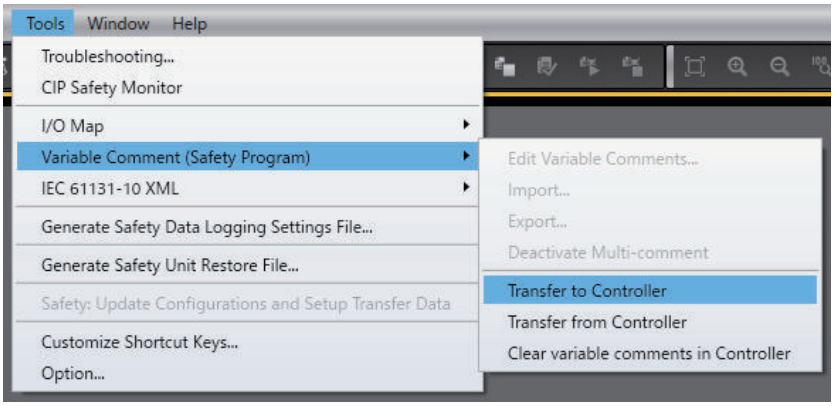
Transferring Variable Comments

The settings for **Comment 2** and the subsequent comments can be downloaded to the controller by using the function introduced below.
If you downloaded the settings for **Comment 2** and the subsequent comments to the controller, the settings for **Comment 2** and the subsequent comments can be restored by the upload.

● Downloading Settings for Comment 2 and the Subsequent Comments to the Controller

Use the following procedure to download the settings for **Comment 2** and the subsequent comments.

- Establish an online connection with the controller. Go to the **Tools** Menu and select **Variable Comment (Safety Program)** - **Transfer to Controller**.



Precautions for Correct Use

Since the settings for **Comment 2** and the subsequent comments are not included in the safety application data, they are not transferred to the Safety CPU Unit.

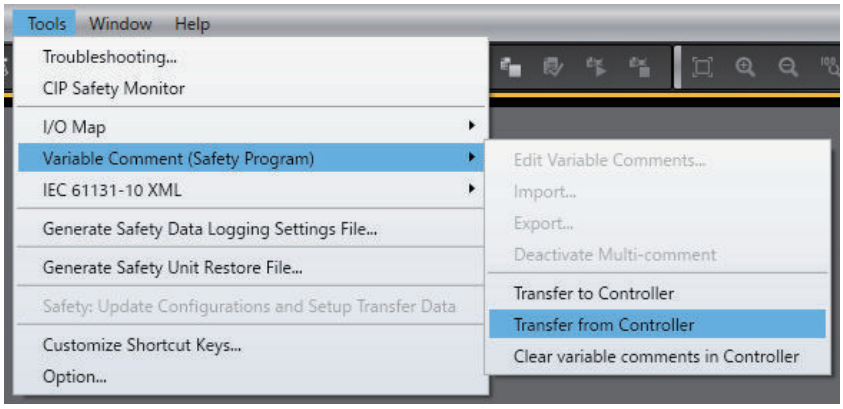
Additional Information

The settings for **Comment 2** and the subsequent comments are downloaded when the safety application data is transferred, such as during the execution of validation check or transfer by synchronization.

● Uploading Settings for Comment 2 and the Subsequent Comments from the Controller

Use the following procedure to upload the settings for **Comment 2** and the subsequent comments.

- Establish an online connection with the controller. Go to the **Tools** Menu and select **Variable Comment (Safety Program)** - **Transfer from Controller**.



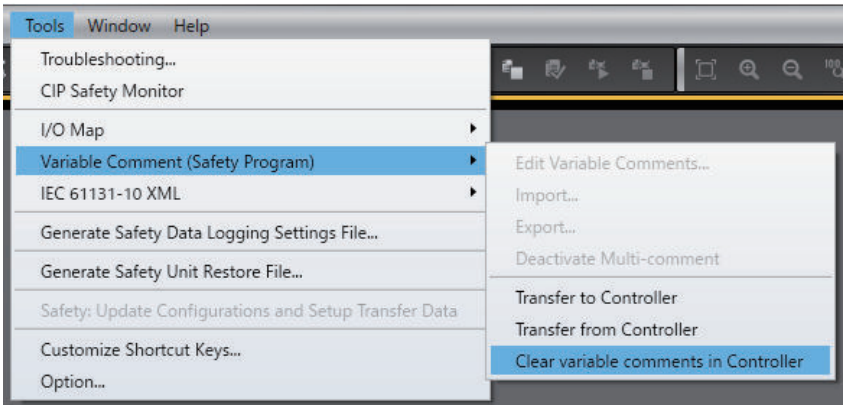
Additional Information

The settings for **Comment 2** and the subsequent comments are uploaded when the transfer of safety application data is executed by synchronization.

● Clearing Settings for Comment 2 and the Subsequent Comments from the Controller

Use the following procedure to clear the settings for **Comment 2** and the subsequent comments.

- Execute the Clear All Memory operation for the controller.
- Establish an online connection with the controller. Go to the **Tools** Menu and select **Variable Comment (Safety Program)** - **Clear variable comments in Controller**.



Precautions for Correct Use

If you use Sysmac Studio Ver.1.28 and earlier to upload safety application data from the controller and the Safety CPU Unit containing a downloaded variable comment file for the Safety CPU Unit, the data for **Comment 2** and the subsequent comments are not restored because Ver.1.28 and earlier does not support the variable comment switching function.

Additional Information

- If you use the SD Memory Card backup function of the controller, the settings for **Comment 2** and the subsequent comments are included in the backup or restored target.
- If you use the controller backup functions of Sysmac Studio, the settings for **Comment 2** and the subsequent comments are included in the backup or restored target.
- If you use the importing/exporting backup files function of Sysmac Studio, the settings for **Comment 2** and the subsequent comments are not included in the import or export target.

8-6 Automatic Programming

This section describes "automatic programming", which generates safety programs based on required specifications for the safety system using the Sysmac Studio.

⚠ WARNING

Programs generated by the automatic programming do not guarantee functional safety. Before you perform validation test of the safety programs, complete debugging of the safety programs.
Otherwise, the Safety CPU Unit will start with safety programs that are not fully debugged, and may cause serious personal injury.

8-6-1 Generation Algorithms for Automatic Programming

When a program is generated by executing the automatic programming function, the Sysmac Studio generates a safety program in the following steps:

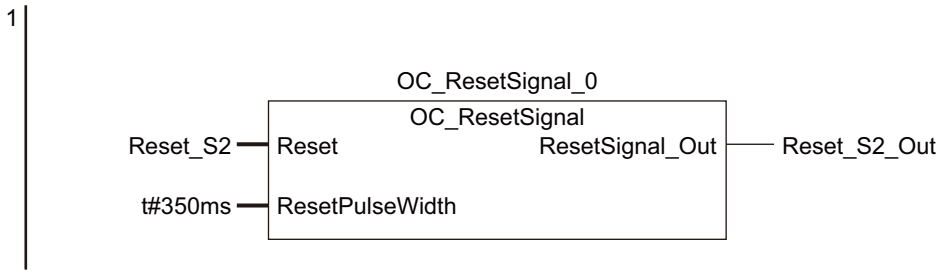
- Reset Signal Generation
- Input Signal Generation
- Generation of Logical Operation Circuit
- Output Signal Generation

● Reset Signal Generation

The automatic programming function creates a function block that generates a reset signal on the first network.

When a variable set in the **Basic Settings** on the Automatic Programming Settings Tab Page changes to FALSE after staying TRUE for a certain period of time, the reset signal detects the change of the variable and is set to TRUE for only one cycle. The default pulse width is set to 350 ms.

The generated reset signal here is used as a reset signal of the safety function block when an input signal is generated.



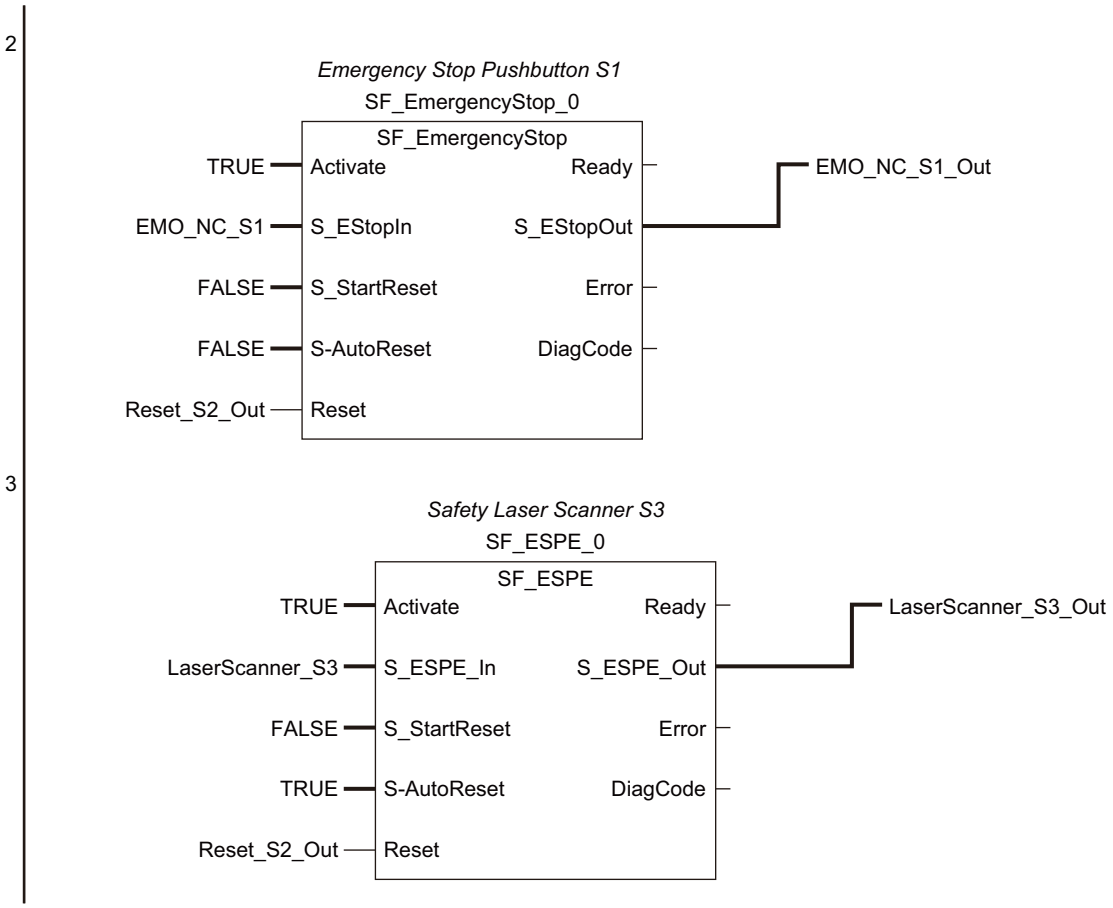
● Input Signal Generation

This step creates the function block that is defined in **Input Settings** on the Automatic Programming Settings Tab Page.

The variable name specified in **Input Settings** in the Automatic Programming Settings Tab Page is used for input variables for the function block. In addition, the output variable of the function block is automatically named as an internal variable, and is used as an input signal when a logical operation circuit is generated.

The following table shows values set to input variables of the function block.

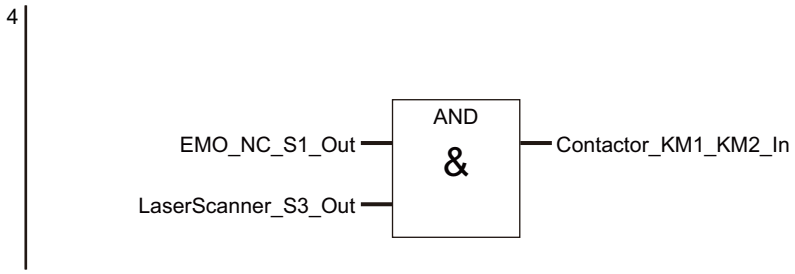
Input variable name	Setting value
Activate	TRUE
S_StartReset	FALSE
S_AutoReset	Value specified for the reset type Manual: FALSE Auto: TRUE
Reset	Variable generated in the reset signal generation step
MonitoringTime	t#300ms
Any other input variables	Variable automatically generated based on the following naming rule: **FB Instance Name_Input Variable Name**



● Generation of Logical Operation Circuit

At this step, an AND logic function is generated for each output variable based on the **Expected Value Settings** in the Automatic Programming Settings Tab Page.

The internal variables, which are automatically generated at the input signal generation, are used as input variables for the AND function. In addition, the output variable of the AND function is automatically generated as an internal variable and is used as an input signal at the following output signal generation.

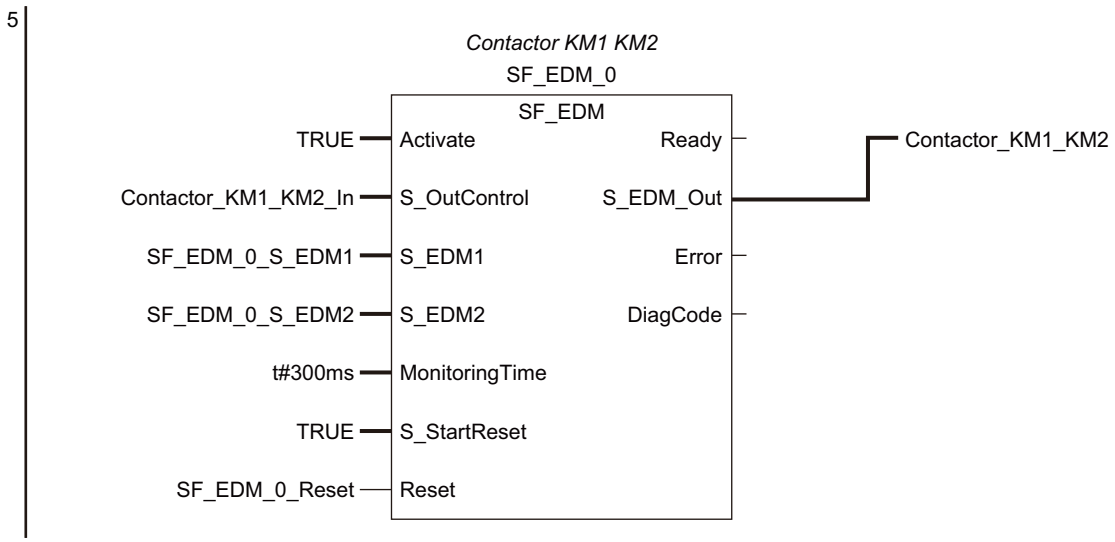


● Output Signal Generation

At this step, an SF_EDM function block is generated based on the Use EDM settings defined for **Output Settings** on the Automatic Programming Settings Tab Page.
The internal variable, which is automatically generated at the generation of logical operation circuit, is used as an input signal for the SF_EDM function block.

In addition, the variable name specified in **Output Settings** in the Automatic Programming Settings Tab Page is used for an output variable of the SF_EDM function block. The output variable, which is generated at the generation of logical operation circuit, is applied if the SF_EDM function block is not used. The following table shows values set to the input variables for the SF_EDM function block.

Input variable name	Setting value
S_StartReset	TRUE
MonitoringTime	t#300ms
Any other input variables	Variable automatically generated based on the following naming rule: **FB Instance Name_Input Variable Name**



Precautions for Correct Use

- The function block **OC_ResetSignal**, which is added by the automatic programming function, is protected with the display prohibition setting. You can display the Help menu for **OC_ResetSignal** by selecting **OC_ResetSignal** in the program or toolbox and pressing the **F1** Key.
- Variables and constants defined for the instances of each function block are necessary information for running the program. You can edit and fine-tune them in accordance with the equipment configuration and applications.

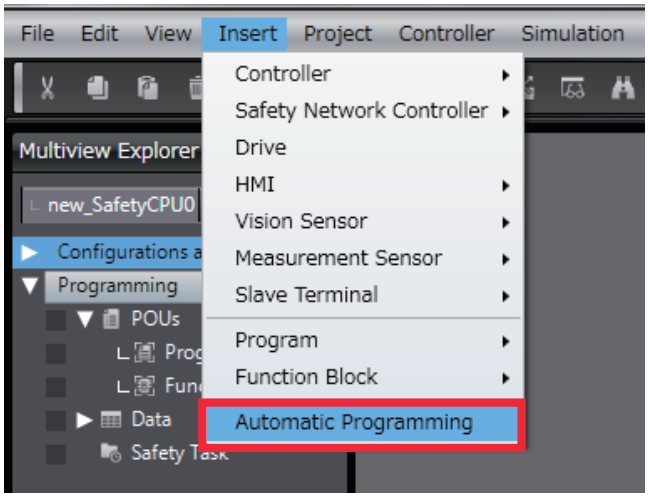
8-6-2 Automatic Programming Settings

To execute the automatic programming, you need to specify the following items on the Automatic Programming Settings Tab Page.

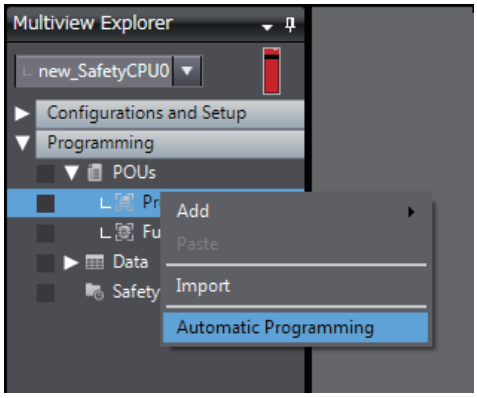
- Reset signal
- Input signal
- Output signal
- Expected value of the output signal corresponding to the input signal

You can open the Automatic Programming Settings Tab Page in either of the following procedures:

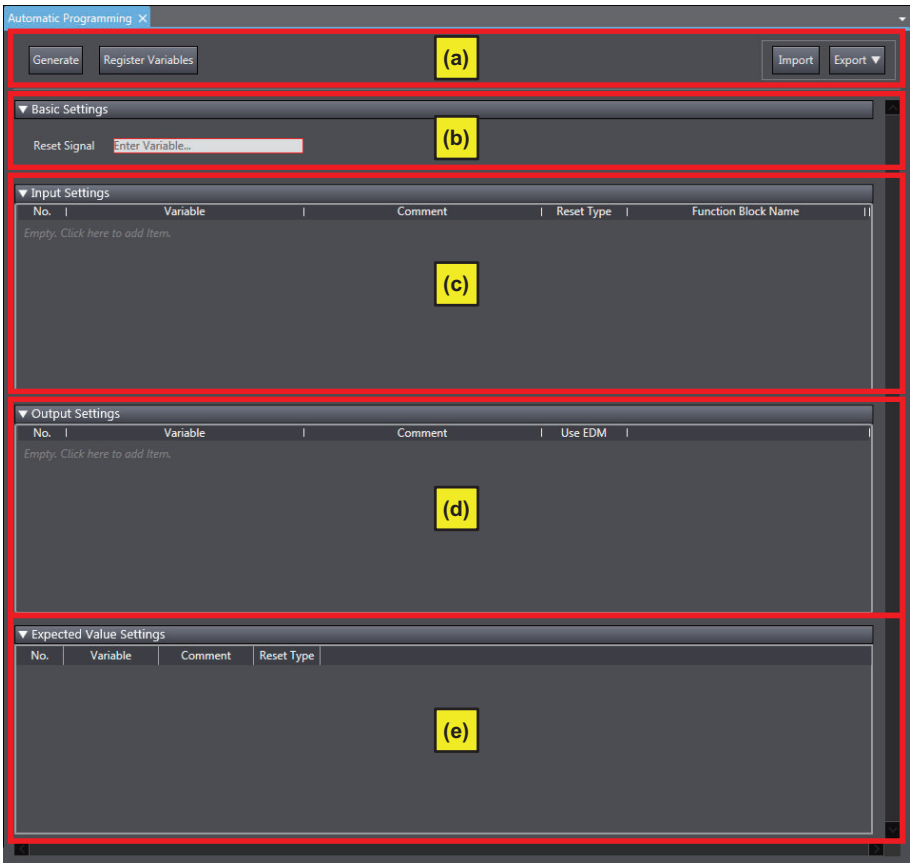
- Select **Automatic Programming** from the **Insert** Menu.



- In the Multiview Explorer, select **Programming** – **POUs** – **Programs**. On the right-click menu, select **Automatic Programming**.



The Automatic Programming Settings Tab Page consists of the items shown in the following table.



Letter	Name	Function	
(a)	Operation Panel	The operation panel is used to make settings for and execute the automatic programming.	
		Generate Button	Generates a program using the automatic programming.
		Register Variables Button	Registers the variables that are used for the automatic programming.
		Import Button	Imports the settings for the automatic programming from a CSV file. If you import the settings, the current settings are overwritten.
		Export – CSV File Output	Exports the current automatic programming settings to a CSV file.
		Export – Export to Simple Automatic Test	Exports the current automatic programming settings to the simple automatic test settings. The settings of the export destination are overwritten.
		Export – Export to Online Functional Test	Exports the current automatic programming settings to the online functional test settings. The settings of the export destination are overwritten.
(b)	Basic Settings	Set the variable to use as a reset signal for the safety program. You can set any SAFEBOOL or BOOL variable that is defined in the global variable table. When a program is generated, the variable name for the configured reset signal is assigned to the input variable *Reset* of the safety function block that is linked to each input signal.	

Letter	Name	Function	
(c)	Input Settings	Specify a variable for the input signal used for automatic programming. In addition to the variable name, you need to specify a reset type and a linked safety function block for the input signal.	
		Variable	Specify a variable name used as input signal for the program. You can specify a SAFEBOOL or BOOL-type variable for the variable name.
		Reset Type	Select a reset type in the box. The default value of the reset time is a manual reset. The selected reset type is assigned to the input variable *S_AutoReset* of the safety function block that is linked to each input signal. When a program is generated, *S_AutoReset* is set t to FALSE for a manual reset, and set to TRUE for an automatic reset.
		Function Block Name	Specify the name of a safety function block that is linked to each input signal. You can also specify a user-defined function block. If you specify a user-defined function block, you need to define at least one SAFEBOOL or BOOL-type variable as the input and output variables.
(d)	Output Settings	Specify a variable for output signal used for automatic programming. Specify a variable name, and enable or disable EDM for the output signal.	
		Variable	Specify a variable name used as the output signal for the program. You can specify a SAFEBOOL or BOOL-type variable for the variable name.
		Use EDM	If it is TRUE, the SF_EDM function block is used when a program is generated.
(e)	Expected Value Settings	A matrix of the variables that are specified in the input settings and the output settings is displayed. Set the expected value of the output variable for each input variable. The expected values set for the output variables have the following meanings: • 0 If the input variable changes to FALSE, the output variable changes to FALSE. • 1 If the input variable changes to FALSE, the output variable changes to TRUE. You can edit the expected value settings by importing or exporting the values, and copying and pasting the values with a spreadsheet program or any other application software.	

Setting Example

This section provides an example of automatic programming settings for the application example given in *A-4-3 Safety Laser Scanners* on page A-36.

Application Overview of Safety Laser Scanner

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 3/PLd	Safety Laser Scanner	0	Auto
	Emergency Stop Pushbutton Switch	0	Manual

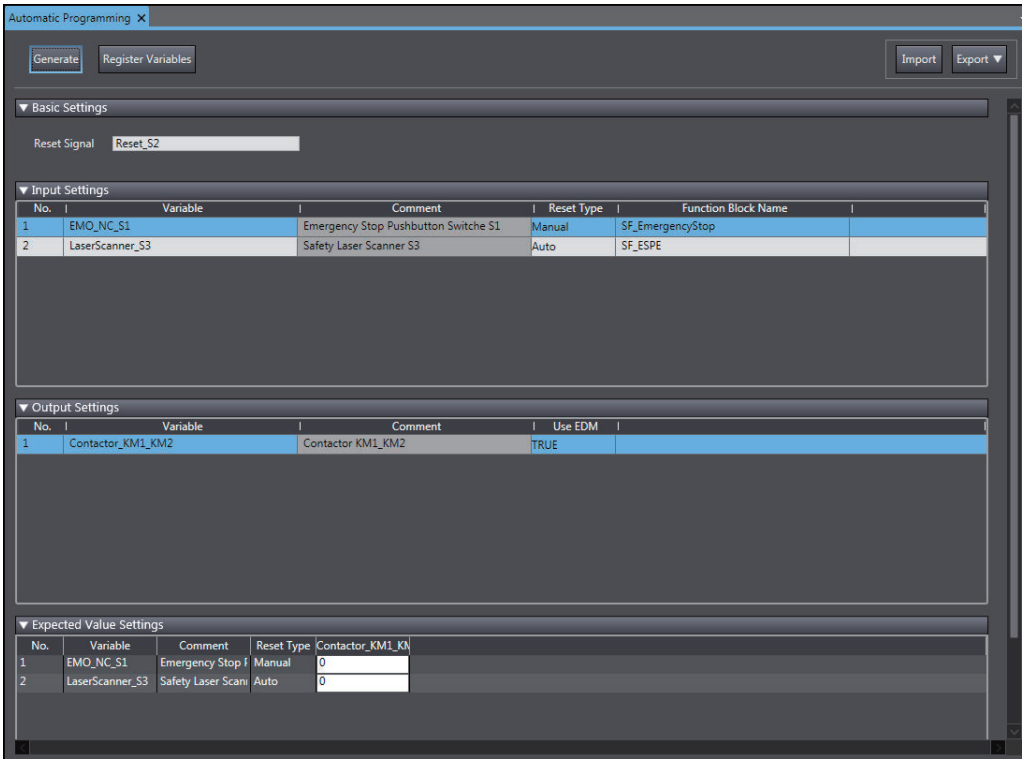
AGV stops when the emergency stop pushbutton S1 is pressed.

AGV stops also when the safety laser scanner detects someone or an object approaching to the safety zone.

At that time, enter the following variables of the safety laser scanner on the Automatic Programming Setting Tab Page.

- Variable that is assigned to the reset switch
- Variables that are assigned to the safety laser scanner and the Emergency stop pushbutton
- Variables that are assigned to contactors

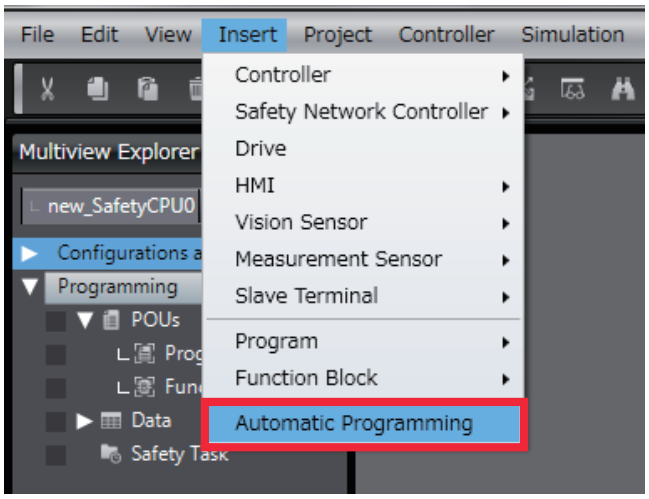
The settings for the above application example are configured in the Automatic Programming Settings Tab Page as shown below.



8-6-3 Automatic Programming Execution Procedure

The execution procedure of automatic programming is explained below.

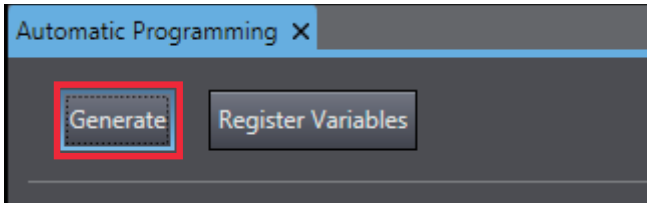
1 Select **Insert - Automatic Programming**.



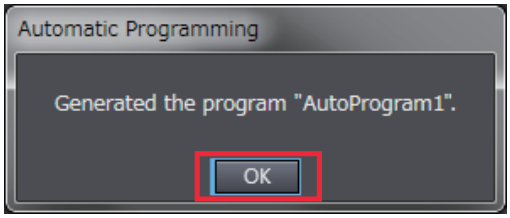
The Automatic Programming Settings Tab Page is displayed.

2 Set **Basic Settings**, **Input Settings**, **Output Settings**, and **Expected Value Settings**.

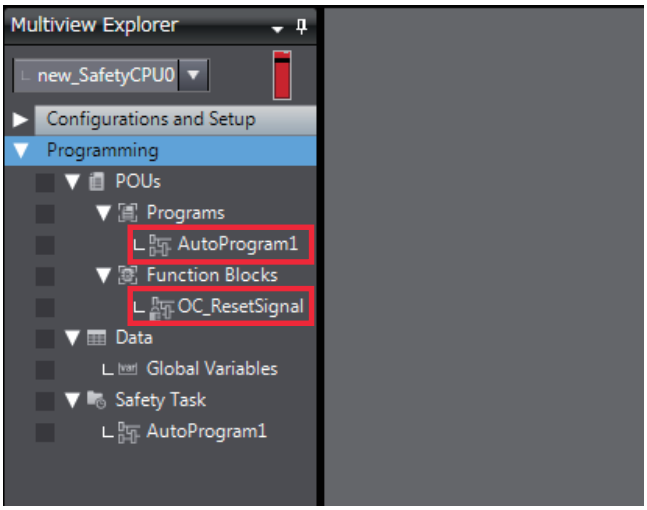
3 On the operation panel of the Automatic Programming Settings Tab Page, click the **Generate** Button.



Once a program is generated, the following dialog is displayed.

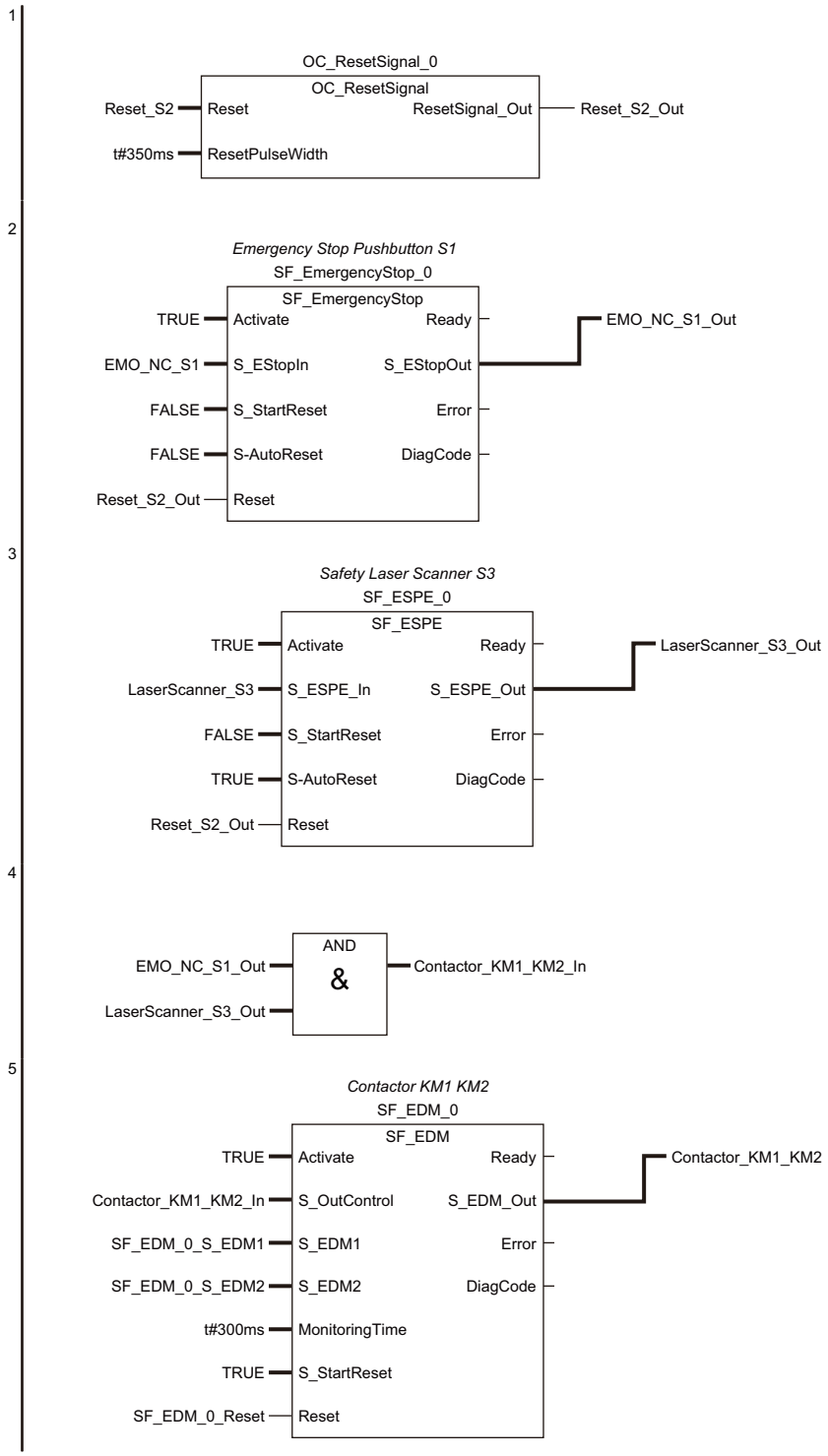


4 Click the **OK** Button.
Once a program is generated, a safety program generated based on the settings and a function block (OC_ResetSignal) used to identify the reset signal are added to the project.



Program Generated through Automatic Programming

Based on the example settings provided in *8-6-2 Automatic Programming Settings* on page 8-90, the following program will be generated.



Additional Information

You can also manually add the function block (OC_ResetSignal) used to identify the reset signal in the following procedure.

- Right-click **Function Blocks** under **Programming** – **POUs** in the Multiview Explorer and select **Import OC ResetSignal** from the menu.

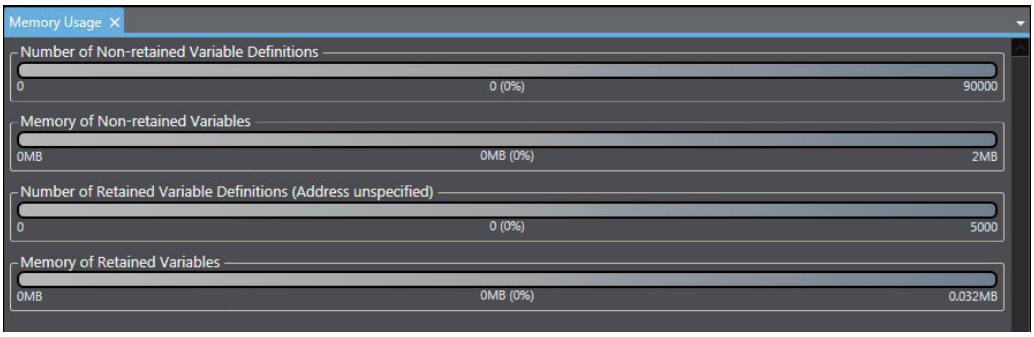
8-7 Monitoring Memory Usage for Communication Control Unit

This monitor shows the estimated memory usage for variables you are editing in Sysmac Studio. If the size of variables exceeds the memory size, transferring the variables to the Communication Control Unit generates an error in the Communication Control Unit.

Displaying Memory Usage

Use the following procedure to display memory usage.

Select Communication Control Unit from the Controller Selection Box in the Multiview Explorer to open the **Communication Control Unit Setup and Programming** View.
Select **Memory Usage** from the **Project** Menu.
The Memory Usage Tab Page is displayed.



Item	Display content
Number of Non-retained Variable Definitions	It is the number of non-retained variables used.
Memory of Non-retained Variables	It shows the memory usage for non-retained variables.
Number of Retained Variable Definitions (Address unspecified)	It shows the number of retained variables used without address specified.
Memory of Retained Variables	It shows the memory usage for retained variables.

8-8 Monitoring Memory Usage for Safety Control Unit

You can display the memory usage of the safety control system and the safety network usage including the I/O data size.

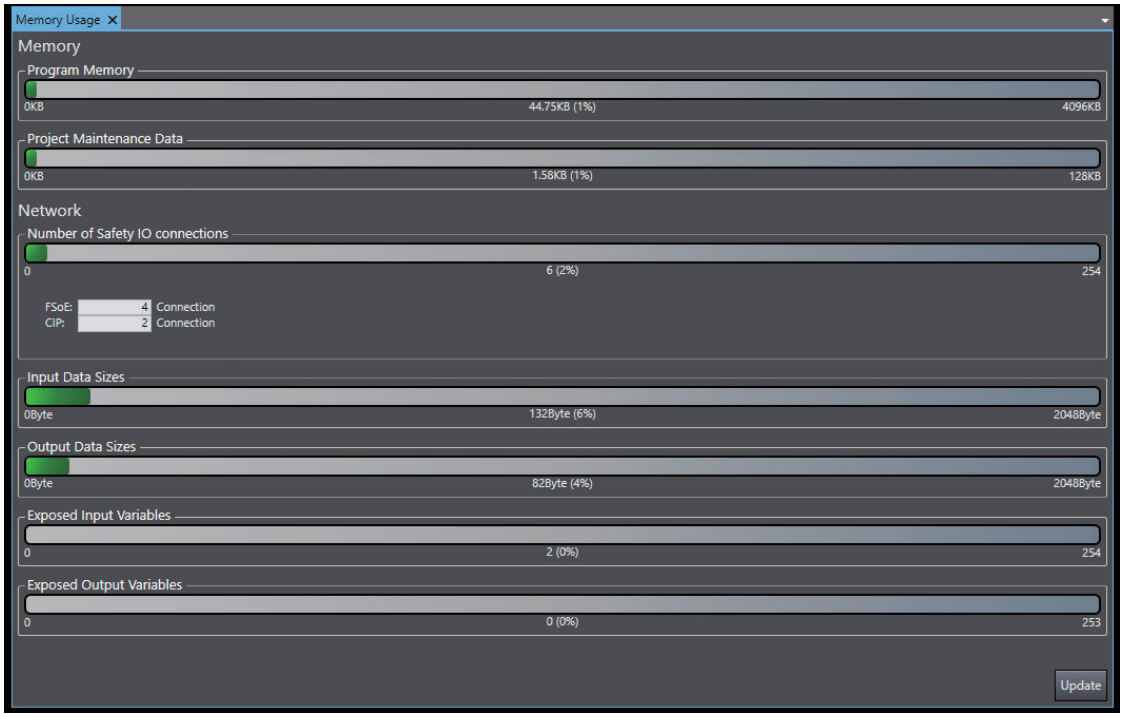
Precautions for Correct Use

Check the memory usage when there are no building errors. If there is a building error, the memory usage is not displayed correctly.

Displaying Memory Usage

Use the following procedure to display memory usage.

Select the Safety CPU Unit from the Controller Selection Box in the Multiview Explorer and open the **Safety CPU Unit Setup and Programming** View.
Select **Memory Usage** from the **Project** Menu.
The Memory Usage Tab Page is displayed.



Item	Display content	Related parameters
Program Memory	Displays the memory usage of the safety program.	• Number of the connected Safety I/O Units • Number of CIP Safety connections, number of target I/O Assemblies • Number of functions blocks and functions in the safety program • Number of exposed variables, global variables and device variables • Comment sizes for exposed variables, global variables, and device variables • Function block names • Number of device settings in the Safety Slave Unit parameter settings • Terminal comments in the parameters for Safety Slave Units
Project Maintenance Data	Displays the memory usage of the project.	• Program names • Number of exposed variables • Comment sizes for exposed variables, global variables, and device variables • Number of device settings in the Safety Slave Unit parameter settings • Terminal comments in the parameters for Safety Slave Units
Number of Safety I/O connections	Displays the number of safety slaves connected to the Safety CPU Unit. **FSoE** shows the number of connections with Safety I/O Units. **CIP** shows the number of CIP Safety connections.	• Number of the connected Safety I/O Units • Number of CIP Safety connections, number of target I/O Assemblies
Input Data Sizes	Displays the input data usage by the Safety CPU Unit.	• Number of the connected Safety I/O Units • Number of CIP Safety connections • Data size of the exposed variables used for input settings
Output Data Sizes	Displays the output data usage by the Safety CPU Unit.	• Number of the connected Safety I/O Units • Number of CIP Safety connections • Data size of the exposed variables used for output settings
Exposed Input Variables	Displays the number of exposed variables in the input settings.	Number of exposed variables used for input settings
Exposed Output Variables	Displays the number of exposed variables in the output settings.	Number of exposed variables used for output settings

8-9 Offline Debugging

Offline debugging allows you to debug a program when you are not connected online to a Safety CPU Unit.
You can debug on a Simulator to check control program logic before transferring the project to the Safety CPU Unit.

⚠ WARNING

Although the Simulator simulates the operation of the Safety CPU Unit, there are difference from the Safety CPU Unit in operation and timing. After you debug the safety program on the Simulator, always check operation on the physical Safety CPU Unit before you use the user program to operate the controlled system.
Accidents may occur if the controlled system performs unexpected operation.



Additional Information

Refer to *A-16 Differences in Checking Operation between the Simulator and Safety CPU Unit* on page A-108 for the differences between the Safety CPU Unit and the Simulator.

8-9-1 Offline Safety Program Debugging

To debug a safety program, it is best to simulate the safety program on the computer first to check the operation logic and parameter settings.
This is called offline debugging.

Simulation Procedures

Use the following procedure to start the Sysmac Studio and connect to the Simulator.

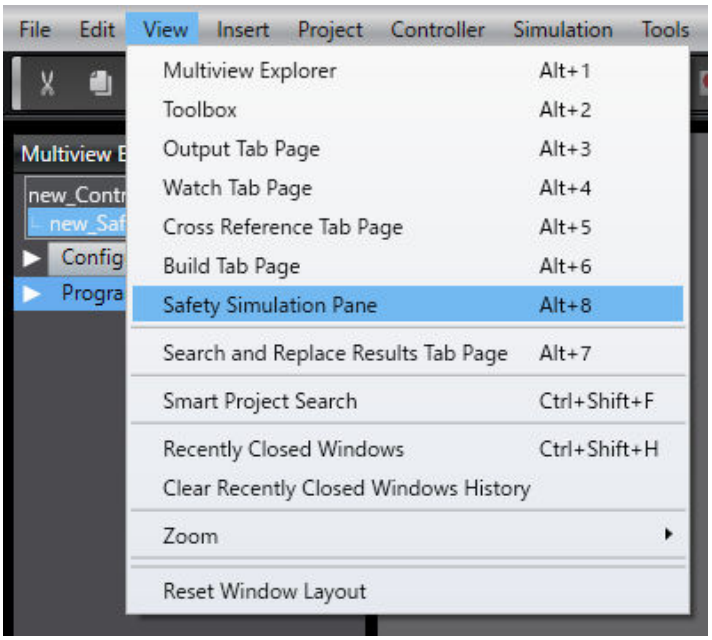
1. Start the Sysmac Studio and create a project.
2. In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.
3. Use the Sysmac Studio to set the Controller Configurations and Setup and create a safety program.
4. Select **Build Controller** from the **Project** Menu to build the program.



Additional Information

You cannot connect to the Simulator if the program is not built.

5. Select **Safety Simulation Pane** from the **View** Menu.



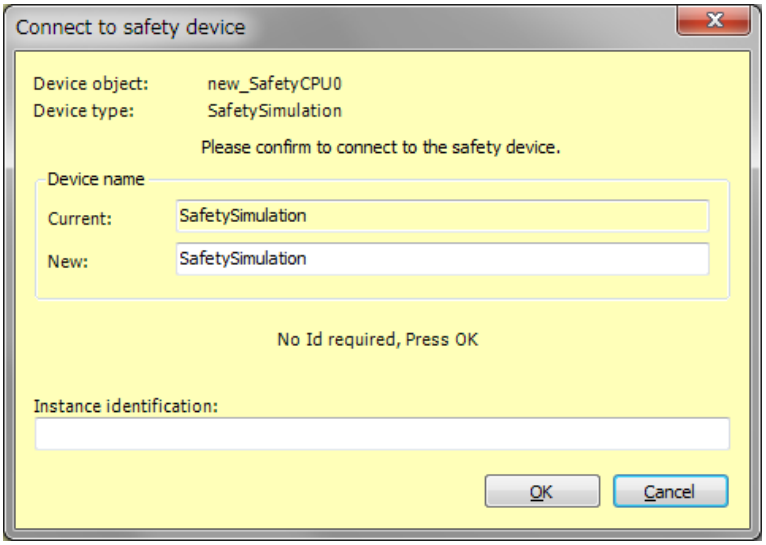
The Safety Simulation Pane is displayed below the Toolbox Pane on the right of the window.



6 Click the **Run** Button in the Safety Simulation Pane. Or, select **Run** from the **Simulation** Menu.

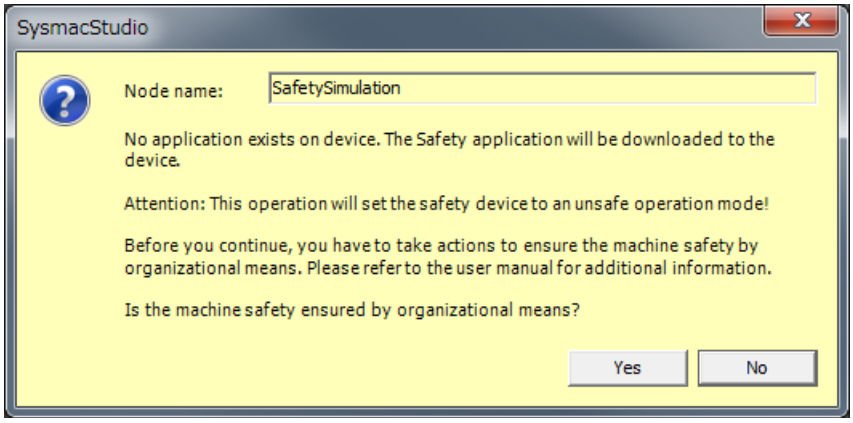


The following Connect to safety device Dialog Box is displayed.



Note 1. It is not necessary to change the name from the current node name.
Note 2. You do not need to enter anything in the **Instance identification** Box.

7 Click the **OK** Button.
The following transfer confirmation dialog box is displayed.

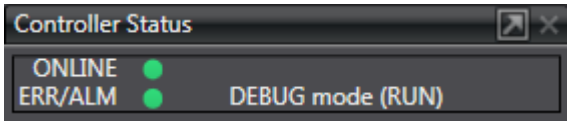


8 Click the **Yes** Button.
The following device confirmation dialog box is displayed.



9 Click the **OK** Button.
Note You do not need to enter anything in the **Password** Box.

10 After the Simulator is started and connected, the Online Indicator in status monitor is lit green.
In this status, the project is completely transferred to the Simulator and RUN mode continues.



11 To stop the simulation, click the **Stop** Button in the Safety Simulation Pane.



12 To end the simulation, click the Close Button **x** in the Safety Simulation Pane.
The values of variables return to their initial values.

Pausing

Use the following procedure to pause a simulation.



The values of variables are retained.
Program execution stops at the start of the program.

8-9-2 Monitoring

You can monitor the present values of variables in the FBD editor or Watch Tab Page to debug the safety programs.

Refer to *9-6-3 Monitoring Variables in the FBD Editor* on page 9-23 and *9-6-4 Monitoring Variables in a Watch Tab Page* on page 9-24 for details.

8-9-3 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing

You can debug the safety program by controlling BOOL variables (Set/Reset), changing present values, and executing forced refreshing from the Sysmac Studio.

Refer to *9-6-5 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing* on page 9-26 for detailed procedures.

8-9-4 Cross References

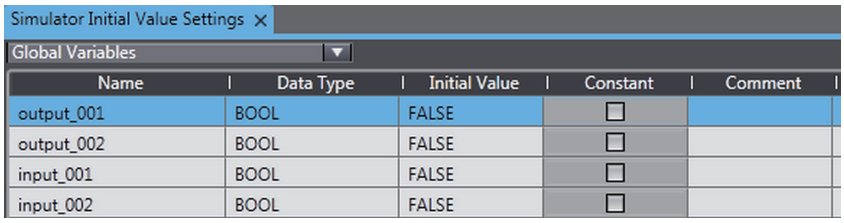
Cross references allow you to see the programs and locations where variables of the safety program are used.
Refer to *9-6-6 Cross References* on page 9-34 for a detailed procedure.

8-9-5 Setting the Initial Values of Variables

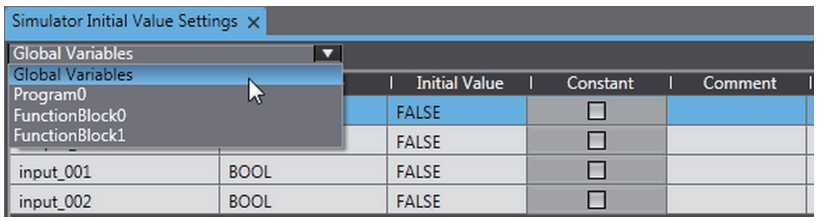
You can set the initial values of variables when you start execution of simulation.
This is useful for reproducing the actual conditions of the system or to evaluate test cases of similar input conditions.
Simulation must be stopped to set the initial values of variables.

Use the following setting procedure.

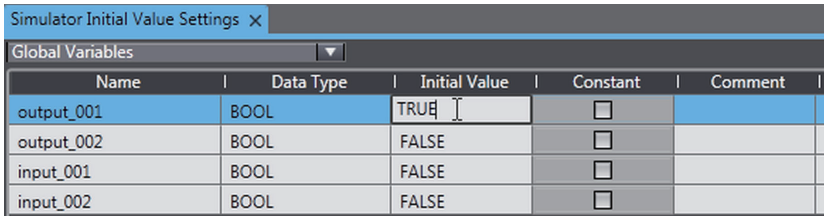
1 Select **Simulation** – **Initial Value Settings**.
The Initial Value Settings Dialog Box is displayed.



2 Select the type of variables.
The selected type of variables is displayed. The following types of variables can be selected: global variables, programs, and function blocks.



3 Change the initial values of the variables.

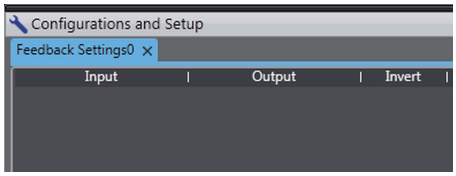


8-9-6 Feedback Settings

You can set input status that is linked to changes in output status, such as feedback inputs for safety relays.
Simulation must be stopped to make the feedback settings.

Use the following setting procedure.

1 Select **Simulation** – **Feedback Settings**.
The Feedback Setting Dialog Box is displayed.

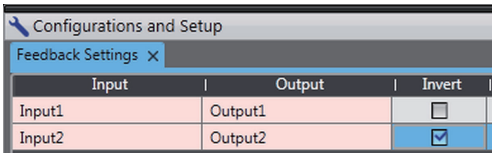


Item	Description	Supported variable types
Input	Set a global variable that is the destination of the feedback. You cannot set a variable that is already set as a feedback destination.	BOOL, SAFEBOOL
Output	Set the global variable that is the source of the feedback.	BOOL, SAFEBOOL

Item	Description	Supported variable types
Invert	This check box is used to invert the input value. If you select this check box, the input value is inverted.	---

2 Press the **Insert** Key in the feedback setting table, or right-click in the feedback setting table and select **Create New** from the menu.
Cells are added for new settings.
You can set up to 128 sets of feedback settings.

3 Set the input source variable and the output destination variable, and if necessary, select the Invert Check Box.
The feedback settings are applied within a maximum of 300 ms.



Precautions for Correct Use

When you use the feedback settings on the Simulator, set **MonitoringTime** in the SF_EDM instruction 300 ms or more.
Make sure to return the setting to the original value when you transfer the program to the physical Safety CPU Unit.

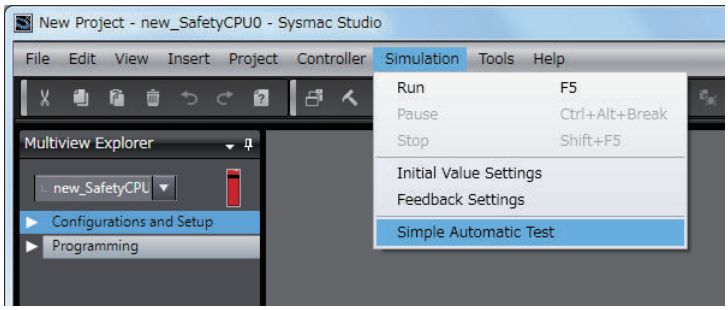
8-9-7 Simple Automatic Test

You can use the Simulator of the Safety CPU Unit to easily confirm if the input signals to the program produce the expected output signal values.

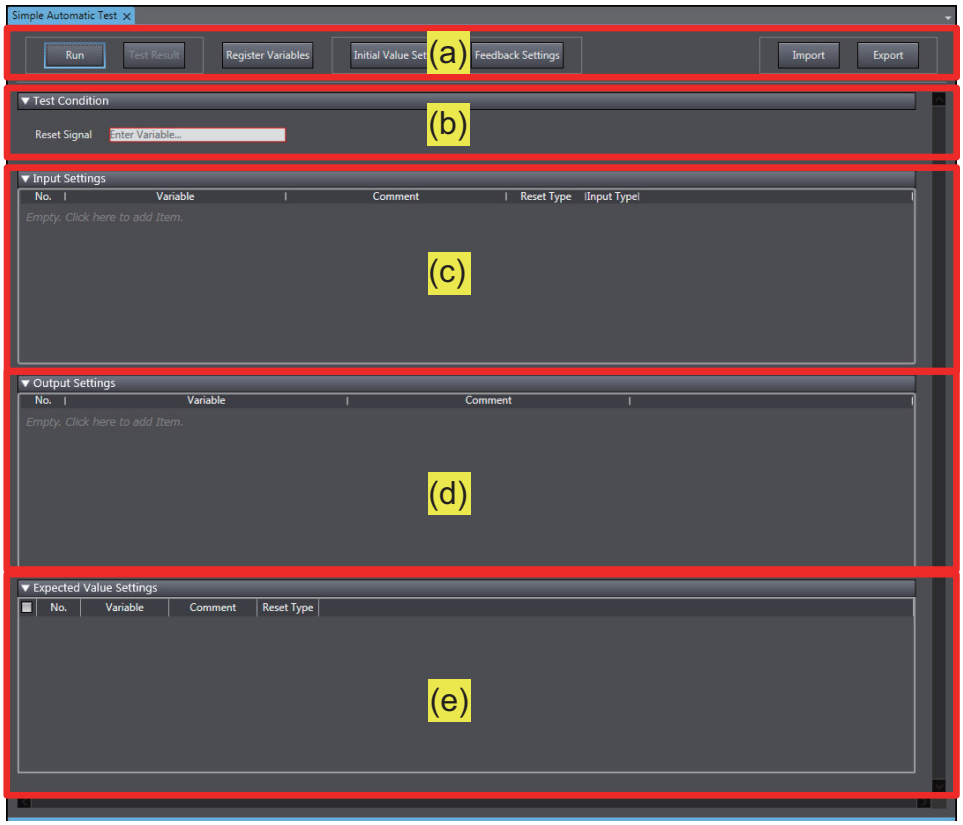
Settings for a Simple Automatic Test

The Simple Automatic Test automatically executes offline debugging operations for safety programs. To use the Simple Automatic Test, set the reset signal, input signals, and output signals, as well as the expected values of the output signals based on the input signals.
Execute the Simple Automatic Test after you have created the program. Also, set initial values and feedback settings if they are necessary.

Select **Simulation** - **Simple Automatic Test** from the menu to display the setting areas for a Simple Automatic Test.



The following Simple Automatic Test Tab Page is displayed.



The setting areas of the Simple Automatic Test are configured as described in the following table.

Item	Name	Function	
(a)	Simple Automatic Test Operation Panel	The operation panel is used to make settings for and execute the Simple Automatic Test. You can perform the following operations.	
		Run Button	Executes the Simple Automatic Test.
		Test Result Button	Shows the previous test results for the Simple Automatic Test.
		Register Variables Button	Used to register the variables that are used for the Simple Automatic Test.
		Initial Value Settings Button	Displays the Initial Value Settings Dialog Box.
		Feedback Settings Button	Displays the Feedback Settings Dialog Box.

Item	Name	Function	
		Import Button	Imports the settings for a Simple Automatic Test from a CSV file. If you import the settings, the current settings are overwritten.
		Export Button	Exports the current settings for the Simple Automatic Test to a CSV file.
(b)	Test Condition Area	Select the variable to use as a reset signal for the safety program. You can set any SAFEBOOL or BOOL variable that is defined in the global variable table.	
(c)	Input Setting Area	Set the variables of the input signals to use in the Simple Automatic Test. In addition to the variable name, set the reset types and input types of the input signals.	
		Variable	Set the names of the variables used as the input signals in the program. You can set any SAFEBOOL or BOOL variable that is defined in the global variable table.
		Reset Type	Select the reset type in the box. The default value of the reset time is a manual reset. • Manual If a manual reset is used for an input signal, a test is executed for the manual reset scenario that uses the reset signal set in the *Test Condition Area (b)*. • Auto If an automatic reset is used for an input signal, a test is executed according to the auto reset scenario.
		Input Type	To set a test for two input signals, such as for a safety door or two-hand switches, set the input type to **2 Inputs**. If you set the input type to **2 Inputs**, a row is added to specify another variable.
(d)	Output Setting Area	Set the variables of the output signals to use in the Simple Automatic Test. You can set any SAFEBOOL or BOOL variable that is defined in the global variable table.	
(e)	Expected Value Setting Area	A matrix of the variables that are specified in the input settings and output setting areas is displayed. Set the test target and the expected value of the output variable for each input variable. The expected values that you set for the output variables have the following meanings: • 0: If the input variable changes to FALSE, the output variable changes to FALSE. • 1: If the input variable changes to FALSE, the output variable changes to TRUE. You can import and export expected value settings to use spreadsheets or other applications to easily edit the settings by copying and pasting them.	

Setting Example

A setting example for the Simple Automatic Test is provided in this section for the application example given in *A-4-2 Safety Doors* on page A-32.

Application Overview from *A-4-2 Safety Doors* on page A-32 is as follows.

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe (Safety Door)	Safety limit switches 1 and 2	0	Auto
	Emergency stop pushbutton	0	Manual

M1 stops when safety door 1 (S3, S4) is opened.
M2 stops when safety door 2 (S5, S6) is opened.
Both M1 and M2 stop when the emergency stop pushbutton S1 is pressed.

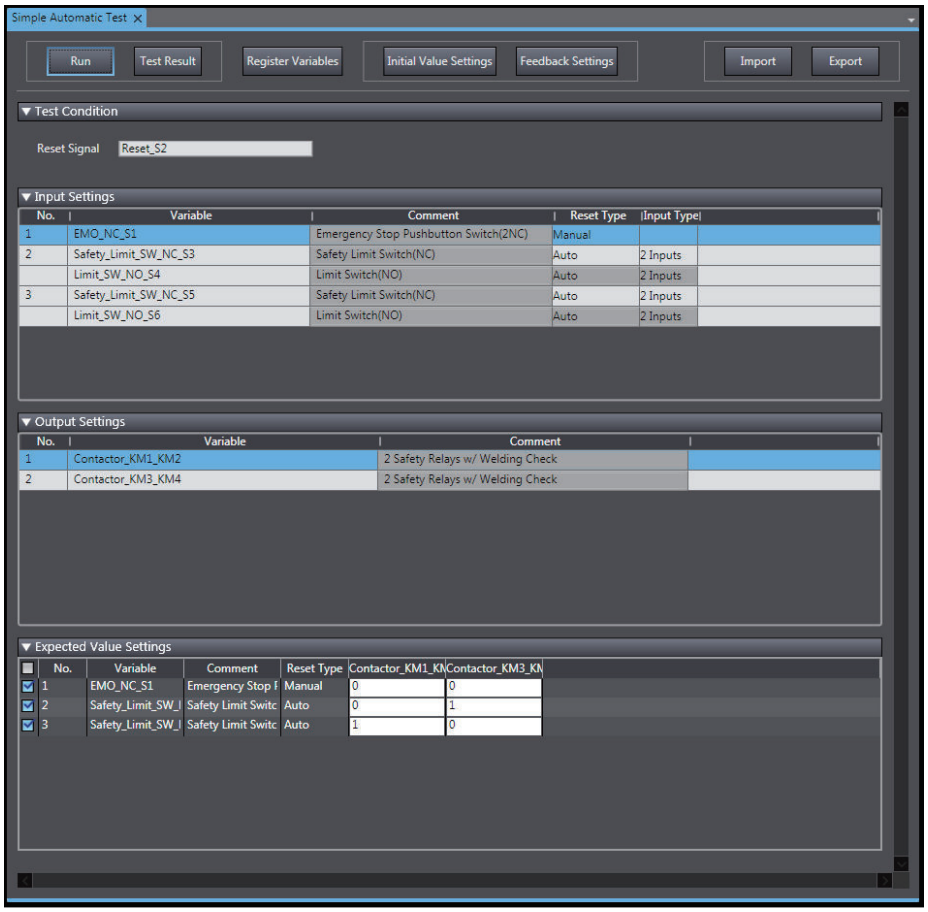
The settings for the Simple Automatic Test are derived from the following points.

- Variable that is assigned to the reset switch
- Variables that are assigned to safety input devices (except for EDM feedback)
- Variables that are assigned to safety output devices

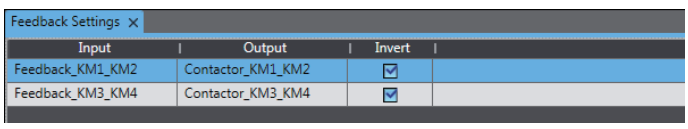
Note 1. To make the program work correctly, set the initial values for simulation so that Activate terminal on the safety function block will be to TRUE.

Note 2. To make the SF_EDM function block work correctly, set feedback for simulation.

The settings for the above application are shown in the setting areas for the Simple Automatic Test.



Feedback Settings Tab Page is shown below.



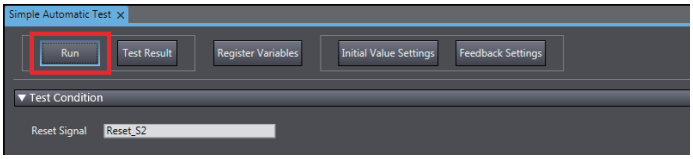
Execution Procedure for a Simple Automatic Test

Use the following procedure to execute the Simple Automatic Test.

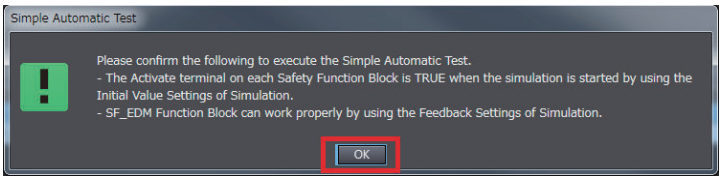
1 Select **Simulation** - **Simple Automatic Test** from the menu.
The Simple Automatic Test Tab Page is displayed.

2 Set the **Test Condition**, **Input Settings**, **Output Settings**, and **Expected Value Settings**.

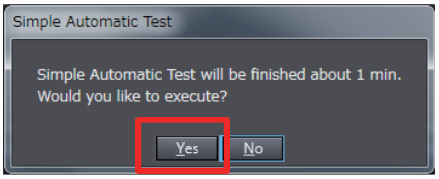
3 Click the **Run** Button on the control panel on the Simple Automatic Test Tab Page.



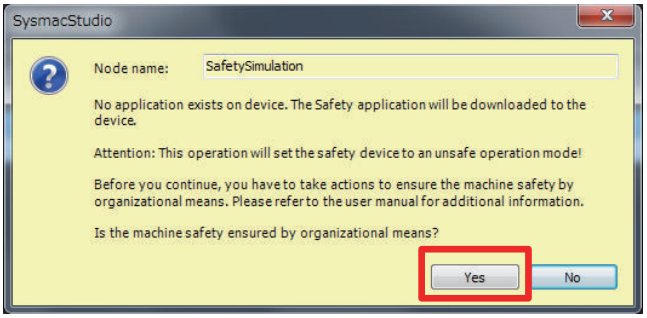
4 A precaution is displayed to ensure proper execution of the Simple Automatic Test. Read the precaution and then click the **OK** Button.



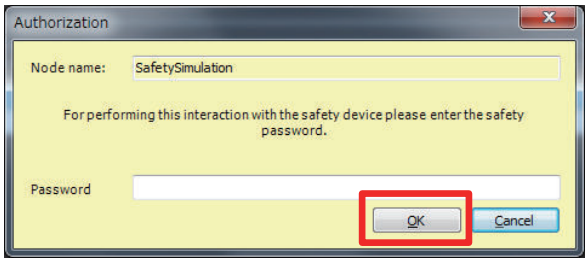
5 The estimated execution time for the Simple Automatic Test is displayed. Click the **Yes** Button to execute the test.



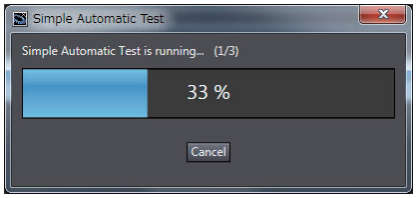
6 The Simulator for the Safety CPU Unit starts. Following the on-screen instructions to complete starting the Simulator.
Click the **Yes** Button.



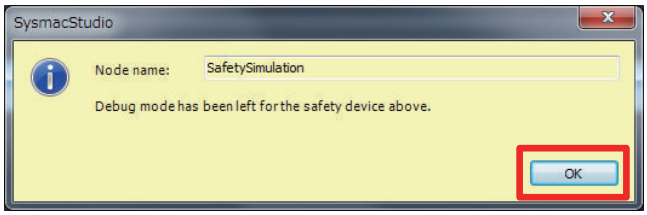
Click the **OK** Button.



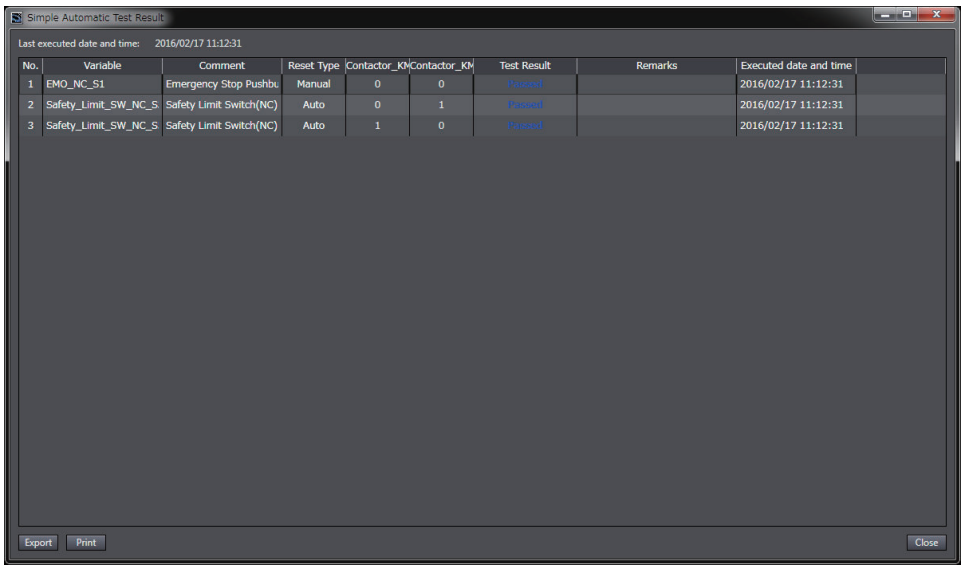
You can check the progress of the Simple Automatic Test in the following dialog box.



The Simulator stops when the test is completed. Click the **OK** Button.



7 The Simple Automatic Test Result Window is displayed when the test is completed. If the results show that the test has failed, correct the safety program or check the test settings.



Precautions for Correct Use

The Simple Automatic Test is provided as a simple means to check the output signal results for the input signals. It may not be able to determine correct test results for complicated conditions or special cases. If necessary, check the program logic manually.

Additional Information

The actual test operations that are performed for the Simple Automatic Test are given in *A-15 Execution Scenarios for the Simple Automatic Test* on page A-105.

9

Checking Operation and Actual Operation

This section describes the procedures to perform before you can operate the Safety Network Controller. It describes the operating modes of the Safety CPU Unit, checking operation in DEBUG mode, and the procedures to perform safety validation.

9-1 Procedures before Operation and Transferring the Required Data 9-3
9-1-1 Commissioning Procedure 9-3
9-1-2 Data That You Must Transfer before Operation and Data Transfer Procedures 9-4

9-2 Transferring the Configuration Information 9-6
9-2-1 Overview 9-6
9-2-2 Transfer Procedure 9-6

9-3 Operating Modes of the Safety CPU Unit 9-8
9-3-1 Startup Operating Mode and Changing the Operating Mode 9-8
9-3-2 Operation When Changing Operating Mode 9-10
9-3-3 Executable Functions in Each Mode of the Safety CPU Unit 9-11

9-4 Changing to DEBUG Mode 9-13

9-5 Checking External Device Wiring 9-16
9-5-1 Overview of Functions for Checking Wiring 9-16
9-5-2 Monitoring Safety I/O Units 9-16
9-5-3 Troubleshooting Safety I/O Terminals 9-19
9-5-4 Clear All Memory Operation for Safety I/O Units 9-20

9-6 Functions for Checking Operation 9-22
9-6-1 Overview of Functions for Checking Operation 9-22
9-6-2 Starting and Stopping the Safety Programs in DEBUG Mode 9-22
9-6-3 Monitoring Variables in the FBD Editor 9-23
9-6-4 Monitoring Variables in a Watch Tab Page 9-24
9-6-5 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing 9-26
9-6-6 Cross References 9-34

9-7 Online Functional Test 9-38
9-7-1 Online Functional Test Settings 9-38
9-7-2 Online Functional Test Execution Procedure 9-42

9-8 Search FB Where Safety Output Is OFF 9-48
9-8-1 Procedure for Operating Search FB Where Safety Output Is OFF 9-48
9-8-2 Editing Function Blocks to be Searched for 9-49
9-8-3 Registering a Data Type in the Function Block Search Settings Window 9-50

9-9 Node Name 9-52

9-10 Security Settings 9-53
9-10-1 Setting the Safety Password 9-53
9-10-2 Data Protection 9-54

9-11 Performing Safety Validation and Operation 9-59
9-11-1 Performing Safety Validation 9-59
9-11-2 Changing to RUN Mode 9-61
9-11-3 Changing to PROGRAM Mode 9-62

9-12 Starting and Stopping the Safety Application Monitoring 9-64
9-12-1 Procedure to Start and Stop the Safety Application Monitoring 9-64
9-12-2 Changing the Monitoring Options for the Safety Application 9-65

9-13 Uploading Configuration Information and Safety Application Data 9-66
9-13-1 Outline 9-66
9-13-2 Upload Procedures 9-66

9-14 Transferring Safety Application Data 9-68
9-14-1 Outline 9-68
9-14-2 Transfer Procedure 9-68

9-15 Monitoring Controller Status 9-70

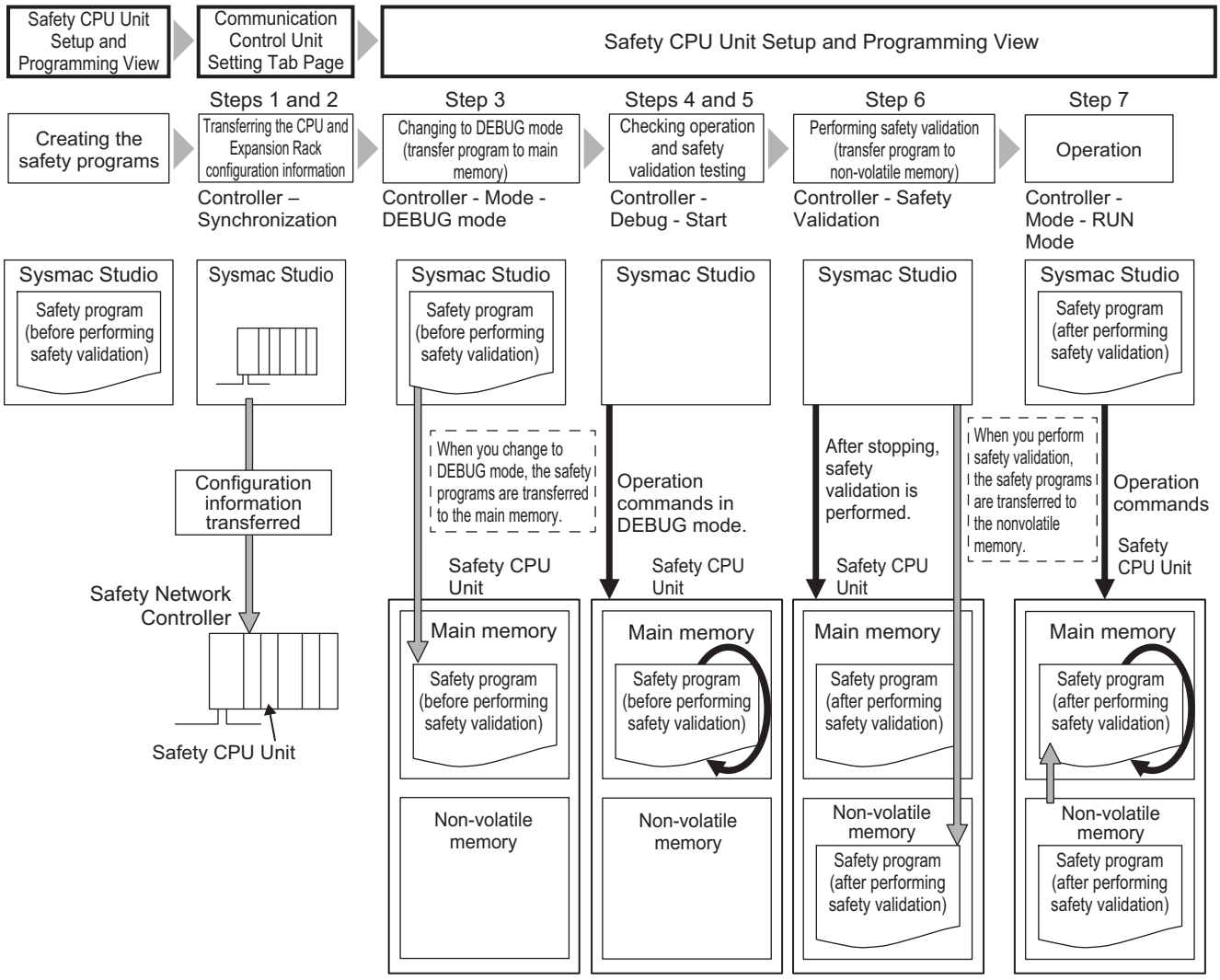
9-16 Restarting and Clearing All Memory 9-72
9-16-1 Restarting 9-72
9-16-2 Clear All Memory Operation 9-72

9-1 Procedures before Operation and Transferring the Required Data

9-1-1 Commissioning Procedure

After you write the safety programs, use the following procedure to start operating the Safety Network Controller.

1. Place the Sysmac Studio online with the Communication Control Unit.
2. Transfer the configuration information to the Communication Control Unit and Safety CPU Unit.
   The rest of the procedure is not required when you transfer validated safety application data.
   After you transfer safety-validated safety application data, use the safety signature displayed by the Sysmac Studio to confirm that the correct data is transferred.
3. Place the Safety CPU Unit in DEBUG mode.
   The safety programs are transferred to the main memory of the Safety CPU Unit.
4. Check the wiring and the operation of the safety programs.
5. Perform a safety validation testing.
6. Execute safety validation from the Sysmac Studio.
   The safety programs are transferred to the non-volatile memory of the Safety CPU Unit to enter the safety-validated status.
7. Place the Safety CPU Unit in RUN mode.
   The safety programs in the non-volatile memory of the Safety CPU Unit are executed.



9-1-2 Data That You Must Transfer before Operation and Data Transfer Procedures

Before you change to RUN mode, you must transfer the Safety Network Controller settings, including the Safety Control Unit settings, to the Unit. The settings and transfer procedures are given below.

Safety Network Controller Settings		Transfer method	Transfer destination
		When connected to Communication Control Unit	
CPU and expansion rack configuration information	Unit configuration information	Perform the following operation on the Communication Control Unit Settings Tab Page: Transfer the CPU and Expansion Rack configuration information from the Synchronization Window.	Communication Control Unit
	I/O allocation information		Communication Control Unit and Safety CPU Unit

Safety Network Controller Settings		Transfer method	Transfer destination
		When connected to Communication Control Unit	
Safety application data	Unvalidated safety application data	The safety application data is transferred automatically when you change to DEBUG mode from the Safety CPU Unit Setup and Programming View.	Safety CPU Unit
	Validated safety application data	In DEBUG mode, execute **Safety Validation** from the Safety CPU Unit Setup and Programming View. This will save the safety application data to the non-volatile memory, and the data is validated.	
		Perform the following operation on the Communication Control Unit Settings Tab Page: Transfer the CPU and Expansion Rack configuration information from the Synchronization Window.	

9-2 Transferring the Configuration Information

This section describes how to start communications and transfer configuration information from the Sysmac Studio to the Communication Control Unit and the NX-series Safety CPU Unit.

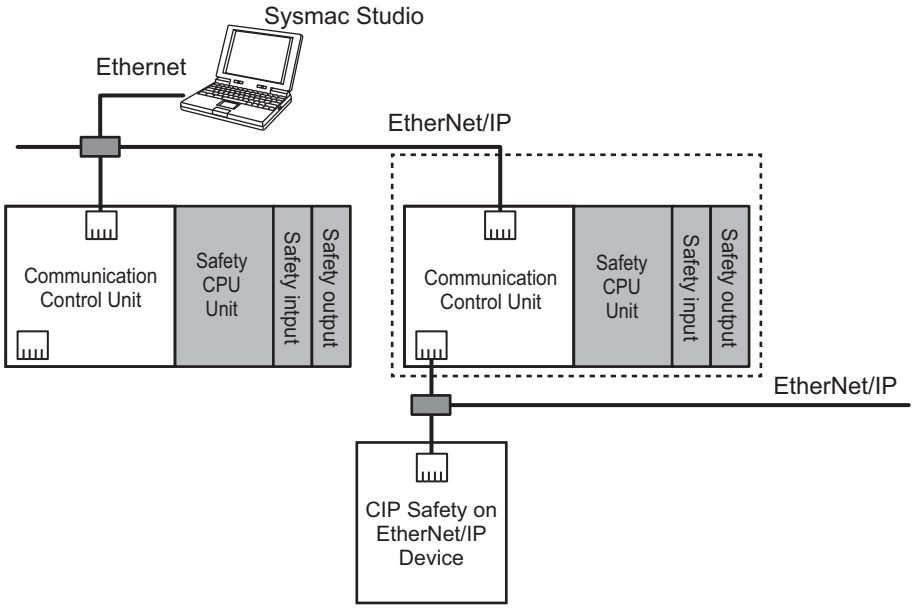
9-2-1 Overview

By transferring the CPU and Expansion Racks configuration information to the Communication Control Unit and Safety CPU Unit, you can connect the Sysmac Studio and Safety CPU Unit online and perform debugging.

Paths for Going Online

Connect the Sysmac Studio online to the Safety CPU Unit via a Ethernet connection with the Communication Control Unit.

A configuration example is given below.



⚠ WARNING

Always confirm safety at the destination node before you transfer Unit configuration information, parameters, settings, or other data from tools such as the Sysmac Studio. The devices or machines may operate unexpectedly, regardless of the operating mode of the Controller.

9-2-2 Transfer Procedure

You can transfer the configuration information by connecting the Sysmac Studio to an Ethernet port on the Communication Control Unit.

To go online with the Safety CPU Unit, use the following procedures.

1. Select the Communication Control Unit from the Controller Selection Box in the Multiview Explorer of Sysmac Studio, and open the Communication Control Unit Setup and Programming View.
2. Set the communications path to the Communication Control Unit.
3. Select **Online** from the **Controller** Menu. Or, click the Go Online Button () in the toolbar.
4. Select **Synchronization** from the **Controller** Menu.
5. Click the **Transfer to Controller** Button*1.
   The Sysmac Studio is enabled for communications with the Safety CPU Unit. The CPU and Expansion Rack configuration information is transferred to the Communication Control Unit and Safety CPU Unit.
   *1. Always click this button when you go online with the Safety CPU Unit for the first time, or when you change the Safety I/O Units or variable data.

Additional Information

- Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for information on connecting and synchronizing with the Communication Control Unit.
- Refer to *9-4 Changing to DEBUG Mode* on page 9-13 for details on transferring the unvalidated safety program.

9-3 Operating Modes of the Safety CPU Unit

This section describes the operating modes of the Safety CPU Unit, state changes, and the functions that can be executed in each mode.

9-3-1 Startup Operating Mode and Changing the Operating Mode

The operating mode of the Safety CPU Unit changes to PROGRAM mode or RUN mode after the power is turned ON, depending on whether the safety programs are validated, as shown in the following figure.

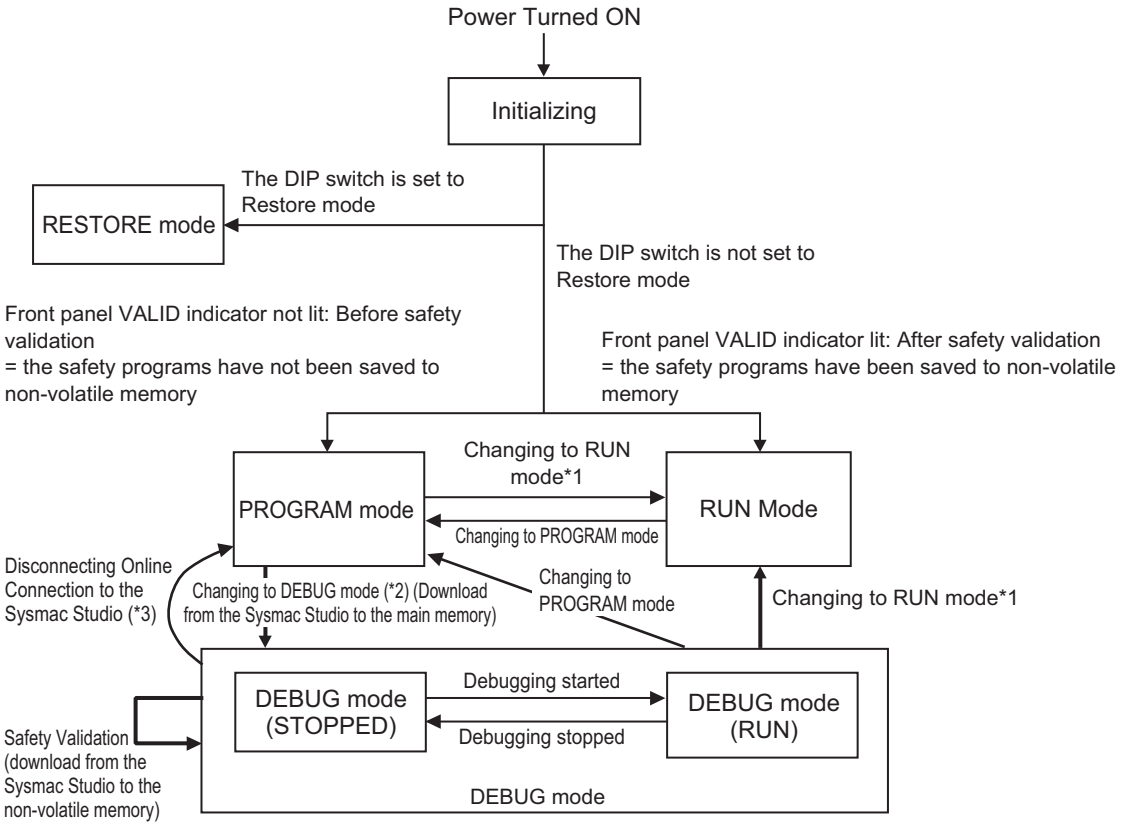
● Before Safety Validation

The Safety CPU Unit starts in PROGRAM mode. This prevents the Safety CPU Unit from running a safety application that has not been validated for safety.

● After Safety Validation

The Safety CPU Unit starts in the RUN mode.

To change the operating mode of the Safety CPU Unit, select the Safety CPU Unit as the Controller and place the Sysmac Studio online with the Safety CPU Unit, and then select the desired operating mode.



*1. The Safety CPU Unit can be operated only after safety validation is performed.

*2. When the operating mode changes from PROGRAM mode to DEBUG mode, the safety application data in the non-volatile memory of the Safety CPU Unit is deleted.
*3. The Safety CPU Unit automatically enters PROGRAM mode if 30 seconds elapses after the connection to the Sysmac Studio is disconnected due to a damaged cable or any other reason.



Additional Information

If you need to use debugging to change present values or other settings while operating in RUN mode (for instance, to troubleshoot a validated safety program), you must stop the machine, and then change the Safety CPU Unit to PROGRAM mode before you can change to DEBUG mode. However, when the operating mode changes from PROGRAM mode to DEBUG mode, the safety programs in the non-volatile memory of the Safety CPU Unit is deleted. Download the safety-validated safety programs to the non-volatile memory in the Safety CPU Unit again.

Operating Modes of Safety CPU Unit and Indicators

The following table specifies details of the Safety CPU Unit operating modes and the indicators displayed for each operating mode.

Operating mode		Description	Indicators	
			RUN	DEBUG
Initializing		This mode indicates that the Safety CPU Unit is starting up and performing hardware self-diagnosis.	Flashing green.	Not lit
PROGRAM mode		This mode indicates that safety communications and the safety program execution are stopped. You can clear or download the safety application data from the Sysmac Studio (Safety CPU Unit Setup and Programming View).	Not lit	Not lit
RUN mode		This mode indicates that safety communications are executed and the validated safety programs are running.	Lit green	Not lit
DEBUG mode	STOPPED	This mode indicates that safety communications are executed and the unvalidated safety programs are on standby. You can control BOOL variables, change present values of data, and use forced refreshing.	Not lit	Lit yellow
	RUN	This mode indicates that safety communications are executed and unvalidated safety programs are running. You can control BOOL variables, change present values of data, and use forced refreshing.	Lit green	Lit yellow
RESTORE mode		This mode allows you to edit user programs and settings of the Safety CPU Unit by using an SD Memory Card. Safety communications and safety programs are not executed.	Flashing green.	Flashing yellow

I/O Data in Each Operating Mode

The following table explains how I/O data is processed, depending on the operating mode of the Safety CPU Unit.

Not received = Not receive data, Cleared = Clear and reset to initial value, Refreshed = Refresh data

Operating mode		Safety Input (FSoE/CIP Safety)	Standard Input (Exposed Variable)	Safety Output (FSoE/CIP Safety)	Standard Output (Exposed Variable)	Status (Safety CPU Status)
Initializing		Not received	Not received	Cleared	Cleared	Cleared
PROGRAM mode		Not received	Not received	Cleared	Cleared	Refreshed
RUN mode		Refreshed	Refreshed	Refreshed	Refreshed	Refreshed
DEBUG mode	STOPPED	Refreshed	Refreshed	Refreshed	Refreshed	Refreshed
	RUN	Refreshed	Refreshed	Refreshed	Refreshed	Refreshed
RESTORE mode		Not received	Not received	Cleared	Cleared	Cleared

9-3-2 Operation When Changing Operating Mode

If you change the operating mode of the Safety CPU Unit, the Safety CPU Unit will operate as shown in the following table.

Before change	→	After change	Operation
PROGRAM mode	→	DEBUG mode (STOPPED)	• Safety process data communications start.
PROGRAM mode	→	RUN mode	• Safety process data communications start. • The variables are initialized and the safety programs are executed from the beginning.
DEBUG mode (STOPPED)	→	DEBUG mode (RUN)	• Safety process data communications continue. • The variables are initialized and the safety programs are executed from the beginning.
DEBUG mode (RUN)	→	DEBUG mode (STOPPED)	• Safety process data communications continue. • The variables are initialized and the safety programs are stopped. • The forced status of variables is cleared.
RUN mode	→	PROGRAM mode	• Safety process data communications stop. The safety input data from the Safety Input Units is initialized to 0. The safety output data to the Safety Output Units is initialized to 0. • The variables are initialized and the safety programs are stopped. • The safety programs are deleted from the non-volatile memory of the Safety CPU Unit.
DEBUG mode (RUN)	→	PROGRAM mode	• Safety process data communications stop. The safety input data from the Safety Input Units is initialized to 0. The safety output data to the Safety Output Units is initialized to 0. • The variables are initialized and the safety programs are stopped. • The forced status of variables is cleared.
DEBUG mode (STOPPED)	→	PROGRAM mode	• Safety process data communications stop. The safety input data from the Safety Input Units is initialized to 0. The safety output data to the Safety Output Units is initialized to 0.

Relationship between Establishing Safety Communications and Execution of the Safety Programs

The Safety CPU Unit starts execution of the safety programs at the same time the safety process data communications are established.
The input data that is refreshed from the Safety Input Units is used for processing.

9-3-3 Executable Functions in Each Mode of the Safety CPU Unit

The following table shows the executable functions in each mode of the Safety CPU Unit.

Function *1		Initializing	PROGRAM mode	DEBUG mode		RUN mode	RESTORE mode
				STOPPED	RUN		
Safety program execution		Not possible	Not possible	Not possible	Possible	Possible	Not possible
Controlling BOOL variables, forced refreshing, and changing present values		Not possible	Not possible	Possible	Possible	Not possible	Not possible
Message communications		Possible	Possible	Possible	Possible	Possible	Possible
NX bus communications		Possible*2	Possible*2	Possible*2	Possible*2	Possible*2	Possible*2
Safety communications		Not possible	Not possible	Possible	Possible	Possible	Not possible
Downloading (transferring data from the Computer to the Controller)	**Configuration information (I/O allocation information)**	Not possible	Possible	Possible	Possible	Possible	Not possible
	Validated safety application data			Not possible	Not possible	Possible	
Uploading (transferring data from the Controller to the Computer)		Not possible	Not possible	Not possible	Not possible	Possible	Not possible
Clear All Memory Operation for NX Unit		Not possible	Possible	Not possible	Not possible	Not possible	Not possible
Clear All Memory Operation for Communication Control Unit*3		Not possible	Not possible	Not possible	Not possible	Not possible	Not possible
Restarting NX Bus/NX Unit		Possible	Possible	Possible	Possible	Possible	Possible
Resetting Controller for Communication Control Unit		Possible	Possible	Possible	Possible	Possible	Possible
Monitoring Controller status		Not possible	Possible	Possible	Possible	Possible	Possible
Monitoring programs		Not possible	Not possible	Possible	Possible	Possible	Not possible
Monitoring in a Watch Tab Page		Not possible	Not possible	Possible	Possible	Possible	Not possible

Function *1	Initializing	PROGRAM mode	DEBUG mode		RUN mode	RESTORE mode
			STOPPED	RUN		
Monitoring for trouble-shooting	Not possible	Possible	Possible	Possible	Possible	Possible
Changing the safety password	Not possible	Possible	Not possible	Not possible	Possible	Not possible
Node Name Change	Not possible	Possible	Not possible	Not possible	Possible	Not possible
Safety Data Logging	Not possible	Not possible	Not possible	Not possible	Possible	Not possible
Safety Unit Restore	Not possible	Not possible	Not possible	Not possible	Not possible	Possible
Online Functional Test	Not possible	Not possible	Not possible	Possible	Possible	Not possible

*1. Hardware Self-diagnosis
In the initializing state, self-diagnosis is performed for all hardware.
In other operating modes, hardware self-diagnosis is performed at fixed intervals.

*2. NX bus communications
The data is refreshed depending on the operating mode, as shown in the following table.

Operating mode		Refreshing
Initializing		The input data is discarded. The output data is fixed to 0.
PROGRAM mode		The input data is discarded. The output data that carries status information is transferred. All data outputs from the safety programs change to 0.
RUN mode		I/O data refreshing is performed with the safety programs.
DEBUG mode	**STOPPED**	Input data refreshing is performed with the safety programs. The output data that carries status information is transferred. All data outputs from the safety programs change to 0.
	RUN	I/O data refreshing is performed with the safety programs.

*3. You can execute the Clear All Memory operation for the Communication Control Unit regardless of the operating status of the Safety CPU Unit, but it will always fail for the Safety CPU Unit.

9-4 Changing to DEBUG Mode

This section describes how to place the Safety CPU Unit into DEBUG mode. When you change to DEBUG mode, the safety application data is transferred to the Safety CPU Unit.

⚠ WARNING

Before you use the Sysmac Studio to change the operating mode of the Safety CPU Unit to DEBUG Mode, make sure that it is safe to do so at the destination for the safety application data.
The outputs may operate and may cause serious injury.

DEBUG Mode Application

DEBUG mode is used to check that the safety communications, the safety programs, and the external devices operate properly before you operate the Safety CPU Unit.
When you place the Safety CPU Unit in DEBUG mode, the unvalidated safety programs are automatically transferred from the Sysmac Studio to the main memory of the Safety CPU Unit.
As a safety precaution, the Sysmac Studio allows you to switch the Safety CPU Unit to DEBUG mode only when the Safety CPU Unit is in PROGRAM mode.

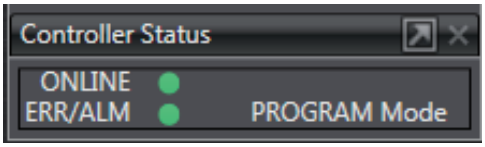
Precautions for Safe Use

Verify that the safety communications with a remote node will be established in the debug mode of the Safety CPU Unit.

Procedure for Changing to DEBUG Mode

Use the following procedure to switch the operating mode of Safety CPU Unit from the PROGRAM to DEBUG mode.
When you change the operating mode to the DEBUG mode, the safety programs must be ready for building.

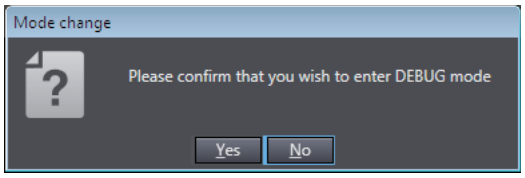
1. Make sure that the Safety CPU Unit is in the PROGRAM mode.
2. Connect to the Safety CPU Unit online.
3. Select the Safety CPU Unit from the Controller Selection Box in the Multiview Explorer of Sysmac Studio and open the Safety CPU Unit Setup and Programming View.
   When you move to the view for Safety CPU Unit, the Sysmac Studio goes online with the Safety CPU Unit, and the Controller status is displayed in the lower right of the Sysmac Studio Window, as shown below.



4 On the Safety CPU Unit Setup and Programming View, perform one of the following operations.

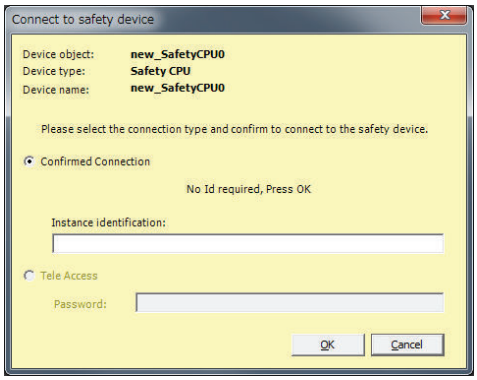
- Select **Mode** – **DEBUG Mode** from the **Controller** Menu.
- Press the **Ctrl** + **2** Keys.
- Click the **DEBUG Mode** Button on the toolbar.

The following mode confirmation dialog box is displayed.



5 Click the **Yes** Button.

The following Connect to safety device Dialog Box is displayed.

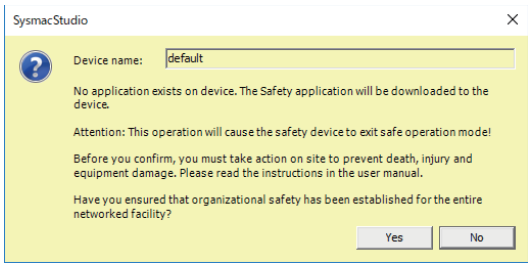


Note 1. When you change the operating mode for the first time, the above dialog box is displayed and allows you to set the node name. You can change the factory-default node name of the Safety CPU Unit.
If you do not want to change the node name, leave the field blank and click the **OK** Button. Refer to *9-9 Node Name* on page 9-52 for details on the node name settings.

Note 2. You do not need to enter anything in the *Instance identification* Box.

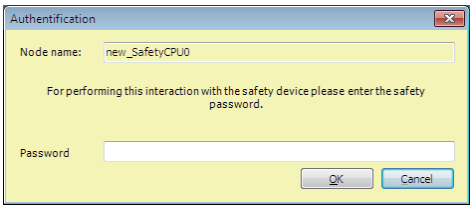
6 Click the **OK** Button.

The following transfer confirmation dialog box is displayed.



7 Check the safety of the system and then click the **Yes** Button.

The following password confirmation dialog box is displayed.



8 When you use the DEBUG mode for the first time, or when the safety password is not specified, leave the **Password** field blank and click the **OK** Button.
When a safety password is specified, enter the security password and click the **OK** Button.
Refer to *9-10 Security Settings* on page 9-53 for the procedure to set a safety password.

Unvalidated safety programs are transferred from the Sysmac Studio to the main memory of the Safety CPU Unit, and the Safety CPU Unit enters DEBUG (STOPPED) mode.

Precautions for Correct Use

Before the safety validation is executed, the safety programs are stored in the main memory of the Safety CPU Unit. When the Sysmac Studio goes offline or when you power off Safety CPU Unit, the safety programs are deleted. Because of this, after you cycle the power supply, you must use the Sysmac Studio to change to DEBUG mode again and transfer the safety programs to the main memory again.

Changing to PROGRAM Mode

If you need to change the safety program, you must change to PROGRAM mode.
Use the following procedure to change the Safety CPU Unit from DEBUG mode to PROGRAM mode.

With the Safety CPU Unit in DEBUG mode, perform one of the following operations.

- Select **Controller** - **Operating Mode** - **PROGRAM Mode**.
- Press the **Ctrl** + **1** Keys.
- Click the **PROGRAM Mode** Button on the toolbar.

The Safety CPU Unit enters PROGRAM mode.

9-5 Checking External Device Wiring

This section describes the functions that you use on the Sysmac Studio to check the wiring of external devices connected to the Safety I/O Units.
You can obtain information on the Safety I/O Units to which external devices are connected and confirm that the external devices are correctly wired by placing the Sysmac Studio online with the Safety CPU Unit and changing to DEBUG mode.

9-5-1 Overview of Functions for Checking Wiring

This section describes the functions that you use on the Sysmac Studio to check external device wiring.

Functions for checking wiring	Reference
Monitoring Safety I/O terminals	*9-5-2 Monitoring Safety I/O Units* on page 9-16
Monitoring Safety I/O data	*9-5-2 Monitoring Safety I/O Units* on page 9-16
Troubleshooting Safety I/O terminals	*9-5-3 Troubleshooting Safety I/O Terminals* on page 9-19
Clear All Memory Operation for Safety I/O Unit	*9-5-4 Clear All Memory Operation for Safety I/O Units* on page 9-20

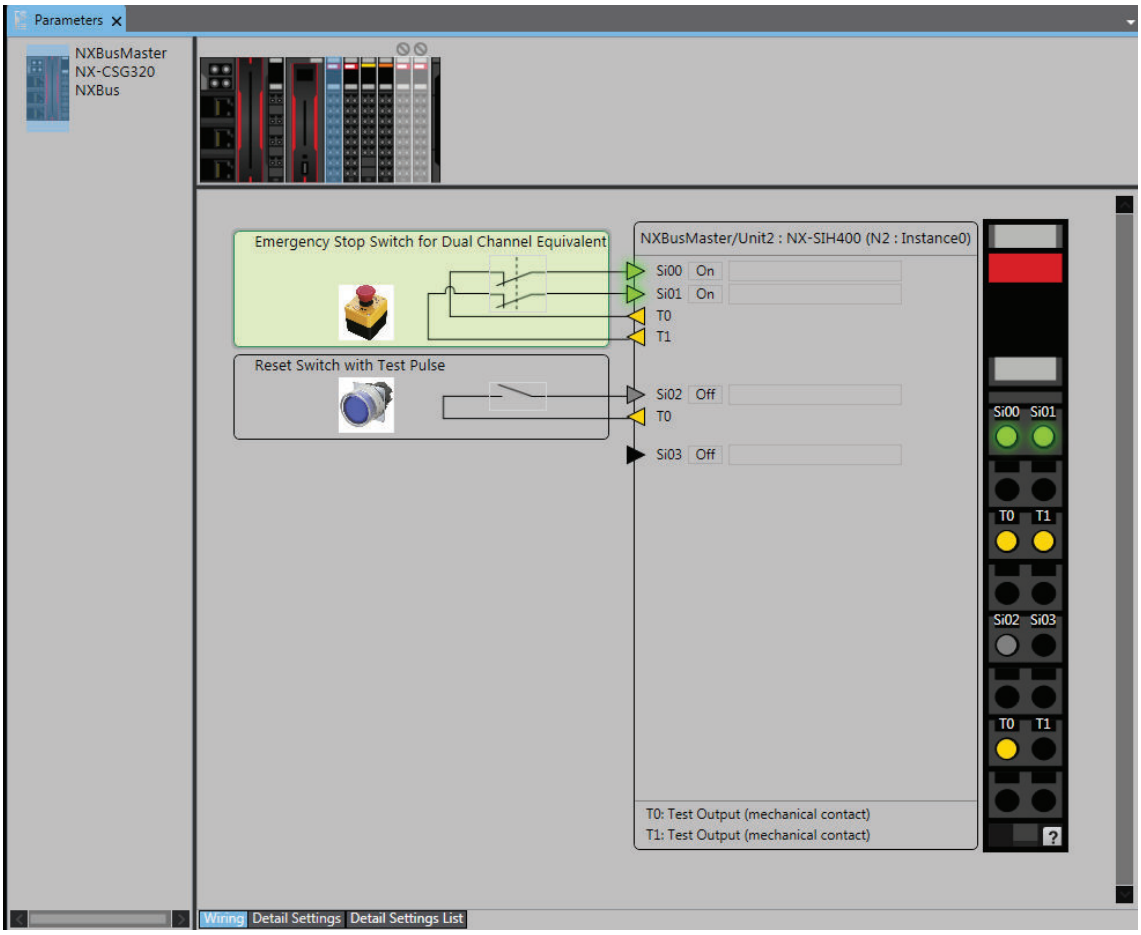
The functions to check wiring should be executed while you are online to the Safety CPU Unit in DEBUG mode or RUN mode.
If the safety application monitoring is stopped, you need to start monitoring. For the procedure to start monitoring, refer to *9-12 Starting and Stopping the Safety Application Monitoring* on page 9-64.

9-5-2 Monitoring Safety I/O Units

This section describes how to monitor I/O terminal information of the Safety I/O Units to check external device wiring.

Executing the Monitor for Safety I/O Terminals

1. Place the Sysmac Studio online with the Communication Control Unit.
   In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.
2. Place the Safety CPU Unit in DEBUG mode.
   Refer to *9-4 Changing to DEBUG Mode* on page 9-13 for the detailed procedure.
3. Select **Configurations and Setup** – **Communications** – **Safety** – **Safety I/O**. Double-click **Parameters** under the name of the Safety I/O Unit.
   The Parameters Tab Page shown below is displayed. Select the Safety I/O Unit to monitor.



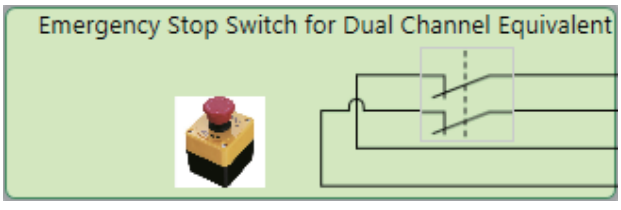
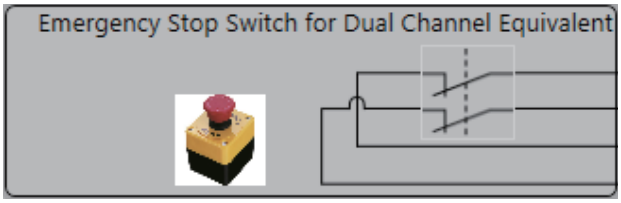
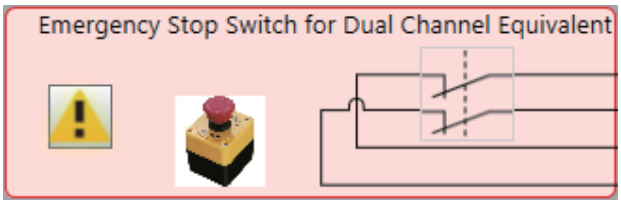
Description of the Monitor Tab Page

- NX Unit Displays

Display	Monitor function	Description
	Enabled	The Safety I/O Unit is present in the actual configuration, and has its communications established. This shows that there is no error at the safety I/O terminals of the Safety I/O Unit.
	Enabled	The Safety I/O Unit is present in the actual configuration, and has its communications established. This shows that there is an error at the safety I/O terminals of the Safety I/O Unit.

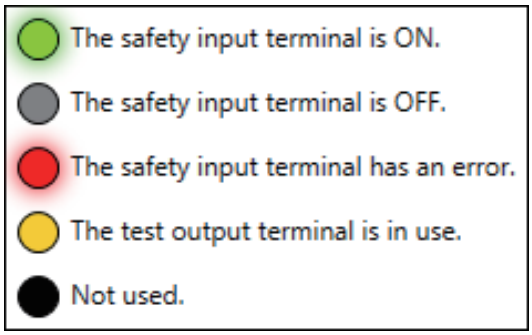
Display	Monitor function	Description
	Disabled	The Safety I/O Unit is present in the actual configuration, and has its safety process data communications disabled. This Safety I/O Unit is not subject to monitoring.
	Disabled	The Safety I/O Unit is present in the actual configuration, and its safety process data communications are not established. This Safety I/O Unit is not subject to monitoring.
	Disabled	The NX Unit mounting settings are disabled for the Safety I/O Unit. This Safety I/O Unit is not subject to monitoring.
	Disabled	Either the Safety I/O Unit is not present in the actual configuration or the communications were not established with it. This Safety I/O Unit is not included in the monitoring target.

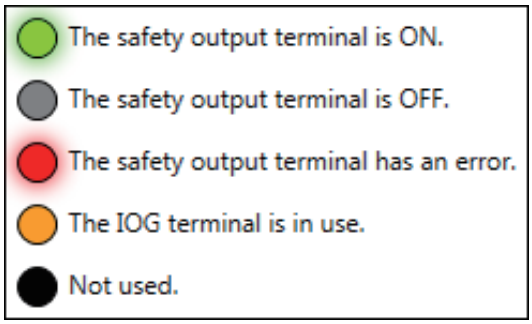
- External Device Displays

Display	Description
	In this state, safety I/O data from external devices is treated as ON. This shows that there is no error at the safety I/O terminals connected to this external device.
	In this state, safety I/O data from external devices is treated as OFF. This shows that there is no error at the safety I/O terminals connected to this external device.
	In this state, safety I/O data from external devices is treated as OFF. This shows that there is an error at a safety I/O terminal connected to this external device.

- Safety I/O Terminal Displays

  Click the ? Icon below the safety input I/O terminals to display the legend for the safety I/O terminal.





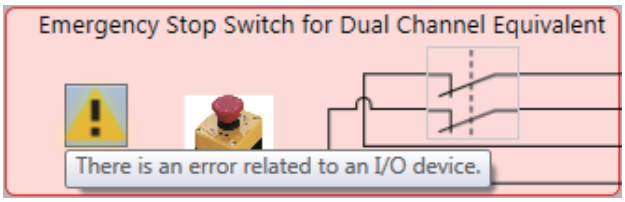
9-5-3 Troubleshooting Safety I/O Terminals

This section describes troubleshooting errors that may occur at a safety I/O terminal because of incorrect external device wiring or incorrect safety I/O settings.

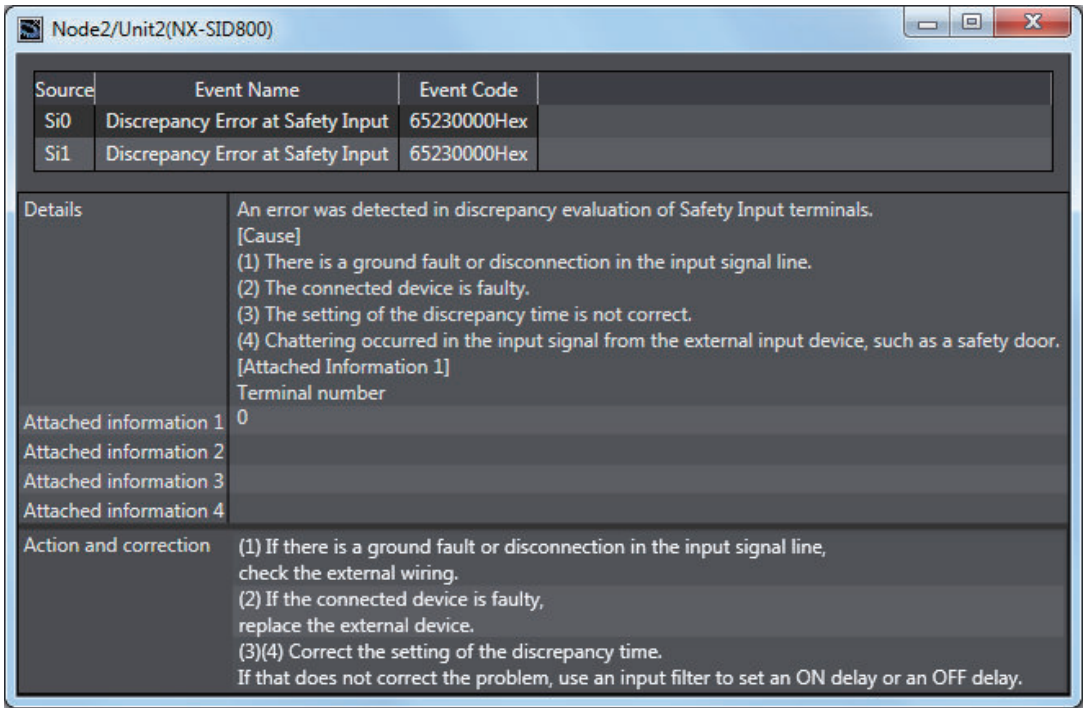
Displaying Safety I/O Terminal Troubleshooting

1 Open the Monitor Tab Page for the Safety I/O Unit for which there is an error in a safety I/O terminal.

2 Click the " ! " Icon for the external device for which the error is displayed or right-click the external device and select **Troubleshooting...** from the menu.



3 The Troubleshooting Dialog Box for the safety I/O terminals is displayed. Check details and corrections, and then eliminate the error.



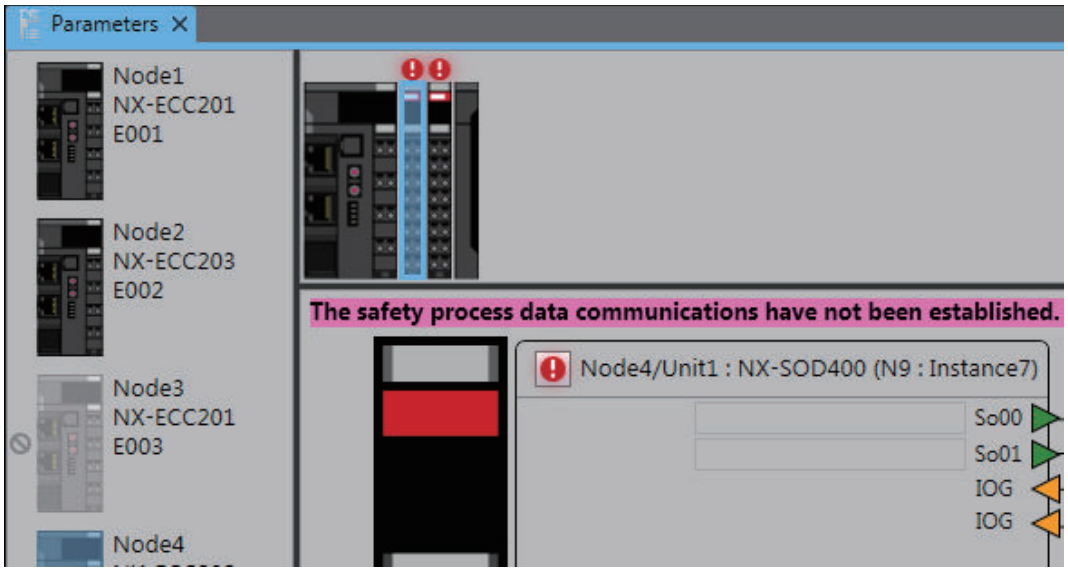
For details on the safety I/O terminal errors, refer to *15-3-4 Safety I/O Unit Error* on page 15-213.

9-5-4 Clear All Memory Operation for Safety I/O Units

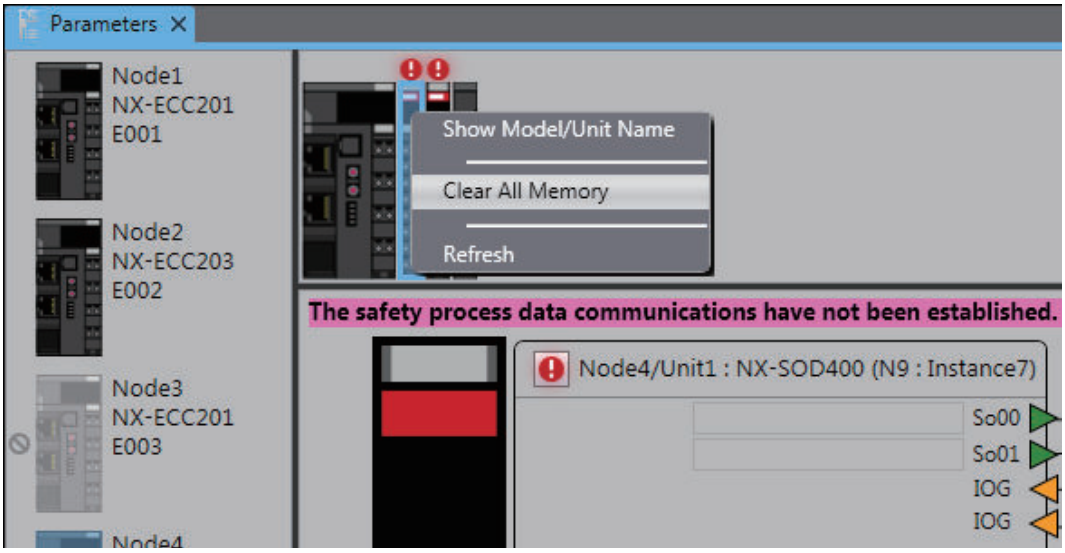
If an attempt to establish safety process data communications fails due to an illegal FSoE Slave Address, you must execute a Clear All Memory operation for the Safety I/O Units.

Executing the Clear All Memory Operation for Safety I/O Units

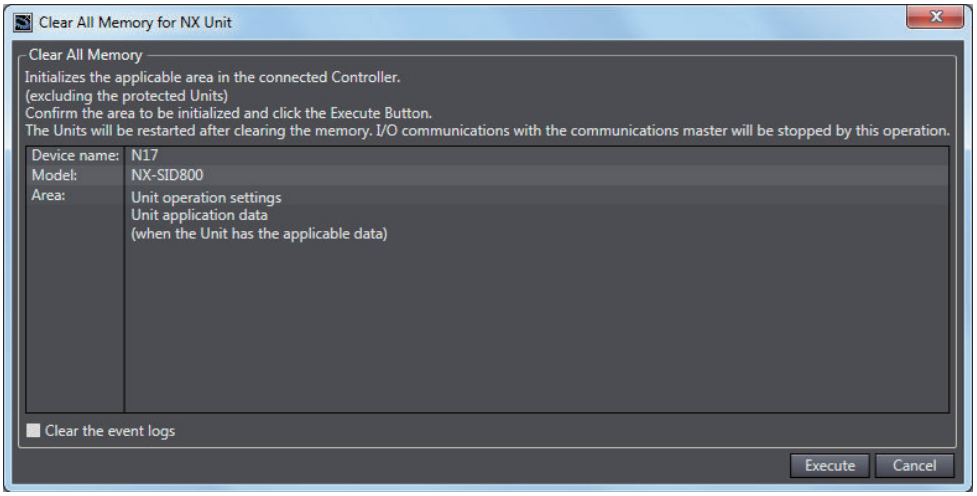
1 Select the Safety I/O Unit in which the error has occurred from the NX Unit list.



2 Right-click the Safety I/O Unit and select **Clear All Memory** from the menu.



3 Click the **Execute** Button on the Clear All Memory Tab Page for the NX Unit.



9-6 Functions for Checking Operation

This section describes the functions that you use on the Sysmac Studio to check the operation on the Safety CPU Unit.
You can check and adjust the operation of safety programs through an online connection between the Sysmac Studio and the Safety CPU Unit. This allows you to control BOOL variables, change present values, and perform other debugging tasks.

9-6-1 Overview of Functions for Checking Operation

This section describes the functions that you use on the Sysmac Studio to check the operation on the Safety CPU Unit.

Functions for Checking Operation	Reference
Monitoring	*9-6-3 Monitoring Variables in the FBD Editor* on page 9-23 *9-6-4 Monitoring Variables in a Watch Tab Page* on page 9-24
Monitoring in a Watch Tab Page	*9-6-5 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing* on page 9-26
Controlling BOOL variables	
Forced refreshing	
Changing present values of data	
Clear All Memory	*9-16-2 Clear All Memory Operation* on page 9-72
Monitoring Controller status	*9-15 Monitoring Controller Status* on page 9-70
Changing the operating mode	*9-3 Operating Modes of the Safety CPU Unit* on page 9-8
Troubleshooting	*Section 15 Troubleshooting* on page 15-1
Monitoring error information	
Displaying error logs	

Procedures to check operation are performed when online to the Safety CPU Unit.

9-6-2 Starting and Stopping the Safety Programs in DEBUG Mode

⚠ WARNING

Before you start the system, perform user testing to make sure that all safety devices operate correctly.
Serious injury may possibly occur due to loss of required safety functions.

⚠ WARNING

Always confirm safety at the destination node before you transfer Unit configuration information, parameters, settings, or other data from tools such as the Sysmac Studio. The devices or machines may operate unexpectedly, regardless of the operating mode of the Controller.

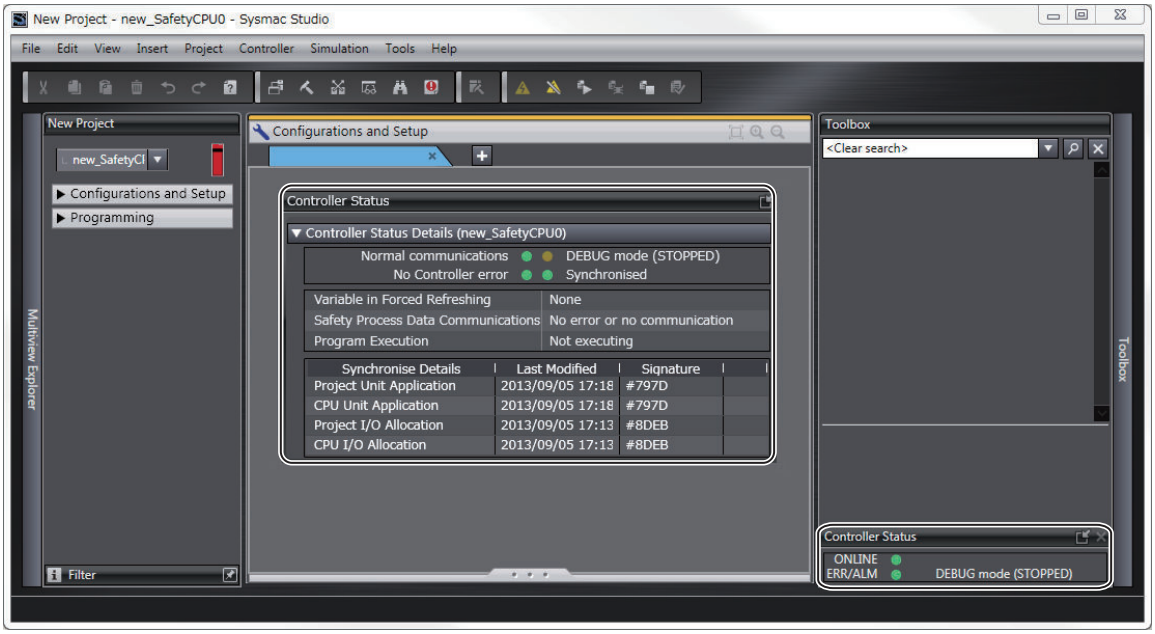
Starting and Stopping the Safety Programs

Use the following procedure to change the Safety CPU Unit to DEBUG mode (RUN) or DEBUG mode (STOPPED).

With the Safety CPU Unit in DEBUG mode, perform one of the following operations.

- Select **Debug** – **Run** or **Stop** from the **Controller** Menu.
- Click the **Start Debugging** or **Stop Debugging** Button in the toolbar.

The Safety CPU Unit moves to DEBUG mode (RUN) or DEBUG mode (STOPPED).



9-6-3 Monitoring Variables in the FBD Editor

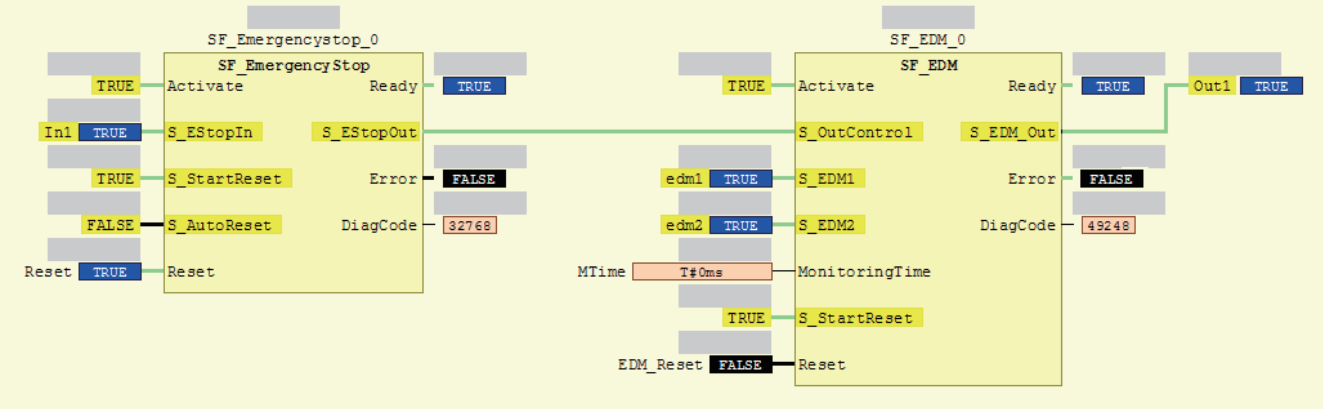
This section describes the procedures to monitor the present values of variables in the FBD editor to debug the safety programs.

To be able to execute the monitoring function for variables on the FBD editor, the Sysmac Studio must be connected to the Safety CPU Unit that is either in the DEBUG mode or in the RUN mode. If the safety application monitoring is stopped, you need to start monitoring. For the procedure to start monitoring, refer to *9-12 Starting and Stopping the Safety Application Monitoring* on page 9-64.

Executing the Operation Monitor for the Safety Programs

You can monitor the present values of variables in the FBD editor. Use the following procedure.

Double-click the program to monitor, in the Multiview Explorer.
The operating status of the selected POU is displayed in the FBD editor.



- The value of the variable is displayed in the frame on the right side of the variable name. “FALSE” is displayed with a black background, and “TRUE” is displayed with a blue background. Numeric values are displayed as decimal numbers. Use the Watch Tab Page to check numerical values as binary or hexadecimal numbers.
- The connecting lines between variables and FBs appear in green when the signal is ON. They appear in black when the signal is OFF.

9-6-4 Monitoring Variables in a Watch Tab Page

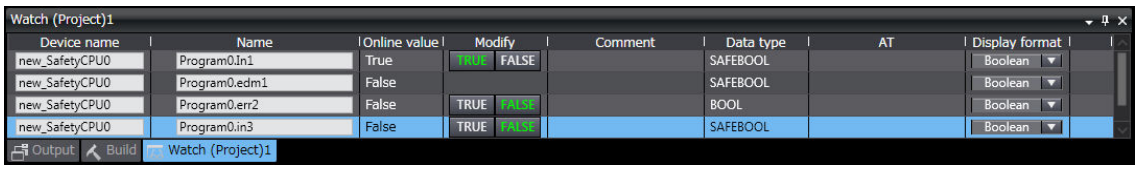
This section describes the procedures to monitor the present values of variables in a Watch Tab Page to debug the safety programs.
To be able to execute the monitoring function for variables on the Watch Tab Page, the Sysmac Studio must be connected to the Safety CPU Unit that is either in the DEBUG mode or RUN mode. If the safety application monitoring is stopped, you need to start monitoring. For the procedure to start monitoring, refer to *9-12 Starting and Stopping the Safety Application Monitoring* on page 9-64.

Monitoring in a Watch Tab Page

You can check the present value of one or more variables in the Watch Tab Page.

Displaying a Watch Tab Page

Select **Watch Tab Page** from the **View** Menu.
The Watch Tab Page is displayed.



To close a Watch Tab Page, right-click the tab to display the menu, and select **Close**.
To display a Watch Tab Page that you closed, select **Watch Tab Page** from the **View** Menu again.

Contents of the Watch Tab Page

The following table gives variable-related information displayed in a Watch Tab Page.

You can right-click an column and use the displayed menu to display or hide the following items: Comment, Data type, AT, and Display format.

YES: Editable, NO: Not editable

Item	Description	Editing
Device name	The device name is displayed.	YES
Name	The variable name is displayed.	YES
Online value	The present value of the variable is displayed.	
Modify	The new value is displayed.	YES
Comment	The comment for the variable is displayed.	NO
Data type	The data type is displayed.	NO
AT	No information is displayed.	NO
Display format	The display format (decimal, hexadecimal, etc.) of the present value and modify value is displayed.	YES

Registering Variables in the Watch Tab Page

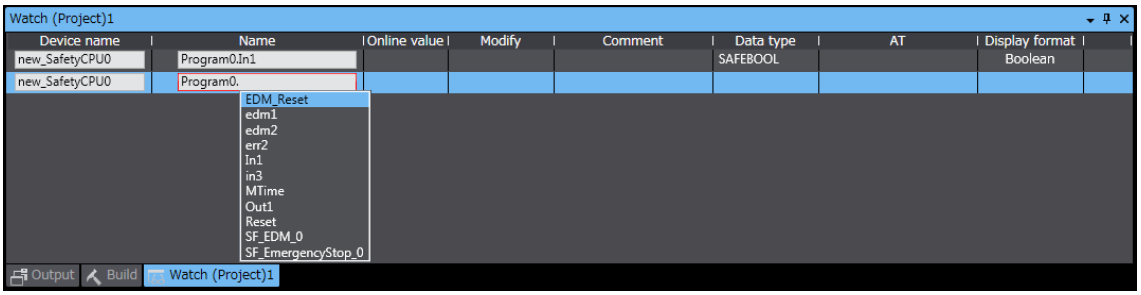
There are two ways to register variables.
Method 1: Enter the variable name in the name cell in the Watch Tab Page.
Method 2: Drag the variable to the Watch Tab Page from a variable table.

● Procedure for Method 1

1 Click the cell that says *Input Name* at the bottom of the Watch Tab Page.

2 Enter the variable name to display the present value.

3 As you enter characters, a list of candidate variable names is displayed. Select the variable name from the list.
The variable name is registered.



● Procedure for Method 2

Drag a variable from a variable table to the Watch Tab Page.
The variable is registered.

Deleting Variable Names from the Watch Tab Page

Right-click the variable name to delete in the Watch Tab Page and select **Delete** from the menu. Or, press the **Delete** Key to delete the variable name directly.
The variable name and the row it was displayed on are deleted.

9-6-5 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing

You can debug the safety program by controlling BOOL variables (Set/Reset), changing present values, and executing forced refreshing from the Sysmac Studio. These functions can be executed only when the Safety CPU Unit is in DEBUG mode (RUN) or DEBUG mode (STOPPED).

⚠ WARNING

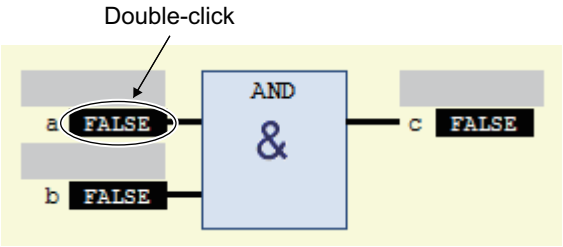
Make sure that the area around the system is safe before you control BOOL variables (Set/Reset), change present values, and execute forced refreshing.
The outputs may operate and may cause serious injury.

Controlling BOOL Variables (Set/Reset)

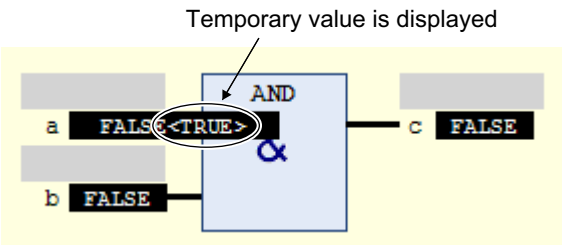
This function allows you to change the values of BOOL variables in the FBD editor or Watch Tab Page to debug safety programs.

● Controlling BOOL Variables in the FBD Editor (Set/Reset)

1 Double-click the present value of the BOOL variable to change.
Example: To set the variable *a*, double-click the present value of *FALSE*.

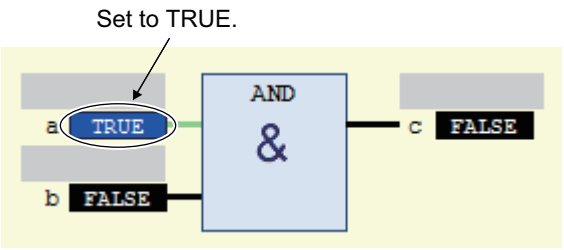


The value changes to a temporary status.
A temporary value appears in <> on the right side of the present value. This indicates that the temporary value, either TRUE or FALSE, is available to replace the present value.



Each double-click toggles the temporary value.

2 Select **Write Values** from the **Controller** Menu.
The temporary value is removed and reflected as the present value.
Example: The present value of variable *a* is set to *TRUE*.

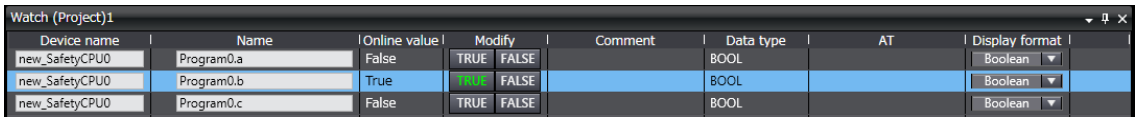


Additional Information

You can replace more than one present value in a single operation. To do this, set multiple BOOL variables with temporary values, and then select **Write Values** from the **Controller** Menu.

● Controlling BOOL Variables in the Watch Tab Page (Set/Reset)

Select **TRUE** in the **Modify** Column to change the variable to TRUE. Select **FALSE** in the **Modify** Column to change the variable to FALSE.
The present value is displayed in the Watch Tab Page as **TRUE** when set, and **FALSE** when reset.

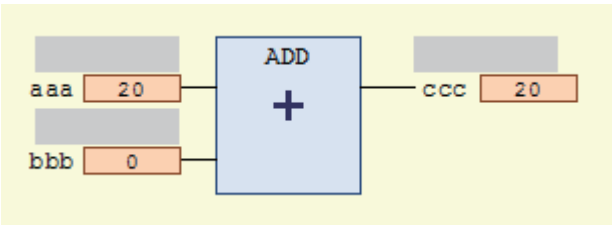


Changing the Present Values of Variables

This function allows you to change the present value of non-BOOL variables to desired values in the FBD editor or Watch Tab Page to debug safety programs.

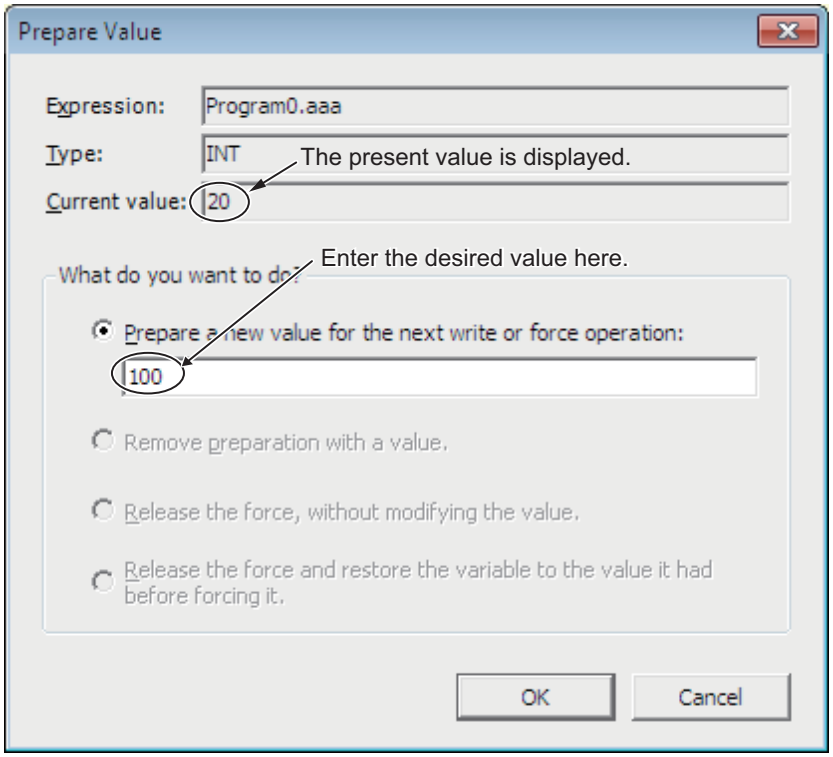
● Changing Present Values on the FBD Editor

1 Double-click the present value of the non-BOOL variable to change.
Example: To change the present value of variable *aaa*, double-click the present value of *20*.

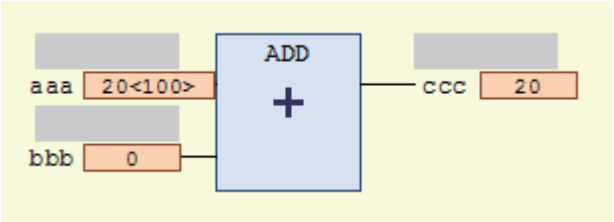


The **Prepare Value** Dialog Box is displayed.

2 Select the **Prepare a new value for the next write or force operation** Option and enter the new value.
Example: This example changes the value to *100*.

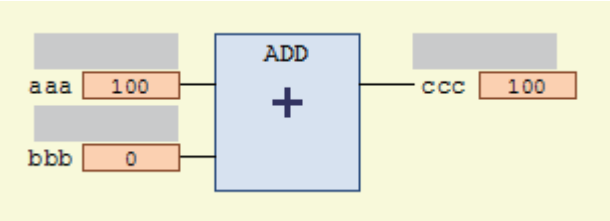


3 Click the **OK** Button.
The **Prepare Value** Dialog Box closes and the new value is prepared as the temporary value. The temporary value appears in <> on the right side of the present value. This indicates that the temporary value is available to replace the present value.



To cancel the temporary value, double-click the present value of the desired variable again. Select the **Remove preparation with a value** Option in the **Prepare Value** Dialog Box, and then click the **OK** Button.

4 Select **Write Values** from the **Controller** Menu.
The temporary value is removed and reflected as the present value.
Example: The present value of variable *aaa* is changed to *100*.



Additional Information

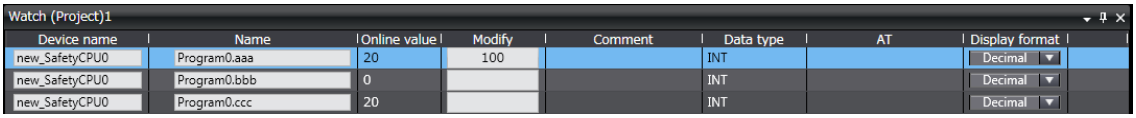
You can replace more than one present value in a single operation. To do this, set multiple present values with temporary values, and then select **Write Values** from the **Controller** Menu.

● Changing Present Values on a Watch Tab Page

Use the following procedure to change present values from the Watch Tab Page.

1 Select **Watch Tab Page** from the **View** Menu to display a Watch Tab Page.

2 Move the cursor to the cell in the **Modify** Column on the Watch Tab Page, enter a value that is compatible with the format that is given in the **Display format** Column, and then press the **Enter** Key.
The present value is changed.



The format for entering a value in the **Modify** Column depends on the **Display format** type that is given in the Data format Column.
Refer to *9-6-4 Monitoring Variables in a Watch Tab Page* on page 9-24 for details.
Press the **Esc** Key to cancel the entry.

- Examples of Entries in the **Modify** Column:

Display format type	Example
Boolean	TRUE or FALSE
Decimal	10, -100
Real number	123.4, 1.234e2, 1.234E2, -1.23e-3
Hexadecimal	1001, FFFF8000
Binary	11110000
String	abc, ABC

Additional Information

If you enter an illegal value in the **Modify** Column, it is detected as an error and the cell is highlighted in red.

Forced Refreshing

Forced refreshing allows you to refresh external inputs and outputs with user-specified values from the Sysmac Studio to debug the system. You execute this in the FBD editor or Watch Tab Page.
Forced refreshing is executed for the specified variables.
The state that is specified with forced refreshing is retained until forced refreshing is cleared from the Sysmac Studio.
All forced refreshing is cleared when a fatal error occurs in the Safety CPU Unit, when a Clear All Memory operation is performed, when the operating mode is changed, when power is interrupted, or when the project is downloaded.
You can use forced refreshing for the following data types.

Boolean	BOOL and SAFEBOOL
Bit string	BYTE and WORD
Integers	INT, SAFEINT, DINT, and SAFEDINT
Times of Day	TIME and SAFETIME

Precautions for Safe Use

- With forced refreshing, the values of variables are overwritten with specified values and then the safety programs are executed.
  If forced refreshing is used for variables that give the results of program processing, the variables will first take the specified values, but they will then be overwritten by the safety program.
- Depending on the difference in the forced status, the control system may operate unexpectedly.

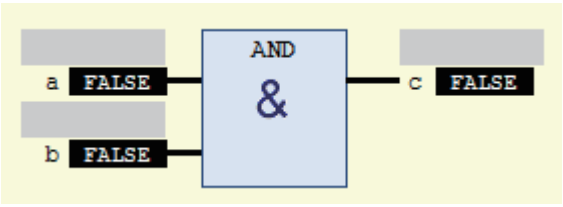
Precautions for Correct Use

- Forced status for forced refreshing is not removed when you change from DEBUG mode (STOPPED) to DEBUG mode (RUN).
- You can use forced refreshing for the following variables: device variables assigned to Safety I/O Units and user-defined variables.
- Even if you use forced refreshing for the device variables assigned to the input terminal to a Safety Input Unit, the forced value will not be applied to the variable that is assigned to the I/O port in the Communication Control Unit.

● Forced Refreshing of BOOL Variables in the FBD Editor

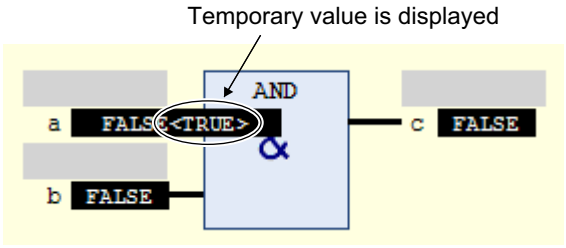
Use the following procedure to execute forced refreshing on BOOL variables.

1 Click the present value of the BOOL variable to change.
Example: To force-refresh variable *a*, click the present value of *FALSE*.



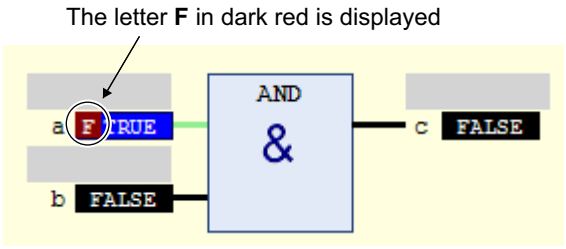
The value changes to a temporary status.

A temporary value appears in <> on the right side of the present value. This indicates that the temporary value is available for forced refreshing.



Each click toggles the temporary value.

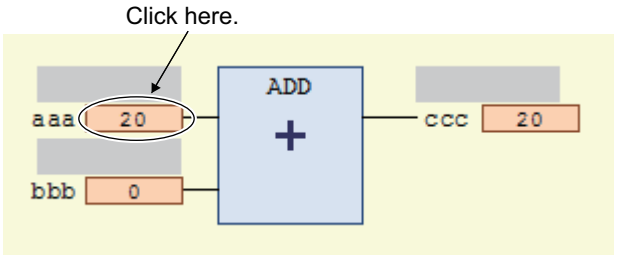
2 Select **Force Values** from the **Controller** Menu.
Forced refreshing is performed with the temporary values.
This removes the temporary value and places the letter [F] in dark red on the left side of the variable.
Example: The value of variable *a* is forced-refreshed to *TRUE*.



● Forced Refreshing of Non-BOOL Variables in the FBD Editor

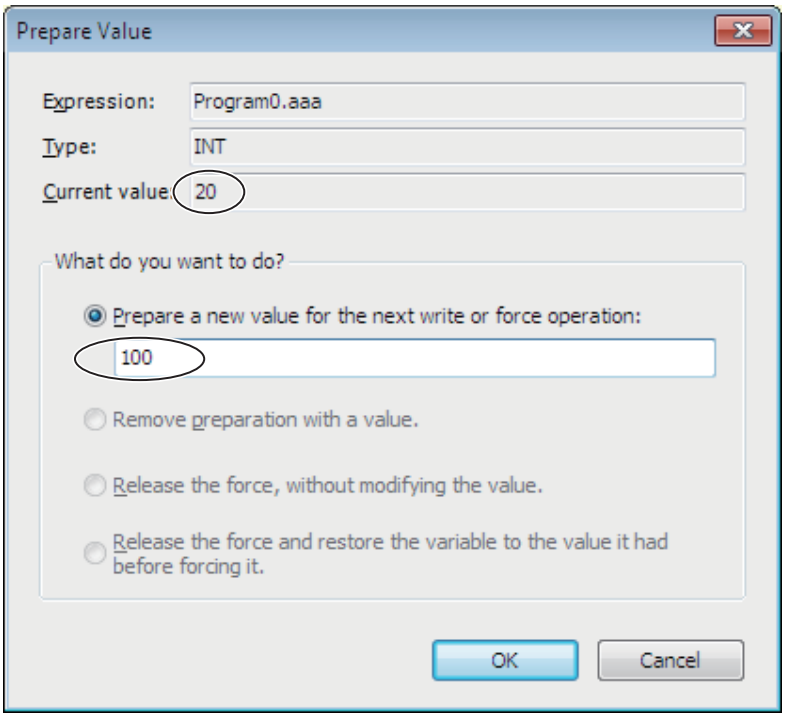
Use the following procedure to execute forced refreshing for non-BOOL variables.

1 Click the present value for the non-BOOL variable to change.
Example: To force-refresh the present value of the variable *aaa*, click the present value *20*.



The **Prepare Value** Dialog Box is displayed.

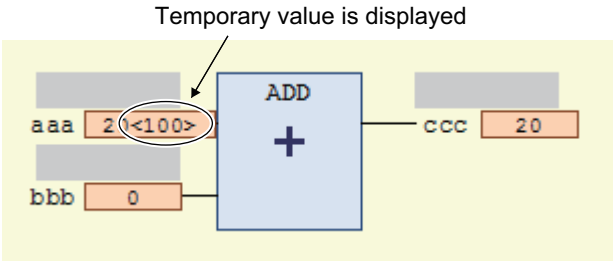
2 Select the **Prepare a new value for the next write or force operation** Option and enter a new value.
Example: This example changes the value to *100*.



3 Click the **OK** Button.

The **Prepare Value** Dialog Box closes and the value changes to a temporary value.

A temporary value appears in <> on the right side of the present value.



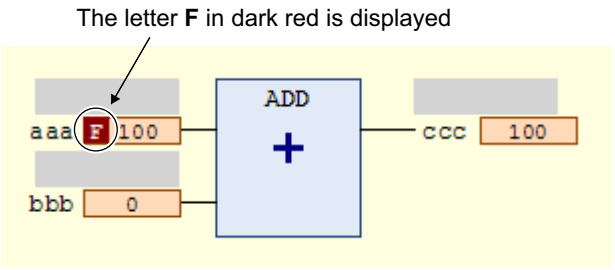
To cancel the temporary value, click the present value of the variable again. Select the **Remove preparation with a value** Option in the **Prepare Value** Dialog Box, and then click the **OK** Button.

4 Select **Force Values** from the **Controller** Menu.

Forced refreshing is performed with the temporary values.

This removes the temporary value and places the letter [F] in dark red on the left side of the variable.

Example: The value of variable *aaa* is forced-refreshed to *100*.



Additional Information

You can use forced refreshing for up to 256 variables at the same time.

● Procedure to Cancel All Forced Refreshing from the FBD Editor

Use the following procedure to batch-clear forced refreshing.

Select **Unforce Values** from the **Controller** Menu.

All forced refreshing is cleared at once.

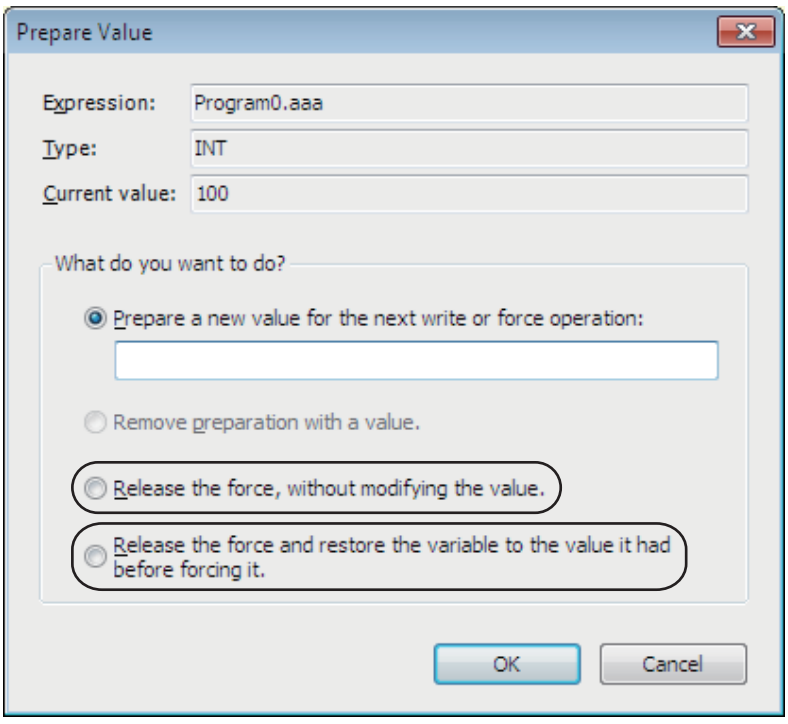
The letter [F] in dark red of all forced refreshing values are removed. The value will not change.

● Procedure to Cancel Individual Forced Refreshing from the FBD Editor

Use the following procedure to individually clear forced refreshing.

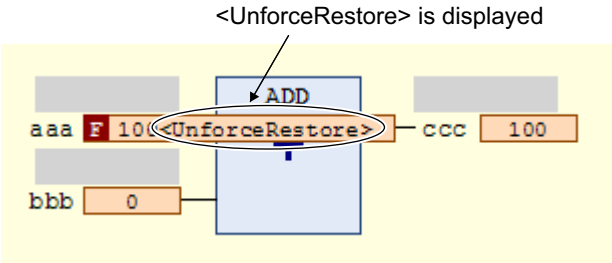
1 Click the present value of the variable to change.

The following **Prepare Value** Dialog Box is displayed.

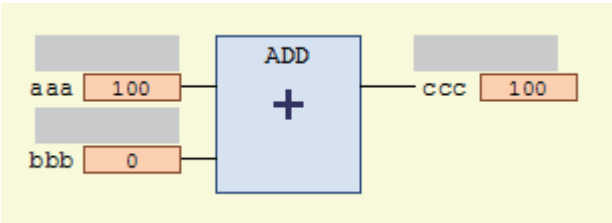


2 To clear the forced refreshing value and restore the original value, select the **Release the force and restore the variable to the value it had before forcing it** Option, and then click the **OK** Button.

To clear forced refreshing without changing the present values, select the **Release the force, without modifying the value** Option, and then click the **OK** Button.



3 Select **Force Values** from the **Controller** Menu.
The forced refreshing is cleared individually. The letter [F] in dark red is removed.



Additional Information

You can simultaneously select up to 256 variables to clear forced refreshing.

9-6-6 Cross References

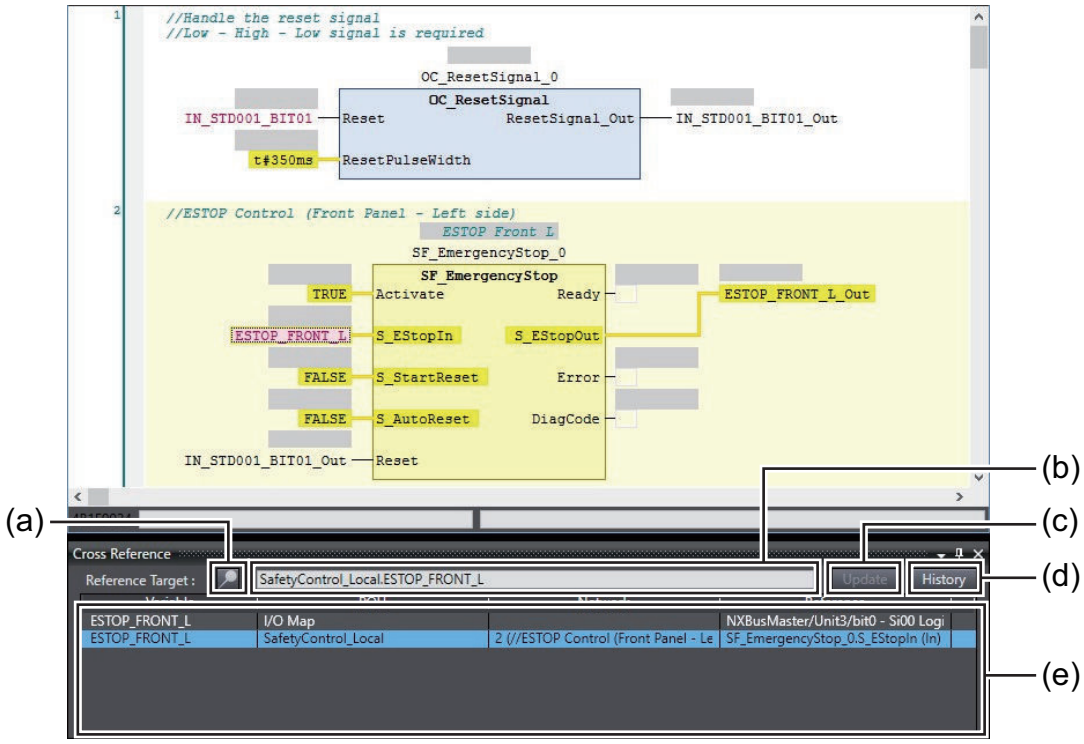
Cross References

Cross references allow you to see the programs and locations where variables of the safety program are used. You can view all locations where an element is used from this list.

Displaying and Manipulating Cross References

1 Select **Cross Reference Tab Page** from the **View** Menu.
The Cross Reference Tab Page is displayed.

2 Select a referenced element.
The name of the selected referenced element is displayed in the Reference Target field, and the locations where the element is used are listed under Cross Reference.
You can directly enter the variable name or member name in the Reference Target field.
Refer to *Referenced Element You Can Select* on page 9-35 for the elements you can select for reference.
For the areas where cross reference can be performed, refer to *Areas for Cross Reference* on page 9-36.



	Item	Description
(a)	Lock Button	Click this button to lock the display of the referenced element and cross reference list. Click the button again to release the lock.
(b)	Reference Target field	The referenced element that is currently selected is displayed. Or, you can directly enter a variable name or variable member name as the reference target in this field.*1
(c)	**Update** Button	This button is enabled only after the lock button is clicked and the display is locked. When the **Update** Button is clicked, the display of the cross reference list is updated.
(d)	**History** Button	When the History Button is clicked, the history window for the referenced element is displayed. On the reference history window, you can select the referenced element that was searched for in the past.
(e)	Cross reference list	The locations in which the referenced element is used are displayed. Refer to *Cross Reference List Details* on page 9-36, for details on items in the list.

*1. Note that an error occurs if the following variables are entered. Also, an error occurs if the directly entered element is not a variable.
- A variable in a POU that is protected with the display prohibition setting

Referenced Element You Can Select

The following table shows the referenced elements you can select and the locations from which you can select the referenced elements. You can select only the elements displayed with a focus in the following locations.

Element		Location
Variable	Global variable	• Global variable table • I/O parameter of functions, I/O parameter of function blocks, or instance name of function blocks on the FBD editor • I/O map
	Internal variable, external variable, input variable and output variable	• Internal variable tab, external variable tab and in-out variable tab in local variable tables • I/O parameter of functions, I/O parameter of function blocks or instance name of function blocks on the FBD editor

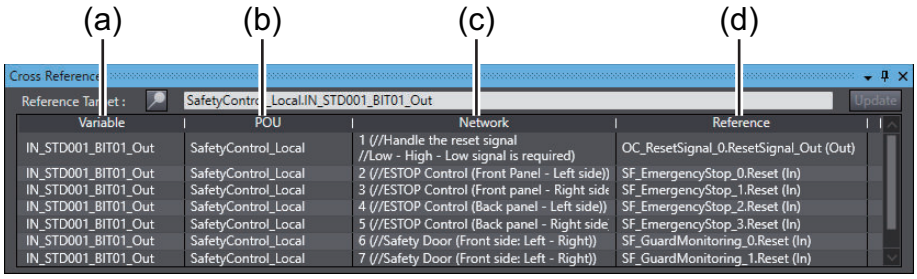
Areas for Cross Reference

The following table shows the areas where the usage locations of referenced element are detected. The following areas are displayed in the cross reference list if the referenced element is used in the areas.

Referenced element	Areas where usage locations are detected
Variable	• I/O parameter of functions, I/O parameter of function blocks, or instance name of function blocks on the FBD editor • I/O Map

Cross Reference List Details

The following table describes the contents of items displayed in the cross reference list.



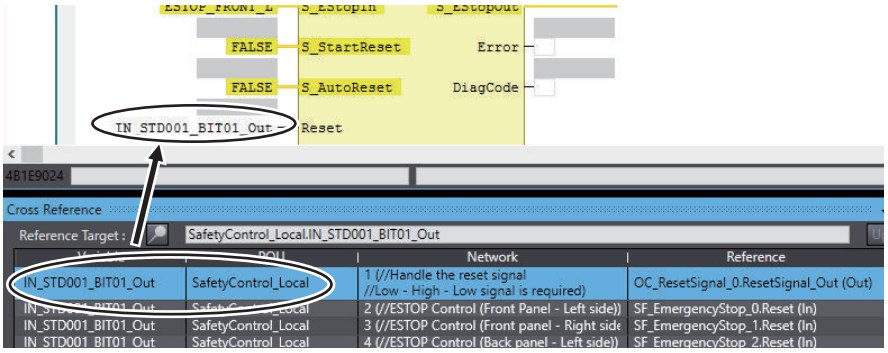
	Item	Description
(a)	Variable	The name of the referenced variable is displayed.
(b)	POU	The name of POU where the variable is used is displayed.
(c)	Network	The network numbers and network comments of the usage locations are displayed.
(d)	Reference	The name of function or function block where the referenced variable is used is displayed.

Additional Information

If a cross reference is for an input variable or output variable of a function block instance, the function block instance is also displayed in the cross reference list.

Viewing Usage Locations from the Cross Reference List

You can view where elements are used from the cross reference list. Select the item you want to find references for from the list. The locations where that item is used appear in the Edit Pane.



9-7 Online Functional Test

This section explains how to perform Online Functional Test to check operation of safety functions of the safety system using the Sysmac Studio. Connect the Sysmac Studio and the Safety CPU Unit online, and operate the Safety Input Units and the reset switch to confirm that the output device is operating normally, and then output the test result.

The Sysmac Studio checks expected values based on variable values assigned to input devices and output devices. The operator should verify whether the actual devices are operating properly or not.

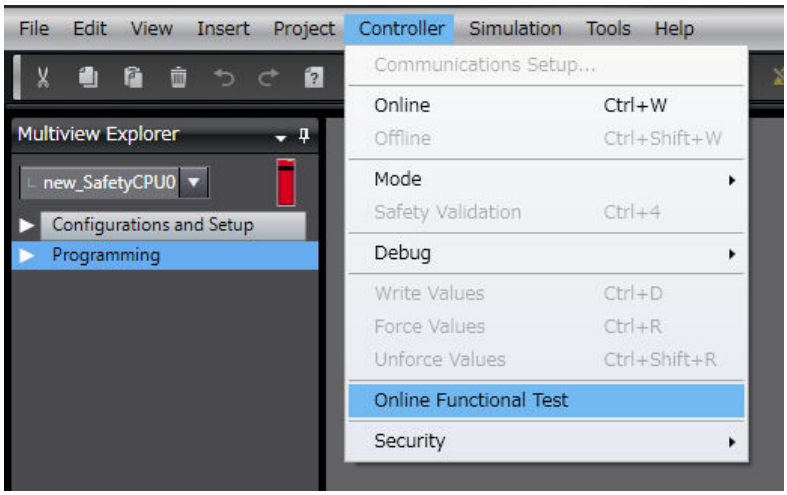
9-7-1 Online Functional Test Settings

Set the following signals and value in the Online Functional Test setting tab page to execute the Online Functional Test.

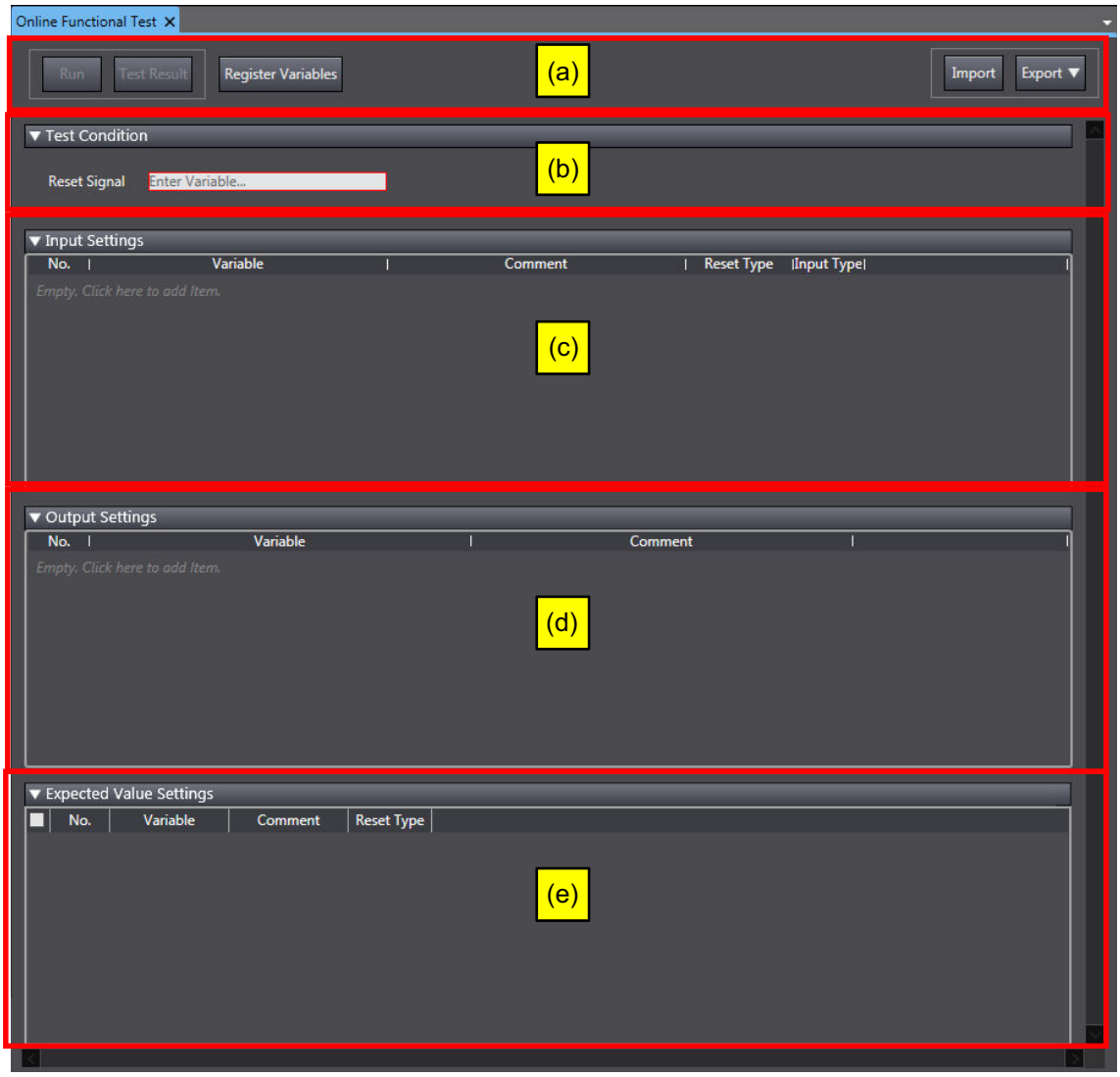
- Reset signal
- Input signal
- Output signal
- Expected value of the output signal corresponding to the input signal

You can display the settings window for the Online Functional Test in the following procedure.

- From the main menu, select **Controller** – **Online Functional Test**.



The following Online Functional Test setting tab page appears.



The configuration of the Online Functional Test setting tab page is as follows:

Letter	Name	Function	
(a)	Operation panel	The operation panel is used to make settings for and execute the online functional test.	
		Run Button	Starts an online functional test. You can execute the test only when the controller is connected to the Safety CPU Unit online. To run the online functional test, the Safety CPU Unit must be in RUN mode or DEBUG mode.
		Test Result Button	Displays results of the previous online functional test.
		Register Variables Button	Registers the variables that are used for the online functional test.
		Import Button	Imports the settings for the online functional test from a CSV file. If you import the settings, the current settings are overwritten.

Letter	Name	Function	
		Export – CSV File Output	Exports the current online functional test settings to a CSV file.
		Export – Export to Automatic Programming	Exports the current online functional test settings to the automatic programming settings. The settings of the export destination are overwritten.
		Export – Export to Simple Automatic Test	Exports the current online functional test settings to the simple automatic test settings. The settings of the export destination are overwritten.
		Export – Export to Online Functional Test	Exports the current automatic programming settings to the online functional test settings. The settings of the export destination are overwritten.
(b)	Test Condition	Specify a variable assigned to the reset switch of the safety system. You can set any SAFEBOOL or BOOL variable that is defined in the global variable table. You will use the reset switch when you check the manual reset operation.	
(c)	Input Settings	Specify a variable assigned to the safety input device used in the online functional test. In addition to the variable name of the input device, specify a reset type and an input type as well.	
		Variable	Specify a variable name assigned to the safety input device of the safety system. You can specify the SAFEBOOL or BOOL-type variable for the variable name.
		Reset Type	Selects a reset type of the safety input device from the box. The default value of the reset type is Manual. • Manual If manual reset is used for the input device, a test is executed for the manual reset scenario that uses the reset signal set in the Test Condition. • Auto If automatic reset is specified for the input device, a test is executed according to the auto reset scenario.
		Input Type	To set a test for two input signals, such as for a safety door or two-hand switches, set the input type to **2 Inputs**. If you set the input type to **2 inputs**, a row is added to specify another variable.
(d)	Output Settings	Specify a variable assigned to the safety output device used for the online functional test. You can set any SAFEBOOL or BOOL variable that is defined in the global variable table.	

Letter	Name	Function
(e)	Expected Value Settings	Displays the matrix of the variables specified in the input setting and output setting. Sets the values subject to test and the expected value of the output variables for each input variable. The expected values that you can set for output variables have the following meanings: • 0: If the input variable changes to FALSE, the output variable changes to FALSE. • 1: If the input variable changes to FALSE, the output variable changes to TRUE. You can edit the expected value settings by importing or exporting the values, and copying and pasting the values with a spreadsheet program or any other application software.

Setting Example

This section provides an example of the Online Functional Test settings based on the application example given in *A-4-2 Safety Doors* on page A-32.

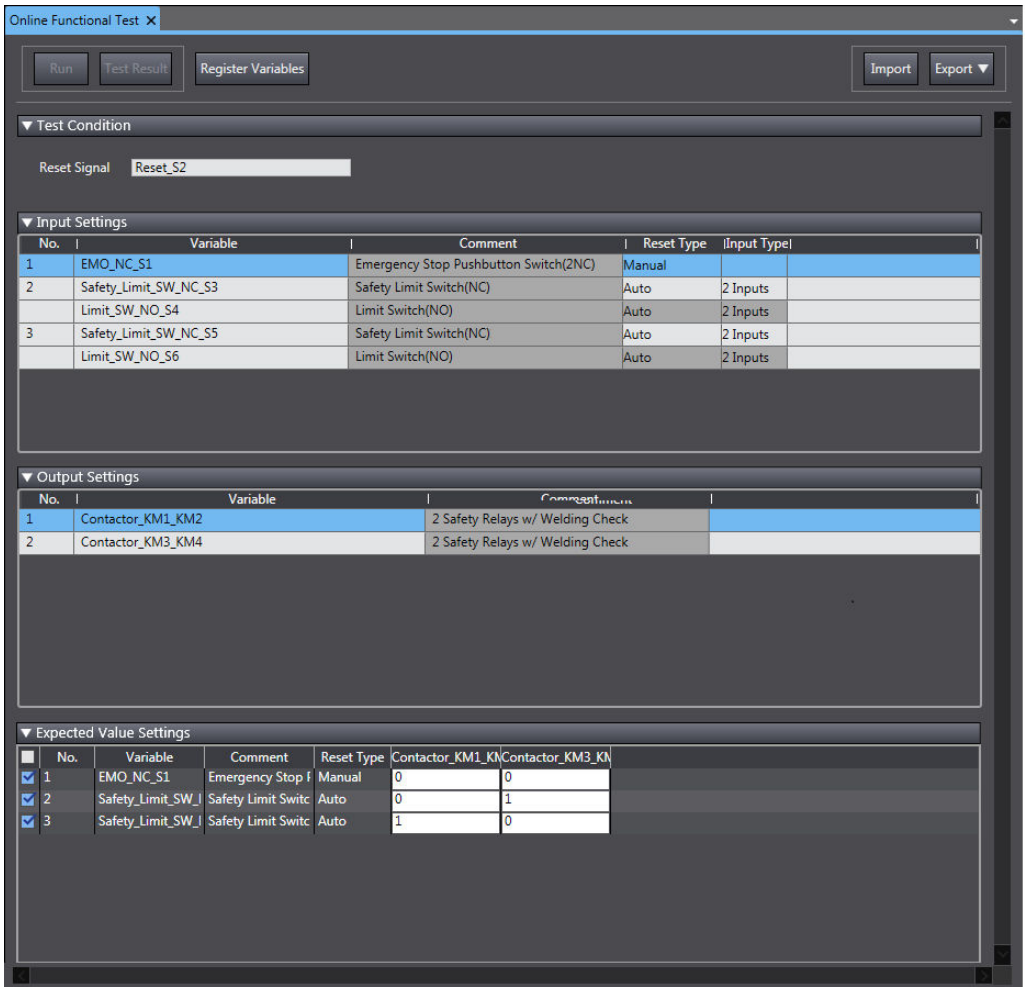
Application Overview from Safety Doors

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe (Safety Doors)	Safety Limit Switches 1, 2	0	Auto
	Emergency Stop Switch	0	Manual

M1 stops when safety door 1 (S3, S4) is opened.
M2 stops when safety door 2 (S5, S6) is opened.
Both M1 and M2 stop when the emergency stop pushbutton S1 is pressed.

At this time, enter the following safety door variables in the setting items on the Online Functional Test setting tab page.
- Variable that is assigned to the reset switch
- Variables assigned to the safety limit switch and the limit switch
- Variables assigned to the safety relays

The settings for the above application are shown in the setting areas for the Online Functional Test.



9-7-2 Online Functional Test Execution Procedure

Use the following procedure to execute the Online Functional Test.

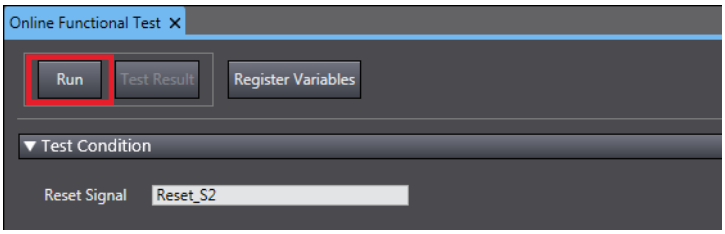
1 Place the Sysmac Studio online with the Safety CPU Unit.

2 Place the Safety CPU Unit in DEBUG mode.
Refer to *9-4 Changing to DEBUG Mode* on page 9-13 for a detailed procedure.

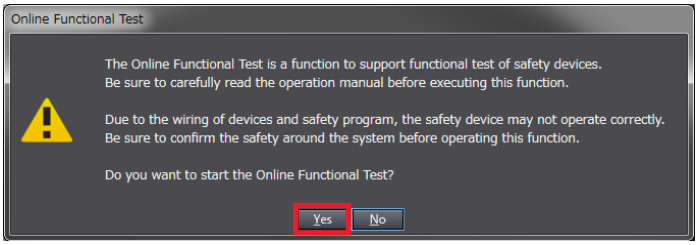
3 Select **Controller** - **Online Functional Test**.
The Online Functional Test Tab Page appears.

4 Set the **Test Condition**, **Input Settings**, **Output Settings**, and **Expected Value Settings**.

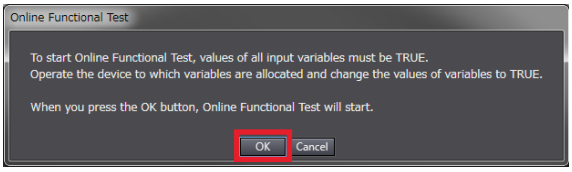
5 Click the **Run** Button on the control panel for the Online Functional Test Tab Page.



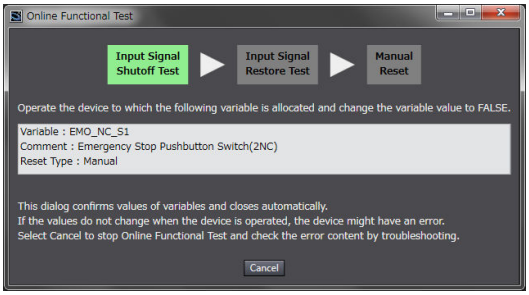
6 Check the precautions for executing the Online Functional Test and select **Yes**.



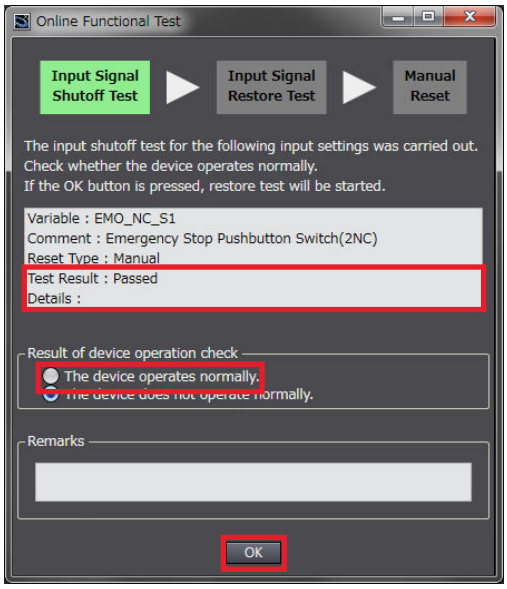
7 Operate the device as instructed on the screen. When you complete the preparations for starting a test, select **OK**.



8 Operate the device as instructed on the screen. Execute a shutoff test.
The operating instructions for the device to be tested will appear. Operate the input device as instructed on the screen and specify FALSE for the variable assigned to the input device.

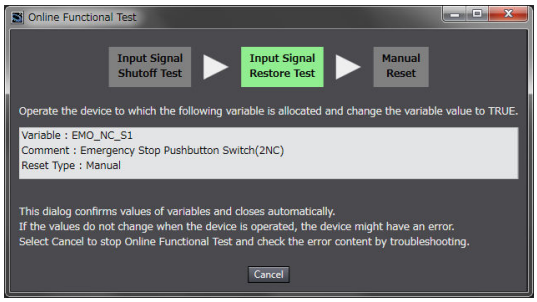


9 Make sure that the device operated normally.
The Controller detects the values of the assigned variables whose statement became FALSE and defines whether the statement of the variables assigned to all the output devices is consistent with the settings of the expected values. The definition results are displayed in the below dialog box. If the device is running in accordance with the settings of the expected values, check the box **The device operates normally** and select **OK**.



10 Operate the device as instructed on the screen. Execute a restore test.

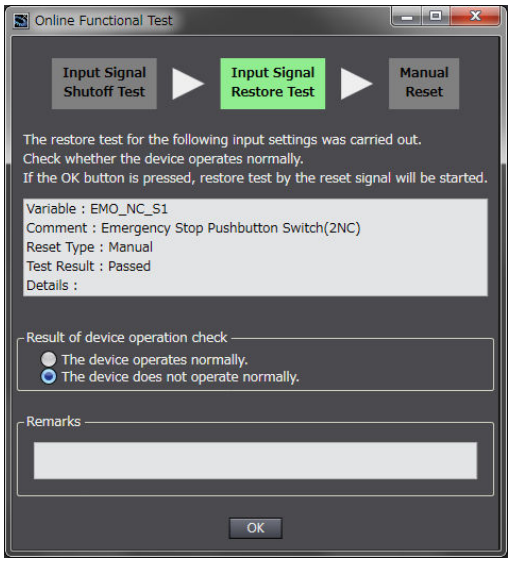
The operating instructions for the device to be tested will appear. Operate the device as instructed on the screen and specify TRUE for the variable assigned to the input device.



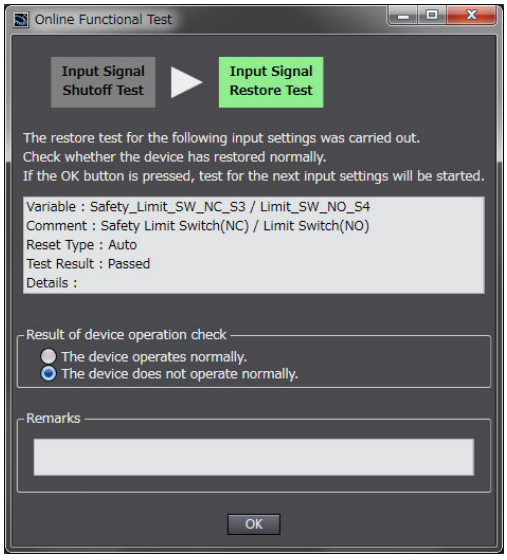
11 Make sure that the device was restored normally.

- Reset Type: Manual

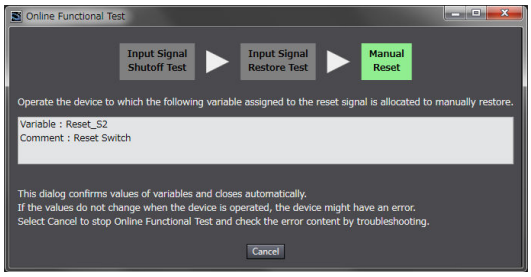
  The Controller checks if no change is made to the variables assigned to all the output devices when detecting that the specified variable is set to TRUE. The test result appears in the dialog shown below. If the devices operate normally as specified in the expected value settings, select the checkbox stating **The device operates normally** and then select **OK**.



- Reset Type: Auto
  The Controller checks if the variables assigned to all the output devices are set to TRUE when detecting that the specified variables are set to TRUE. The test result appears in the dialog shown below. If the devices operate normally as specified in the expected value settings, select the checkbox stating **The device operates normally** and then select **OK**.



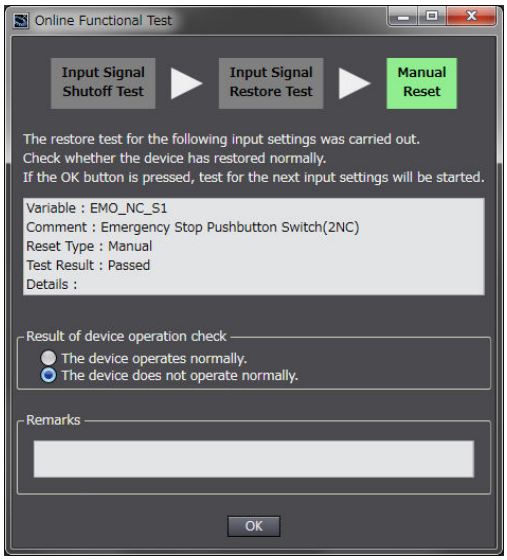
12 Operate the device as instructed on the screen. Execute a function reset.
It is displayed for manual reset only.
The window shows instructions to reset the function, which will allow you to confirm that the tested input device is normally restored. Operate the reset switch as instructed on the screen and change the variable assigned to the reset switch from FALSE to TRUE and then FALSE again.



13 Check the operation of function reset.

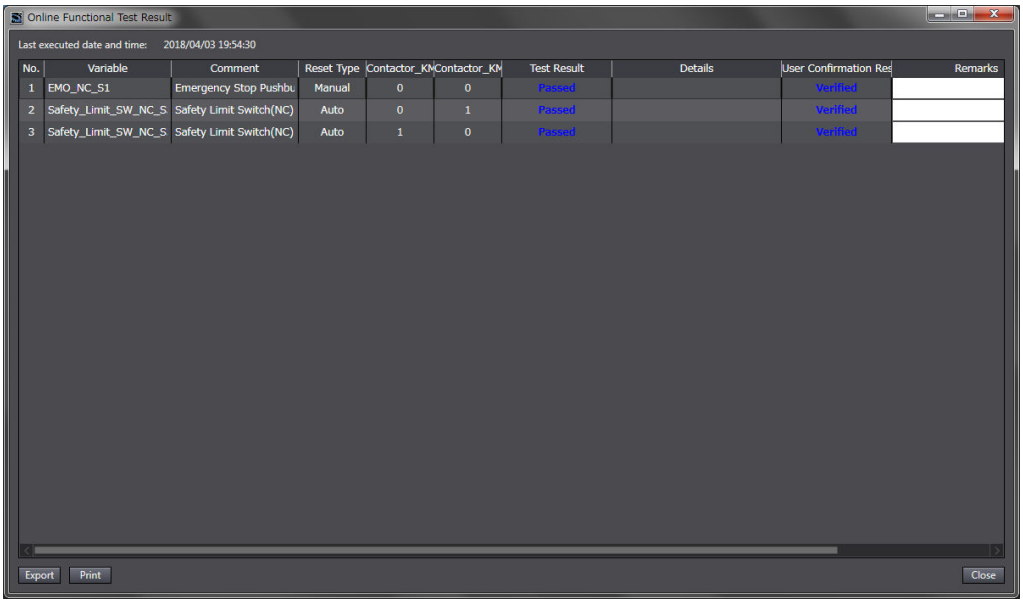
It is displayed only for Manual Reset.

The Controller checks if the variables assigned to all the output devices are set to TRUE when detecting that the variable assigned to the reset switch changed from FALSE to TRUE, and then FALSE again. The test result appears in the dialog shown below. If the devices operate normally as specified in the expected value settings, select the checkbox stating **The device operates normally** and then select **OK**.



14 Repeat the steps 8 through 13 for all the input devices.

Once the operations for all the input devices are completed, the Online Functional Test Result Page shown below appears.



15 Export or print the test results if a CSV file if needed.

Precautions for Correct Use

The Online Functional Test allows you to perform basic operation check by executing manual reset or auto reset. The test result may not be accurate for complex conditions or special cases. Perform advanced operation check separately if needed.

Additional Information

If you print the results of the Online Functional Test, when the safety validation of the safety programs is in process, a safety signature is printed in the lower-right of each page.

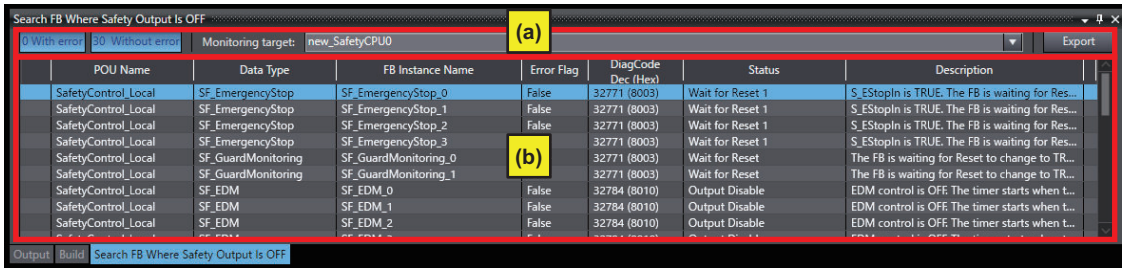
9-8 Search FB Where Safety Output Is OFF

This section describes the function for searching for a function block instance that causes safety output to be turned off in the safety program currently being executed by using Sysmac Studio.
Using this function, you can identify a function block instance where output has been turned off after an input signal had been disrupted or an error had occurred, without analyzing a safety program.

9-8-1 Procedure for Operating Search FB Where Safety Output Is OFF

1 Start Sysmac Studio. Monitor safety application.
For the procedure to start monitoring, refer to *9-12 Starting and Stopping the Safety Application Monitoring* on page 9-64.

2 From the Controller Menu, select **Controller** – **Search FB Where Safety Output Is OFF** – **Start**.
The Search FB Where Safety Output Is OFF window is displayed.



The Search FB Where Safety Output Is OFF window is configured as described in the following table:

Letter	Name	Function	
(a)	Operation panel	This is an operation panel for performing setup or export for Search FB Where Safety Output Is OFF.	
		Total number with error	Displays the total number of function block instances where safety output is turned off due to an error during execution of the relevant function block. You can show or hide this by clicking it.
		Total number without error	Displays the total number of function block instances where safety output is turned off due to a cause other than a function block error, such as input signal disruption. You can show or hide this by clicking it.
		Monitor Target	Select the Safety CPU Unit to monitor. To search for a function block where safety output is off, it is necessary that the Safety CPU Unit be in the RUN or DEBUG mode.
		Export	Exports the current search results to a CSV file.

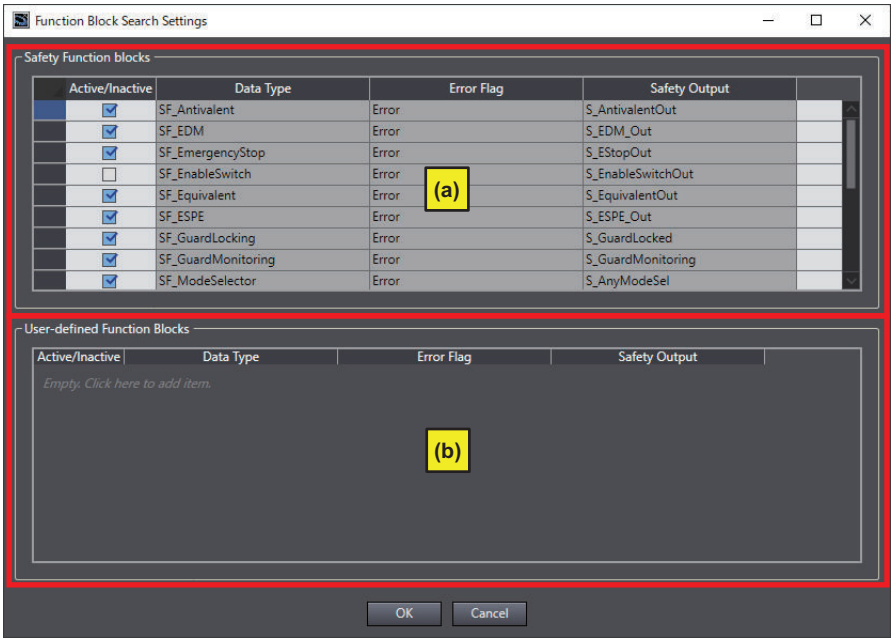
Letter	Name	Function	
(b)	Search results	This section lists function block instances where safety output is turned off in the safety program currently being executed.	
		POU Name	Displays the name of the POU where relevant function block instance is being executed.
		Data Type	Displays the name of the relevant function block.
		FB Instance Name	Displays the name of the relevant function block instance.
		Error Flag	Displays the present value of the output variable set as an error flag on the Function Block Search Settings window.
		DiagCode Dec (Hex)	Displays the present value of the *DiagCode* (diagnostic code), which is an output variable of a safety function block, as decimal and hexadecimal numbers.
		Status	Displays the name of the status described in the Instructions Reference based on the *DiagCode* (diagnostic code).
		Description	Displays the description of the status described in the Instructions Reference based on the *DiagCode* (diagnostic code).

You can jump to the point of execution of a function block instance by double-clicking a row in the search results list.
To display the Help menu for function blocks, select a row in the search results list and press the **F1** key, or right-click a row and select **Display Help**.

9-8-2 Editing Function Blocks to be Searched for

By default, this function searches for safety function blocks. Use the following procedure to exclude function blocks to be searched for or add user-defined function blocks.

From the Controller Menu, select **Controller** – **Search FB Where Safety Output Is OFF** – **Set**.
The Function Block Search Settings window is displayed.



The Function Block Search Settings window is configured as described in the following table:

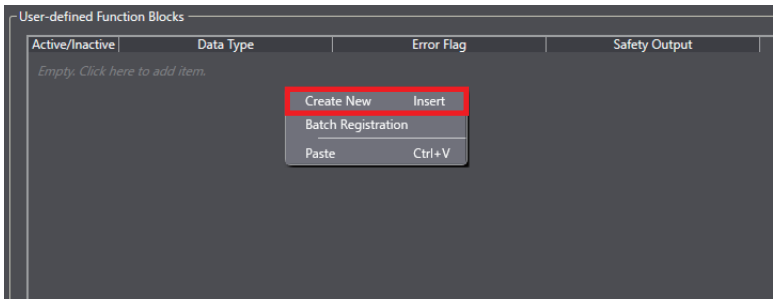
Letter	Name	Description	
(a)	Safety Function block search settings table	Displays search settings for safety function blocks. Search settings are predefined for available safety function blocks by default.	
		Active/Inactive	Select the check box to include the function block as a search target, or clear the selection of the check box to exclude it.
		Data Type	Displays the name of the data type of the target function block.
		Error Flag	Displays the name of the output variable used as an error judgment condition.
		Safety Output	Displays the name of the output variable used as a condition for judging if safety output is off.
(b)	User-defined Function Block search settings table	Displays search settings for user-defined safety function blocks. Set user-defined function blocks to be searched for on Search FB Where Safety Output Is OFF.	
		Active/Inactive	Select the check box to include the function block as a search target, or clear the selection of the check box to exclude it.
		Data Type	Set the name of the data type of the target function block.
		Error Flag	Set the name of a BOOL or SAFEBOOL output variable used as an error judgment condition.
		Safety Output	Set the name of the SAFEBOOL output variable used as a condition for judging if safety output is off.

9-8-3 Registering a Data Type in the Function Block Search Settings Window

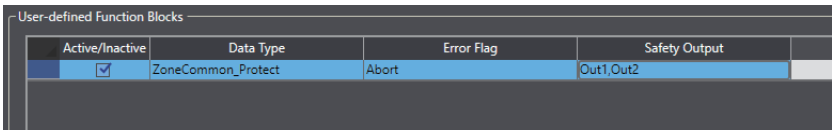
This section describes the procedure for registering a function block to be searched for on the Function Block Search Settings window.

1 From the Controller Menu, select **Controller** – **Search FB Where Safety Output Is OFF** – **Set**.

2 Press the **Insert** Key in the search setting table in User-defined Function Blocks, or right-click in the table and select **Create New** from the menu.



3 Enter necessary items in the added row, and then press the **Enter** key.


User-defined Function Blocks
Active/Inactive
Data Type
Error Flag
Safety Output
ZoneCommon_Protect
Abort
Out1,Out2

9-9 Node Name

This section describes the node name setting for the Safety CPU Unit.

● Node Name Application

The node name is a unique name that you assign to each Safety CPU Unit within the project. This helps you recognize the correct Safety CPU Unit when you begin online operations.
Check the node name that is displayed before you begin operation to prevent you from controlling the wrong Safety CPU Unit.

The node name that you set is stored in the Safety CPU Unit.
The node name that you set is displayed in the confirmation dialog box when you begin online operations.

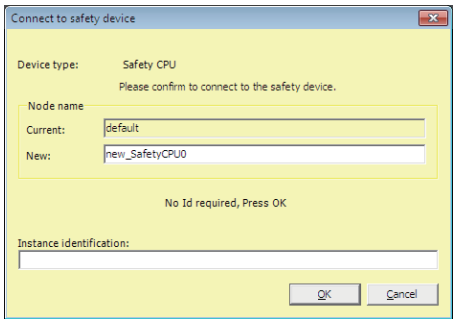
● Characters Allowed for Node Names

The following characters can be used for node names.
The name must have 79 or less printable ASCII characters.
The default node name for all Safety CPU Units is *default*.

● Setting the Node Name

You set the node name in the Connect to safety device Dialog Box, which is displayed when you go online with the Safety CPU Unit. The Connect to safety device Dialog Box is displayed when you perform one of the following operations.

- Connecting the Safety CPU Unit online for the first time with the factory default settings.
- Connecting the Safety CPU Unit online for a new project file after performing online operations for other projects.



Note The factory-default node name is displayed.

Check to see if the destination node is correct. Type a node name and click the **OK** Button.
The node name that you set is stored in the Safety CPU Unit. After this point of time, the new node name is displayed in the confirmation dialog box, which appears before you start online operations on the Safety CPU Unit.

Precautions for Correct Use

Set a unique node name for the Safety CPU Unit.

9-10 Security Settings

You can use the Sysmac Studio to restrict operations and to protect POUs (programs and function blocks) in order to prevent unauthorized access to safety functions and to protect assets.

An overview of the applications and functions of security settings is given below.

Function	Application	Outline of function
Safety Password	To prevent unauthorized access to safety functions	You can set a password for the Safety CPU Unit in order to prevent unauthorized operations, including changing the operating mode and performing the Clear All Memory operation.
Data Protection	To protect assets	You can set passwords for POUs (programs and function blocks), so that they cannot be individually displayed or changed.

9-10-1 Setting the Safety Password

This section describes the safety password setting for the Safety CPU Unit.

● Safety Password Application

The safety password prevents unauthorized access to the safety functions of the Safety CPU Unit. When a safety password is set, the user is required to enter the password before performing an operation that affects the safety functions.

After you enter the safety password, it is retained in the Sysmac Studio. You do not need to enter it again until you take the Safety CPU Unit offline or close the project.

The safety password protects the following online operations on the Safety CPU Unit.

- Changing the operating mode (This does not apply when changing between DEBUG mode (STOPPED) and DEBUG mode (RUN).)
- Downloading (transferring data from the Computer to the Controller)
- Uploading (transferring data from the Controller to the Computer)
- Changing the safety password
- Clear All Memory operation*1
- Performing safety validation

*1. The password must be entered each time for this operation.

The safety password is empty by default.

You can set a safety password before or after you perform safety validation.

Precautions for Correct Use

- For security purposes, we recommend that you set a safety password for the Safety CPU Unit.
- If you lose the password set to the Safety CPU Unit, you will no longer be able to make changes to the Safety CPU Unit. Take caution not to lose the password. If the password is lost and needs to be reset, contact your OMRON representative.

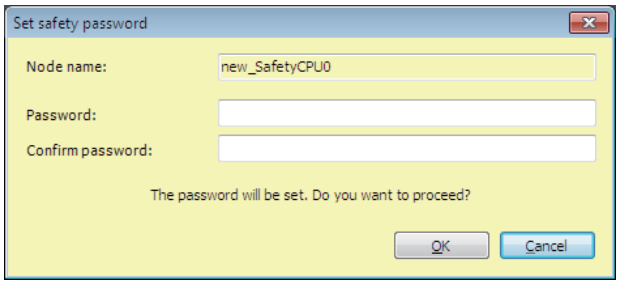
● Characters Allowed for Passwords

The following characters can be used for the password.

Item	Description
Number of Characters	32 characters max.
Applicable Characters	Single-byte alphanumeric characters (case sensitive)

● Setting a New Safety Password

1 Go online with the Safety CPU Unit and then select **Security** − **Set Safety Password** from the **Controller** Menu on the Safety CPU Unit Setup and Programming View.
The **Set safety password** Dialog Box is displayed.



2 Enter the safety password in the **Password** Box. Enter the same password in the Confirm password Box, and click the **OK** Button.
The password is set.

Additional Information

We recommend that you set text strings that contain both letters and numbers.
The login name and password are case sensitive.
Do not use words that would be easily guessed by another person, words that are in dictionaries, or text strings like abcdefg.

9-10-2 Data Protection

This section describes the data protection of the Safety CPU Unit.

● Data Protection

The data protection function allows you to set passwords for individual data units to restrict displaying and changing them (access restrictions). You can enter the password to temporarily release the protection from a data unit. Data protection is set and released offline.

● Types of Access Restrictions

The following table describes the types of access restrictions.

Access restriction	Operation	Remarks
Display prohibition	The restricted data cannot be displayed.	This restriction applies to jumping from other windows, viewing search results, and printing previews.
Change prohibition	The restricted data cannot be changed. The data can be displayed but not changed on the display.	This restriction applies to changing or replacing text in POU names.

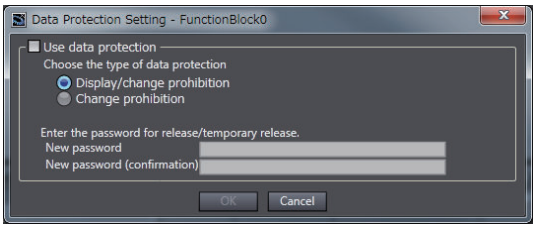
● Data That Can Be Protected

The following table lists the data that you can protect from being displayed and changed.

Target data		Display prohibition		Change prohibition	
		Display	Change	Display	Change
Program	**Program names**	Possible	Not possible	Possible	Not possible
	Variable tables	Not possible	Not possible	Possible	Not possible
	FBD editor	Not possible	Not possible	Possible	Not possible
Function Block	**Function block names**	Possible	Not possible	Possible	Not possible
	Variable tables	Not possible	Not possible	Possible	Not possible
	FBD editor	Not possible	Not possible	Possible	Not possible

● Procedure to Set Protection

1 Select the data to protect, and then select**Security**−**Set/Release Data Protection**from the**Controller**Menu. Or right-click the data to protect, and select**Security**−**Set/Release Data Protection**from the menu.
The Data Protection Setting Dialog Box is displayed.



2 Select the**Use data protection**Check Box and select the access restrictions. Enter the password, and click the**OK**Button.
Data protection is set and the icon on the protected data changes in the Multiview Explorer.

Icon	Description
	Data protection is disabled.
	Data protection is enabled.

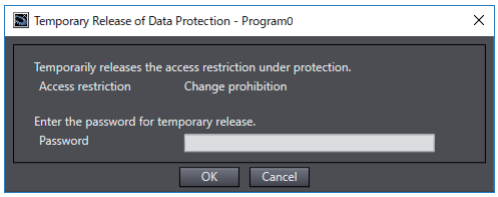
Precautions for Correct Use

- You will not be able to temporarily release protection or remove the protection setting if you forget the password. Protection settings are also transferred for synchronization operations. If you forget the passwords for protected data that was transferred to the Controller, you will no longer be able to display or change the protected data. Record the password in case you forget it.
- If you change the data protection setting, the safety program in the project will change to an unvalidated state. Execute safety validation again.

● Temporarily Releasing Protection

To perform operations on protected data, you can enter the password to temporarily release the protection.

1 Perform the restricted operation for the protected data. When you temporarily release data protected with **Change prohibition**, right-click the data and select **Security** − **Temporary Release of Change Prohibition** from the menu.
The Temporary Release of Data Protection Dialog Box is displayed.



2 Enter the password that was set when data protection was set.
The access restrictions are temporarily released.
The following table gives the lengths of time for which the access restrictions are temporarily released.

Access restriction	Length of time that protection is cleared
Display prohibition	While the project is open
Change prohibition	While the project is open While the project is open or until **Finish Temporary Release of Change Prohibition** is selected from the menu

The Sysmac Studio is locked for 10 minutes if you consecutively enter wrong passwords 5 times for the same Controller. The Temporarily Release of Data Protection Dialog Box is displayed again in 10 minutes.

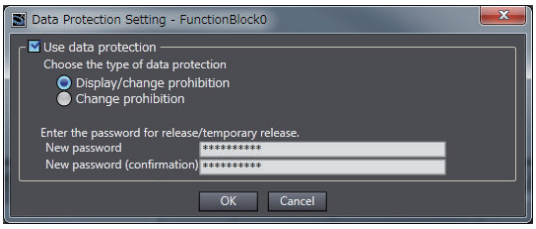
Precautions for Correct Use

Even if the access restrictions for **Display prohibition** are set, the Temporary Release of Data Protection Dialog Box is not displayed for printing or printing previews.
Display the data from the Multiview Explorer and temporarily release protection before you use printing or print previews.

● Procedure to Release Protection

1 Select the data for which to release protection, and then select **Security** − **Set/Release Data Protection** from the **Controller** Menu. Or right-click the data for which to release protection, and select **Security** − **Set/Release Data Protection** from the menu.
The Temporary Release of Data Protection Dialog Box is displayed.

2 Enter the password, and click the **OK** Button.
The Data Protection Setting Dialog Box is displayed.



3 Clear the **Use data protection** Check Box and click the **OK** Button.
Data protection is released and the protection icon returns to the normal icon.

● Data Protection Version

You can increase the level of protection for POU data by setting a higher Data Protection Version. The Data Protection Version can be set for each Safety CPU Unit. We recommend setting a higher Data Protection Version.

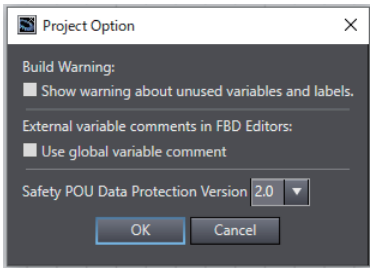
Version Information

- You can set Data Protection Version with Sysmac Studio version 1.54 or higher.
- If a new project is created, the Data Protection Version is 1.0. Set a higher version if necessary.

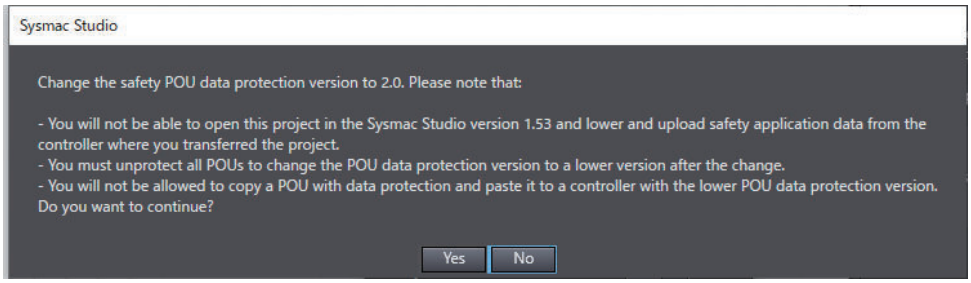
● Procedure to Change the Data Protection Version

1 Select **Project Option** from the **Project** Menu on the Safety CPU Unit Setup and Programming View.

2 Select the Safety POU Data Protection Version in the Project Option Dialog Box, and then click the **OK** Button.

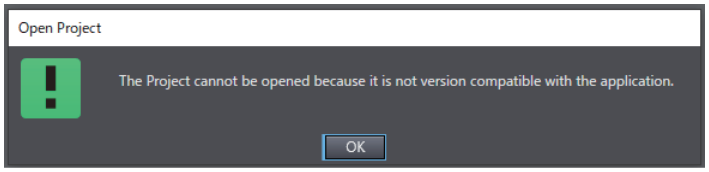


3 Check the contents of the confirmation message to change the Data Protection Version, and then click the **Yes** Button.



Precautions for Correct Use

- The Data Protection Version cannot be lowered unless the protection setting is released. Refer to *Procedure to Release Protection* on page 9-56 for the procedure for releasing data protection settings.
- A project whose Data Protection Version is set to 2.0 cannot be opened with Sysmac Studio version 1.53 or lower. The following message is displayed.



- If you set a lower Data Protection Version, use it only for the purpose of maintaining compatibility with lower versions of Sysmac Studio.

9-11 Performing Safety Validation and Operation

This section describes the procedure for safety validation testing. Safety validation testing is used to confirm that all safety functions and all Safety Control Units meet the required specifications of the safety system. If safety validation testing demonstrates that the safety controls meet the required specifications of a safety system, the safety application data is appended with confirmation information through a process called "safety validation".
When you perform safety validation on a Safety CPU Unit that is operating in DEBUG mode, the safety application data is saved in the non-volatile memory of the Safety CPU Unit.
Note that a safety program for which safety validation has been performed is saved in the project file as a validated program with a safety signature assigned.

This section describes how to perform safety validation and start operation after you have debugged the safety programs.

9-11-1 Performing Safety Validation

You must perform safety validation before you change Safety CPU Unit to the RUN mode and start any safety control system that uses safety application data*1 that is created with Sysmac Studio.
You perform safety validation after you perform safety validation testing with the Safety CPU Unit in DEBUG mode (RUN) to make sure that all safety functions operate as intended.
To perform safety validation, it is necessary that the Safety CPU Unit be in DEBUG mode.

*1. The safety application data includes the safety programs and the safety task settings and variables. Refer to *9-1 Procedures before Operation and Transferring the Required Data* on page 9-3 for details.

⚠ WARNING

Before you perform safety validation of the safety programs, complete debugging of the safety programs.

Otherwise, the Safety CPU Unit will start with safety programs that are not fully debugged and may cause serious personal injury.

⚠ WARNING

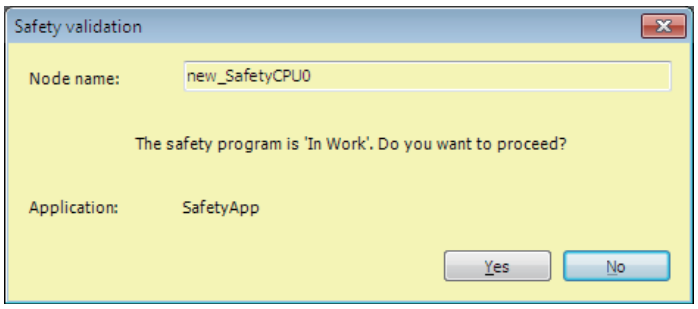
Verify the calculated reaction times for all safety chains to confirm that they satisfy the required specifications.
Serious injury may possibly occur due to loss of required safety functions.

Additional Information

You can manage changes in the safety application data before you perform safety validation after debugging is completed, or after you perform safety validation. Refer to *A-5 Change Tracking* on page A-67 for details.

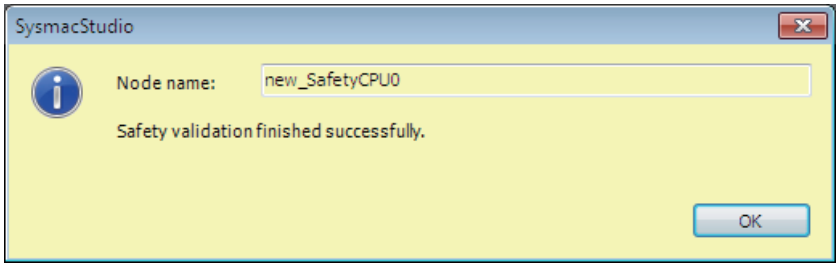
● Performing Safety Validation

1 Connect the Sysmac Studio online with the Safety CPU Unit, place the Safety CPU Unit in DEBUG mode, and select **Safety Validation** from the **Controller** Menu.
The following confirmation dialog is displayed.



2 Click the **Yes** button.
After the validated safety programs are saved to non-volatile memory in the Safety CPU Unit, the following dialog is displayed to indicate the process was completed, and then the Safety CPU Unit enters the state shown below.

- Safety CPU Unit is set to the validated state, and assigned with a safety signature.
- The safety program in the project file is set to the validated state, and assigned with a safety signature.
- The VALID indicator of the Safety CPU Unit changes from not lit to lit yellow.
- When you cycle the power, the Safety CPU Unit starts in RUN mode.



3 Click the **OK** button.

Precautions for Safe Use

Note that the Safety CPU Unit automatically starts in RUN Mode at the next start-up if the safety validation is successful.
When you download the parameters for the Communication Control Unit and NX Units, the Safety CPU Unit automatically restarts.

● Checking the Validated State

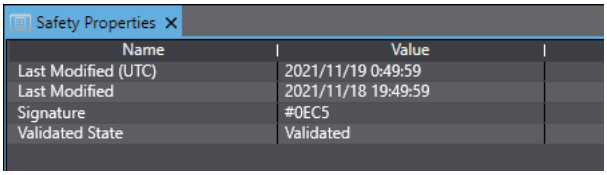
Use the following procedure to check if the safety program in the project has been validated.

1 Start Sysmac Studio. Open a project containing safety application data.

2 In the Multiview Explorer, select Safety CPU Unit from Controller Selection.

3 From the Controller Menu, select **Project** – **Safety Properties**.

The following window is displayed.



The contents of each item are described in the following table.

Item	Description
Last Modified (UTC)	The time on the computer on which safety validation has been performed.
Last Modified	
Signature	Displays the signature code (four-digit hexadecimal number) of the validated safety program. **---** is displayed if safety validation has not been performed.
Validated State	Displays whether safety validation has been performed.

If *Validated* is displayed for Validated State, the safety program in the project file has been validated.

9-11-2 Changing to RUN Mode

After you perform safety validation, you can change the Safety CPU Unit to RUN mode.
Use one of the following procedures to change the Safety CPU Unit to RUN mode.

- Cycle the power supply to the Safety CPU Unit
- Change to RUN mode via the Sysmac Studio.

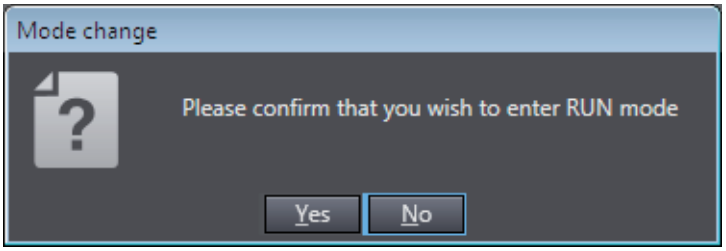
Change to RUN Mode via the Sysmac Studio

The safety programs must be validated.

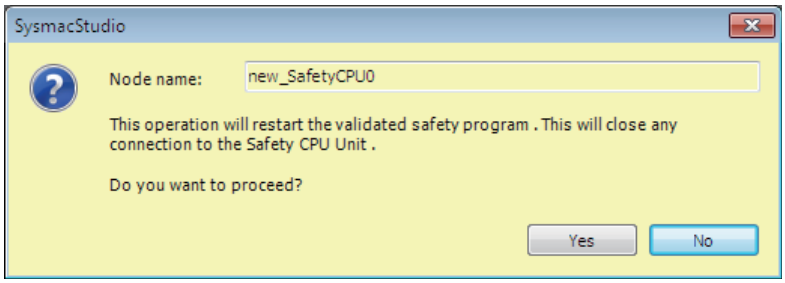
1 With the Safety CPU Unit connected online, perform one of the following operations on the Safety CPU Unit Setup and Programming View.

- Select **Mode** – **RUN Mode** from the **Controller** Menu.
- Press the **Ctrl** + **3** Keys.
- Click the **RUN Mode** Button on the toolbar.

A confirmation dialog box is displayed.



Click the **Yes** Button. A dialog box is displayed to confirm the node.



2 Check the node name, and click the **Yes** Button.
A Mode Change Confirmation Dialog Box is displayed. Click the **OK** Button to change the Safety CPU Unit to RUN mode.

9-11-3 Changing to PROGRAM Mode

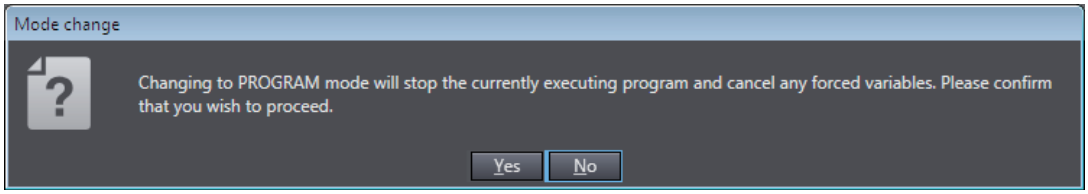
If you need to change the safety programs, or if you need to change the operating mode of the Safety CPU Unit from RUN mode to DEBUG mode, you must first change to PROGRAM mode.

Changing to PROGRAM Mode

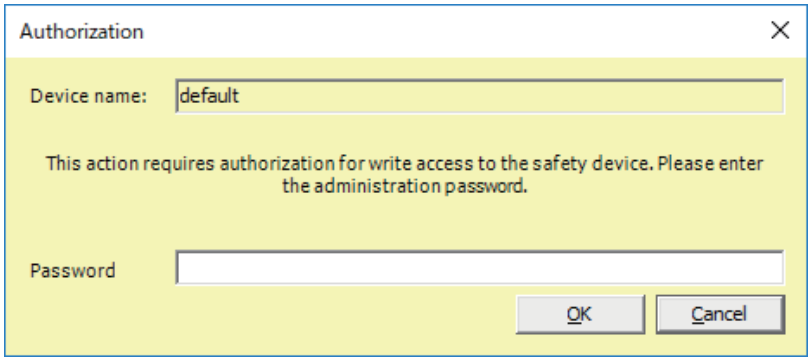
Use the following procedure to change the Safety CPU Unit from RUN mode to PROGRAM mode.

1 With the Safety CPU Unit connected online, perform one of the following operations.
- Select **Mode** – **PROGRAM Mode** from the **Controller** Menu.
- Press the **Ctrl** + **1** Keys.
- Click the **PROGRAM Mode** Button on the toolbar.

A confirmation dialog box is displayed.

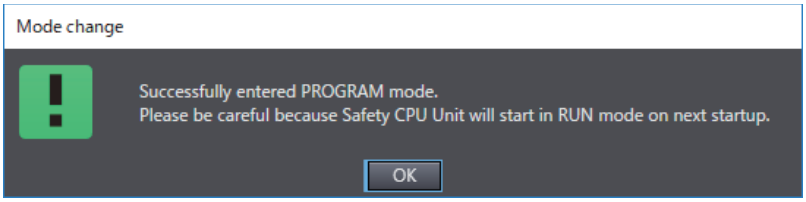


When you click the **Yes** Button, a dialog box to confirm the Safety Password appears.



2 Enter the safety password, and click the **OK** Button.
The Safety CPU Unit enters PROGRAM mode.

The following dialog box is displayed.



Click the **OK** Button.

9-12 Starting and Stopping the Safety Application Monitoring

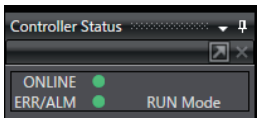
This section describes how to start and stop the monitoring function for variables and the Safety I/O Unit by using Sysmac Studio. This function can be executed only when the Safety CPU Unit is in the RUN mode.
For details on monitoring the variables, refer to *9-6-3 Monitoring Variables in the FBD Editor* on page 9-23 and *9-6-4 Monitoring Variables in a Watch Tab Page* on page 9-24. For details on monitoring the Safety I/O Unit, refer to *9-5-2 Monitoring Safety I/O Units* on page 9-16.

9-12-1 Procedure to Start and Stop the Safety Application Monitoring

1 Make sure that the Safety CPU Unit is in the RUN mode.

2 Connect to Safety CPU Unit online.

3 Select Safety CPU Unit from the Controller Selection Box in the Multiview Explorer of Sysmac Studio and open the Safety CPU Unit Setup and Programming View.
When you open the view for the Safety CPU Unit, the Controller status is displayed in the lower-right corner of the screen as shown below.

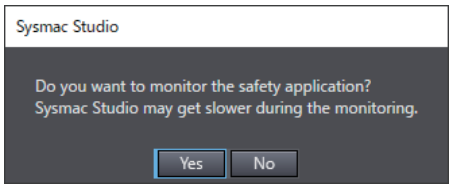


4 On the Safety CPU Unit Setup and Programming View, perform one of the following operations.

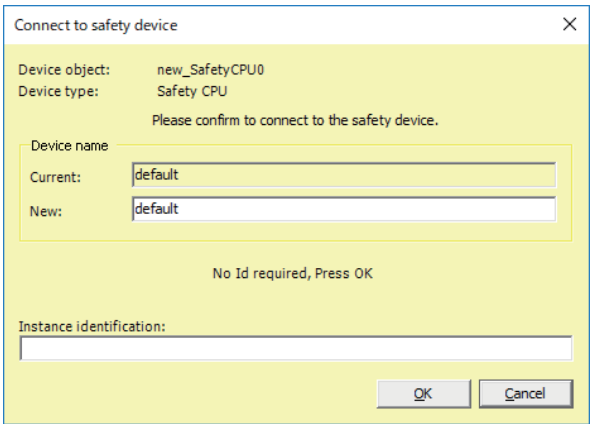
To Start Monitoring:

- On the menu bar, select **Controller** - **Monitor**.
- Click the **Monitor** Button on the toolbar.

Before monitoring starts, the following confirmation dialog box appears. Click the **Yes** button.



A confirmation dialog box for connection to a safety device is displayed. Click the **OK** button.



To Stop Monitoring:

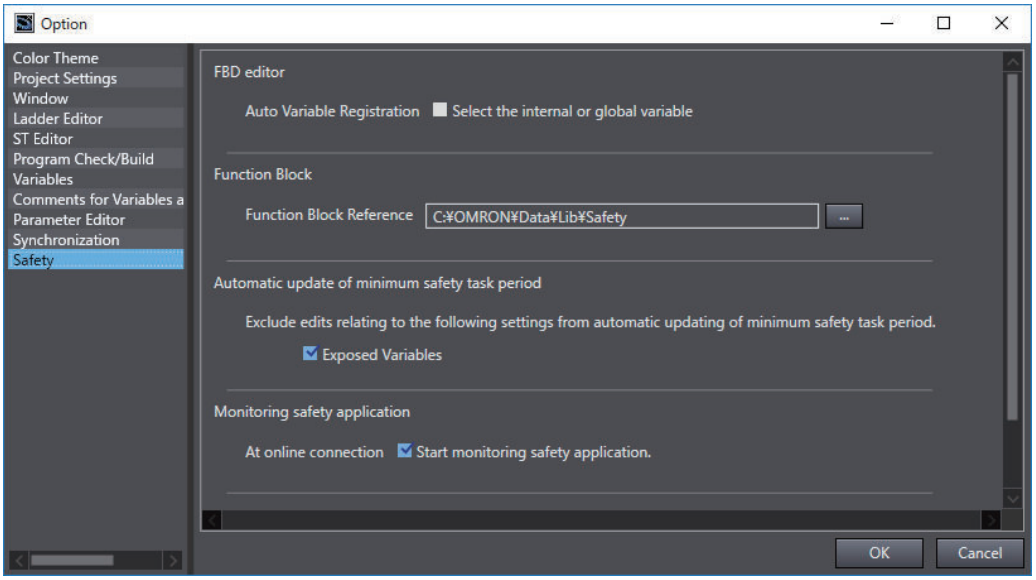
- On the menu bar, select **Controller** - **Stop Monitoring**.
- Click the **Stop Monitoring** Button on the toolbar.

9-12-2 Changing the Monitoring Options for the Safety Application

You can select whether you will start the safety application monitoring when Sysmac Studio is connected online. Use the following procedure.

1 On the menu bar, select **Tools** - **Option**.
The **Option** Dialog Box is displayed.

2 Click the **Safety** Tab.
The monitoring options for the safety application will appear.



3 Specify the option **At online connection Start monitoring safety application** and click the **OK** Button.
If this option is disabled, the safety application monitoring will not start. For the procedure to start monitoring, refer to *9-12-1 Procedure to Start and Stop the Safety Application Monitoring* on page 9-64.

9-13 Uploading Configuration Information and Safety Application Data

This section describes how to transfer the configuration information and safety programs from the Safety Control Units to the computer with the Sysmac Studio.

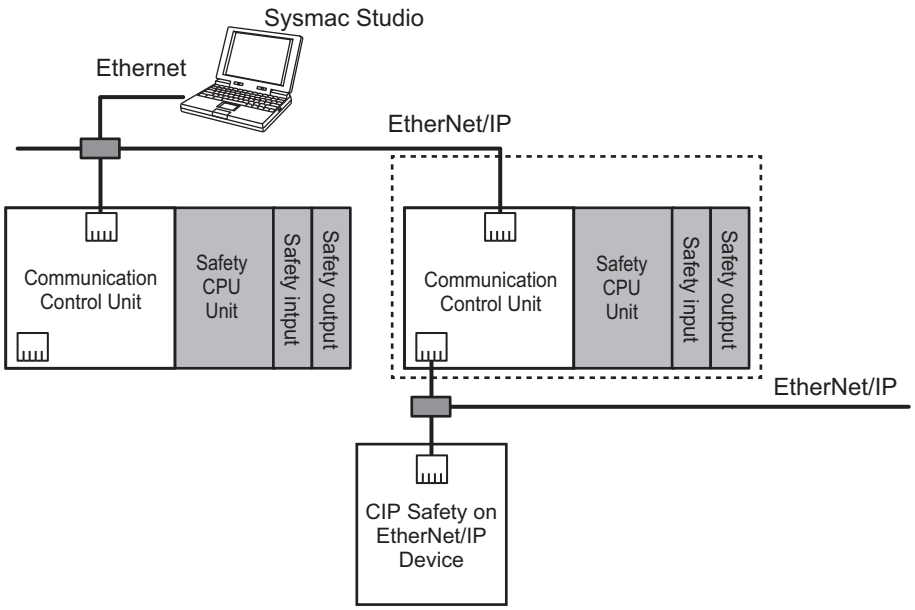
9-13-1 Outline

You can transfer the settings of the Safety Control Units and the safety programs from the Safety Control Units to the computer.

Paths for Going Online

Connect the Sysmac Studio online to the Safety CPU Unit via a Ethernet connection with the Communication Control Unit.

A configuration example is given below.



9-13-2 Upload Procedures

You can connect the Sysmac Studio to the Ethernet port on the Communication Control Unit to upload the configuration information and safety application data.
Use the following procedure to upload the data.

1 Select the Communication Control Unit from the Controller Selection Box in the Multiview Explorer on the Sysmac Studio to change to the Communication Control Unit Setup and Programming View.

2 Set the communications path to the Communication Control Unit.

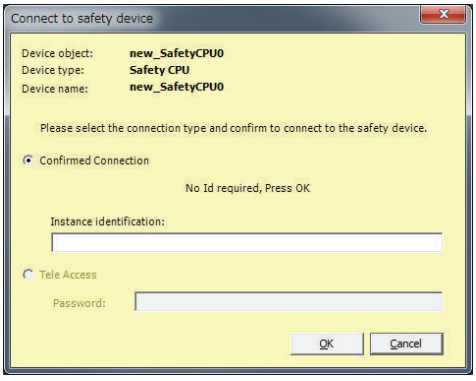
3 Select **Online** from the **Controller** Menu. Or, click the **Go Online** Button ( ) in the toolbar.

4 Select **Synchronization** from the **Controller** Menu.

5 In the Synchronization Window, clear the selections of the following check boxes.
- Do not transfer the following. (All the items are not to be synchronized.)
- NX Unit application data on the CPU Rack

6 Click the **Transfer From Controller** Button.
An execution confirmation dialog box is displayed.

7 Click the **Yes** Button.
The following **Connect to safety device** Dialog Box is displayed.



Note You do not need to enter anything in the *Instance identification* Box.

8 Click the **OK** Button.
A password confirmation dialog box is displayed.

9 Enter the password, and click the **OK** Button.
The settings of all the Units that are connected to the Communication Control Unit are transferred to the Sysmac Studio.

9-14 Transferring Safety Application Data

This section describes how to transfer safety application data that was validated in the procedure specified in the preceding section *9-11 Performing Safety Validation and Operation* on page 9-59 to another Safety CPU Unit.

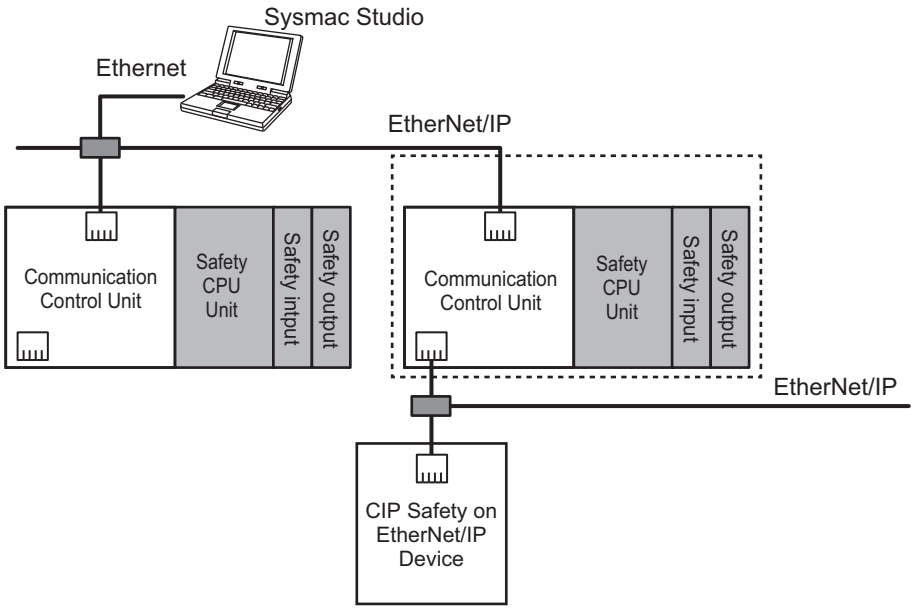
9-14-1 Outline

You can transfer the settings of the Safety Control Units and the safety programs that perform safety validation from the computer to the Safety Control Units.

Paths for Going Online

Connect the Sysmac Studio online to the Safety CPU Unit via a Ethernet connection with the Communication Control Unit.

A configuration example is given below.



9-14-2 Transfer Procedure

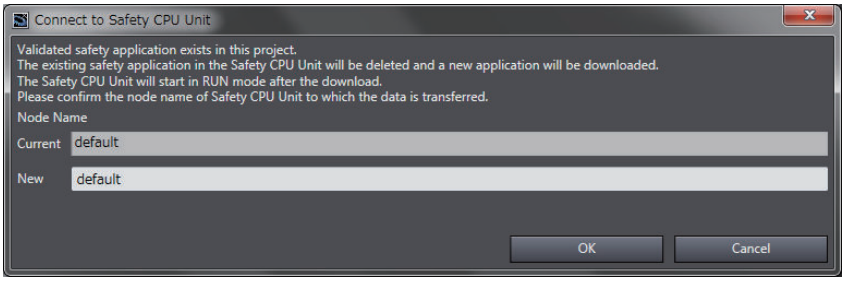
1. Select the Communication Control Unit from the Controller Selection Box in the Multiview Explorer on the Sysmac Studio to change to the Communication Control Unit Setup and Programming View.
2. Set the communications path to the Communication Control Unit.
3. Select **Online** from the **Controller Menu**. Or, click the **Go Online** Button ( ) in the toolbar.

4 Select **Synchronization** from the **Controller** Menu.

5 In the Synchronization Window, clear the selections of the following check boxes.
- Do not transfer the following. (All the items are not to be synchronized.)
- NX Unit application data on the CPU Rack

6 Click the **Transfer to Controller** Button.
An execution confirmation dialog box is displayed.

7 Click the **Yes** Button.
The following **Connect to Safety CPU Unit** Dialog Box is displayed.



8 Click the **OK** Button.
A password confirmation dialog box is displayed.

9 Enter the password, and click the **OK** Button.
The settings of all the Units that are connected to the Communication Control Unit are transferred from the Sysmac Studio.

9-15 Monitoring Controller Status

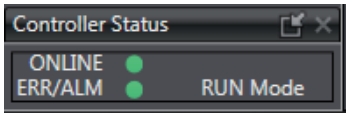
This section describes how to display the status of Safety CPU Unit that is connected to Safety CPU Unit online or the status when the Simulator is connected.

Controller Status Monitor

Control status monitoring is used to display the status of the connected Safety CPU Unit or Simulator in the Controller Status Pane. The Controller Status Pane is displayed when the Sysmac Studio is online or the Simulator is connected.

Displaying the Controller Status Pane

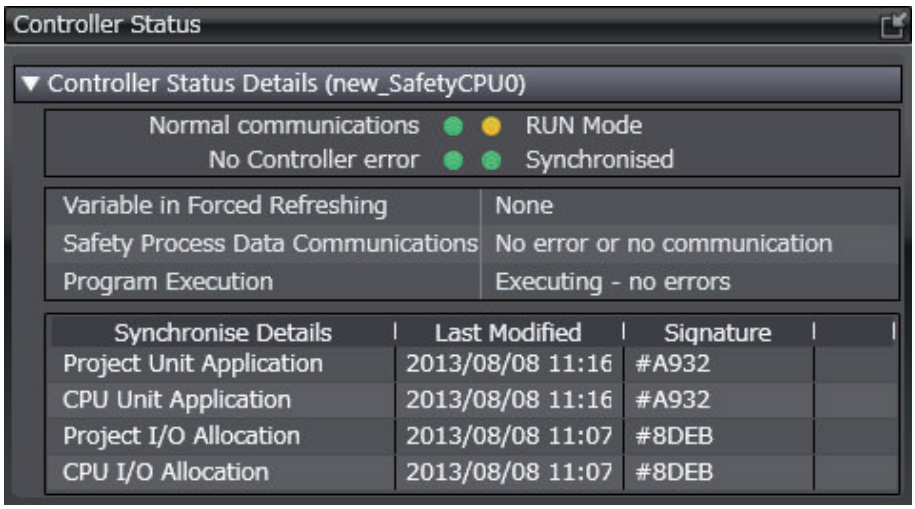
The basic view of the Controller Status Pane is displayed in the Toolbox in the lower right corner of the Safety CPU Unit Setup and Programming View when the Safety CPU Unit is online or the Simulator is connected.



Expansion Operations in the Controller Status Pane

Use the buttons () in the title bar of the Controller Status Pane to switch between the basic and detailed views.

- Detailed View



Information	Displayed information and indicator colors
Communications Status	Displays the communications status between the Safety CPU Unit and Sysmac Studio or displays the Simulator startup status. • Normal communications: Lit green • Communications error: Flashing red
Error Status	Displays the error status of the Safety CPU Unit or Simulator. • No Controller error: Lit green • Partial or minor fault level Controller error occurs: Lit yellow.
Operating Mode	Displays the operating mode of the Safety CPU Unit. • RUN Mode: Lit yellow. • DEBUG mode (RUN): Flashing yellow. • DEBUG mode (STOPPED): Flashing yellow. • PROGRAM Mode: Not lit. • UNKNOWN Mode: Flashing red.
Synchronization Status	Displays the comparison results between the project file on the computer and the data in the Safety CPU Unit. • Synchronized: Lit green. • Not synchronized/not executed: Lit yellow.
Variable in Forced Refreshing	Displays the forced-refreshing status of variables in the safety programs. • None • Present
Safety Data Communications	Displays the status of communications between the Safety CPU Unit and Safety I/O Units. • No error or no communications • Communications error
Program Execution	Displays the execution status of the safety programs. • Executing - no errors • Executing - instruction execution error • Not executing
Synchronise Details	Displays the synchronization information item, last modified date, and signature (CRC data).



Additional Information

You can use the color of the top of the Edit Pane to check if you are online with the Safety CPU Unit or connected to the Safety Simulator.

- Connected to the Safety CPU Unit online
  The top of the Edit Pane is yellow.
- Connected to the Safety Simulator:
  The top of the Edit Pane is green.

9-16 Restarting and Clearing All Memory

9-16-1 Restarting

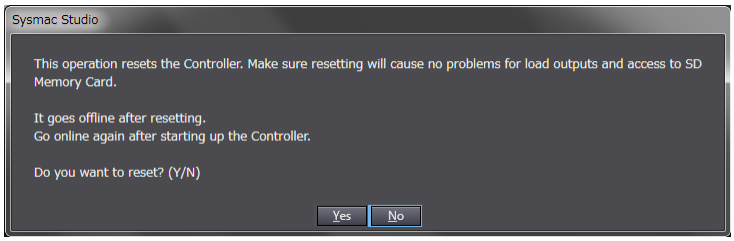
Restarting allows you to restart the CPU Rack that includes the Safety CPU Unit and Safety I/O Units without cycling the unit power supply to the Communication Control Unit.

Precautions for Safe Use

If the safety application data in the Safety CPU Unit is validated, be careful when you execute the Restart operation because the Safety CPU Unit will automatically start in RUN mode.

Use the following procedure to restart all of the Units on the CPU Rack.

1 Go online, and select **Controller** – **Reset Controller** from the Communication Control Unit Setup and Programming View.
The following confirmation dialog box is displayed.



2 Click the **Yes** Button.
After the Units are restarted, a Restart Completion Dialog Box is displayed.

9-16-2 Clear All Memory Operation

For the Clear All Memory operation, you use the Sysmac Studio to initialize the contents of the Safety CPU Unit and Safety I/O Units to the default settings.
The Clear All Memory operation can be performed in the following two ways.

Type	Function
Clear All Memory operation for NX Units	This method clears all memory contents from the Safety CPU Unit and Safety I/O Units.
Clear All Memory operation for Controllers	This method clears all memory from the Communication Control Unit and all NX Unit, including the Safety I/O Units that are connected to the Communication Control Unit. The Safety CPU Unit memory cannot be cleared.

Precautions for Correct Use

- The memory in the Safety CPU Unit is not cleared even when you perform the Clear All Memory operation for controllers. To clear the memory of the Safety CPU Unit, use the Clear All Memory operation for NX Units.
- You can execute the Clear All NX Unit Memory operation for a Safety CPU Unit only when the Safety CPU Unit is in PROGRAM mode.

Scope of Data to Clear and State of Memory After It Is Cleared

Safety CPU Unit

Data item	Status after clear all memory operation
I/O allocation information	This data is set to the default settings (I/O size = 0 bytes).
Safety programs	This data is set to the default settings (no programs).
Safety password	This data is set to the default settings (no password).
Event logs	Event logs are cleared if you select the Clear the event logs Option when you execute the Clear All Memory operation.

Safety I/O Units

Data item	Status after clear all memory operation
FSoE slave address	This data is set to the default setting (no setting).
Event logs	Event logs are cleared if you select the Clear the event logs Option when you execute the Clear All Memory operation.

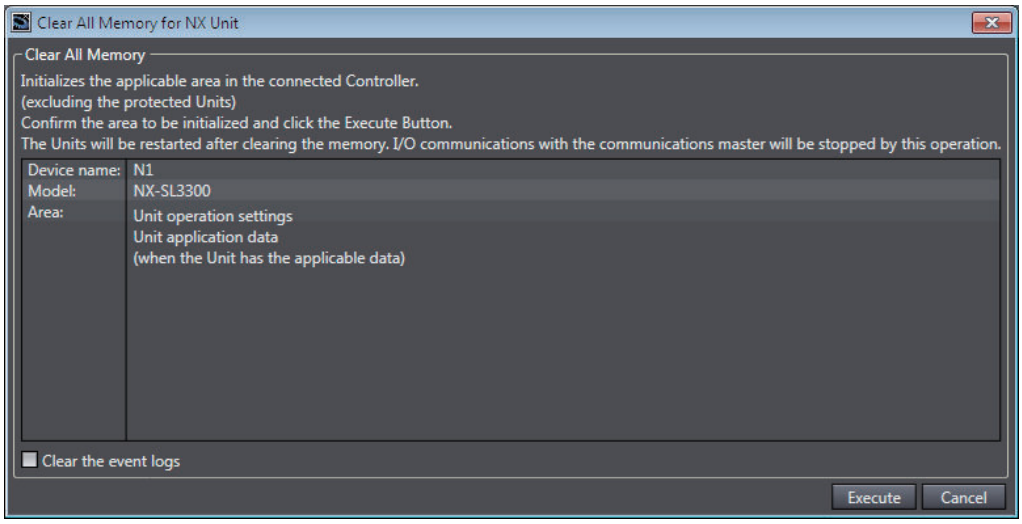
Precautions for Safe Use

After you clear the memory, the Controller operates in the same way as immediately after you create the system configuration with the Controller in the factory default condition.

Procedure for Clear All Memory Operation

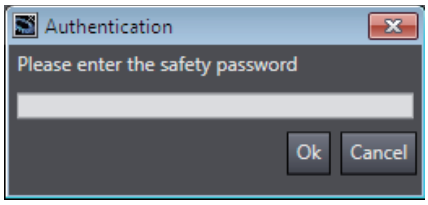
Clear All Memory Operation for Units

1 Go online, right-click the Safety CPU Unit on the CPU Racks Tab Page or the Safety I/O Units, and select **Clear All Memory** from the menu. You can select this menu command only when the Safety CPU Unit is in PROGRAM mode.
The Clear All Memory Dialog Box for the NX Unit is displayed.

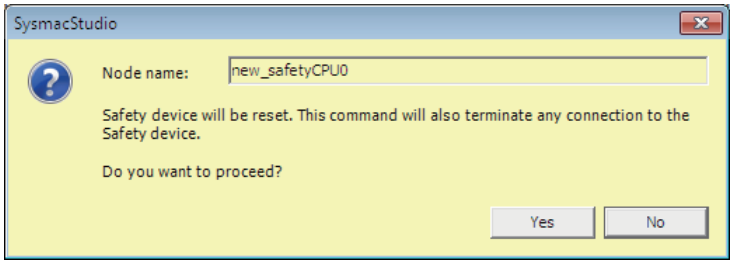


2 Click the **Execute** Button. The Clear All Memory Confirmation Dialog Box is displayed.

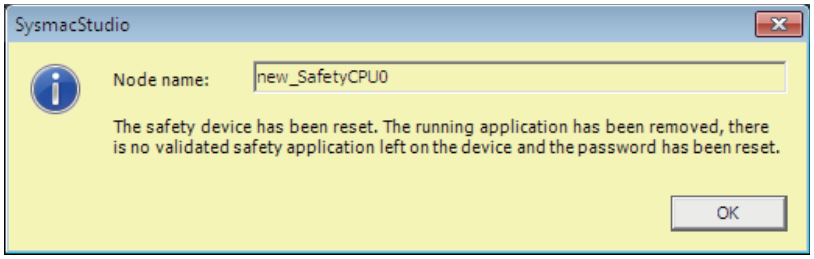
3 Click the **Yes** Button. The **Authentication** Dialog Box is displayed.



4 Enter the password, and click the **OK** Button. If a password is not set, leave the box empty and click the **OK** Button.
A dialog box is displayed to confirm the node.



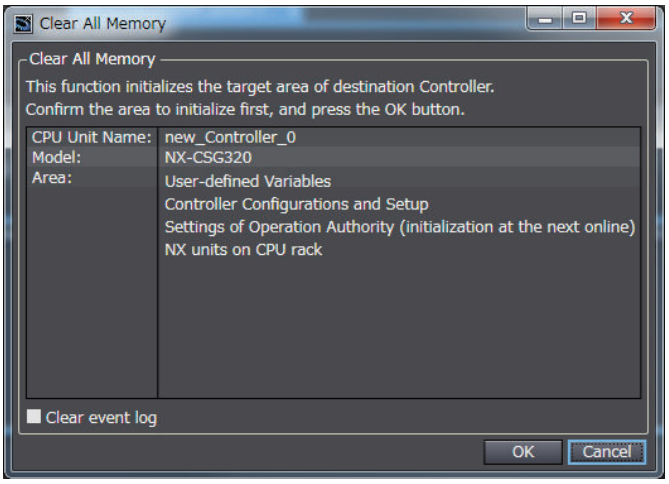
5 Click the **Yes** Button. The following dialog box is displayed.



6 Click the **OK** Button.
After memory is cleared, the Memory All Cleared Dialog Box is displayed.

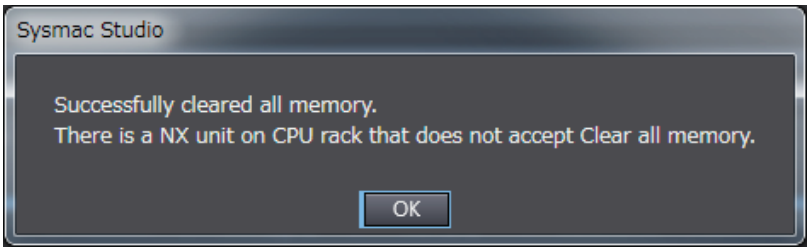
● Clear All Memory Operation for Controllers

1 Go online, and select **Controller** – **Clear All Memory** from the Communication Control Unit Setup and Programming View.
The **Clear All Memory** Dialog Box is displayed.



2 Check the areas to clear and then click the **OK** Button.
- To clear the event logs, select the **Clear the event logs** check box.

After memory is cleared, the Memory All Cleared Dialog Box is displayed.



10

Calculating Safety Reaction Times

This section describes how to calculate safety reaction times for Safety Control Units.

10-1 Safety Reaction Time 10-2
10-1-1 Calculating the Safety Reaction Time 10-2
10-1-2 Verifying Safety Reaction Times 10-4

10-2 Safety Task 10-5
10-2-1 Safety Task 10-5
10-2-2 Operation of Safety Task 10-5
10-2-3 Minimum Safety Task Period 10-5
10-2-4 Setting the Safety Task Period 10-6

10-3 FSoE Watchdog Timer 10-7
10-3-1 FSoE Watchdog Timers 10-7
10-3-2 Checking FSoE Watchdog Timers 10-7
10-3-3 Changing FSoE Watchdog Timers 10-7

10-4 EPI (Data Packet Interval) 10-9
10-4-1 Changing the EPI 10-9
10-4-2 EPI Restrictions 10-9

10-1 Safety Reaction Time

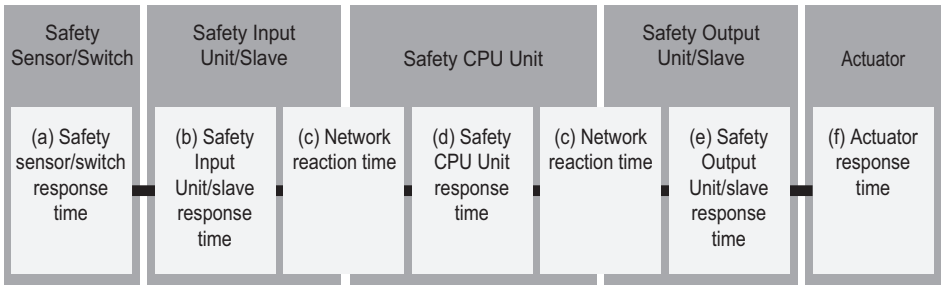
This section describes the safety reaction time (i.e., the safety response performance) of Safety Control Units.
The safety reaction time is the maximum time required to turn OFF an output in consideration of possible failures and breakdowns over safety chains*1. In the safety system design, the safety distance is calculated based on the safety reaction time. For all safety chains, the longest time required to stop moving equipment from when a safety input was activated must satisfy the required specifications.

*1. The safety chain is the logical connections that are required to achieve a safety function, including the safety input device, Safety Control Units, and the safety output device.

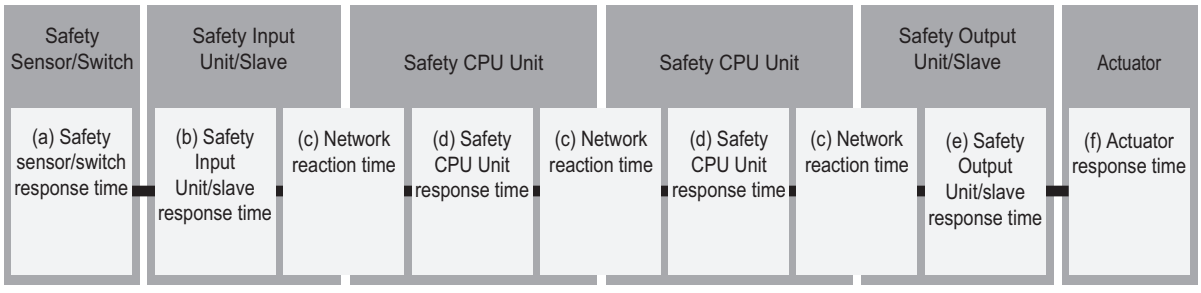
10-1-1 Calculating the Safety Reaction Time

As shown in the figure below, the safety reaction time is the sum of (a) safety sensor/switch response time, (b) Safety Input Unit/slave response time, (c) Network reaction time, (d) Safety CPU Unit response time, (e) Safety Output Unit/slave response time, and (f) actuator response time. The number of elements and the duration of time vary depending on the safety chain route.

Basic Configuration



Network Configuration between Controllers



Details of each time element are described in the following table.

Letter	Time element	Description
(a)	Safety sensor/ switch response time	This is the response time that is required for a safety sensor or switch, such as a light curtain, to turn OFF. The value is defined for each sensor or switch. Use the following values when an OMRON Special Safety Input Device is connected to a Safety Input Unit. E3ZS/E3FS Single-beam Safety Sensors : 14 ms D40A-2/D40A Non-contact Door Switches : 6 ms + 0.4 ms x No. of linked Switches*1 D40Z Non-contact Door Switches : 29 ms UM/UMA Safety Mats : 24 ms*2 SGE Safety Edges : 24 ms
(b)	Safety Input Unit/ slave response time	This is the input response time required for a FSoE salve or CIP Safety slave, such as Safety Input Units. A specific value is defined for each device. The response time of Safety Input Units is as follows. NX-SIH400: 9 ms + On-Off delay time NX-SID800: 5 ms + On-Off delay time GI-SID1224: 11 ms + On-Off delay time GI-SMD1624: 11 ms + On-Off delay time NXR-SXD1204□-CST: 10ms + Safety input terminal On-Off delay time For any other device, refer to the manual for the device.
(c)	Network reaction time	This is the response time required for the CIP Safety connections or the FSoE connections. These values can be verified on the Sysmac Studio. For details on how to check the network reaction time, refer to *7-5 CIP Safety Communication Settings* on page 7-21. For FSoE connections: FSoE Watchdog Timer value For CIP Safety connections: Network reaction time value calculated by the Sysmac Studio
(d)	Safety CPU Unit response time	Response time of the Safety CPU Unit. This value is an integer multiple of the safety task period. The value varies, depending on the safety chain route as follows. When the FSoE connections are used for both input and output : Safety task period x 0 When the CIP Safety connections are used for both input and output : Safety task period x 2 When the FSoE connections are used for input and CIP Safety connections are used for output : Safety task period x 1 When the CIP Safety connections are used for input and the FSoE connections are used for output : Safety task period x 1
(e)	Safety Output Unit/slave response time	This is the output response time required for a FSoE salve or CIP Safety slave, such as Safety Output Units. A specific value is defined for each device. The response time of the Safety Output Units is as follows. NX-SOH200: 1 ms NX-SOD400: 1 ms GI-SMD1624: 4.5 ms + Output test pulse width NXR-SXD1204□-CST: 5ms + Safety output terminal On-Off delay time For any other device, refer to the manual for the device.
(f)	Actuator response time	This is the response time that is required for an actuator, such as a safety relay, to turn OFF. The value is defined for each actuator.

*1. The fault detection time for a 24 V short-circuit fault in a D40A-2/D40A Non-contact Door Switch is 18 ms. If usage is for an application other than a Door Switch, use a safety sensor/switch response time of 18 ms.

*2. Refer to *Precaution for Conformance to ISO 13856-1:2013* on page 10-4 for a precaution on conformance to ISO 13856-1:2013.

Precautions for Correct Use

- If the safety task period changes due to changes in the safety program or other reasons, re-calculate the safety reaction times.
- To calculate the safety reaction times, add the "delaying influences from the input filter delay settings", the "safety program function block delay settings", and the "safety program loopback connections".

Precaution for Conformance to ISO 13856-1:2013

If you use UM/UMA Safety Mats to build a pressure-sensitive protective device that conforms to ISO 13856-1:2013 (Safety of machinery -- Pressure-sensitive protective devices -- Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors), the NX-series Safety Control Unit must meet the following condition in order to satisfy the requirement for the specified reaction time.

- The value of the FSoE watchdog timer in the NX-SIH400 that is connected to the UM/UMA Safety Mats must be 42 ms or less.

10-1-2 Verifying Safety Reaction Times

Verify the calculated safety reaction times for all safety chains to confirm that they satisfy the required specifications.

If a calculated safety reaction time exceeds the required specifications, consider the following measures and correct the software or hardware design.

- Shorten the safety task period.
  Example: Reduce the size of the safety program.
  Reduce the number of Safety I/O Units.
- Reduce EPI values of CIP Safety connections.

10-2 Safety Task

This section describes the safety task of the Safety CPU Unit.
The safety task period of the Safety CPU Unit affects the safety reaction times.

10-2-1 Safety Task

The safety task is used to assign an execution condition to a series of processes, such as for data exchange with the Safety I/O Units and the CIP Safety target device, as well as for safety program execution.
The Safety CPU Unit executes one safety task.
The safety task is executed on a fixed period.

More than one program*1 can be assigned to a safety task. The programs that are assigned are executed in the order that they are assigned. Execution of all of the programs assigned to the task is called "program execution".

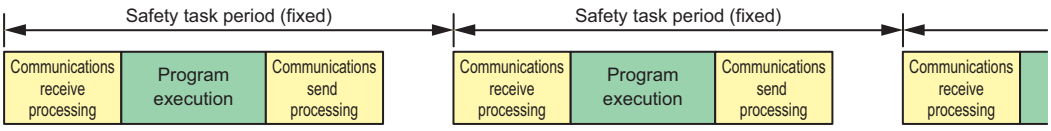
*1. There is no limit to the number of programs.

Data exchange between the Safety CPU Unit and, the Safety I/O Units and the CIP Safety target device is called "communications receive processing" and "communications send processing".

Type of task	Number of tasks	Task execution priority	Execution conditions	Main processing contents
Safety task	1	None	The safety task is executed once every safety task period during operation in RUN or DEBUG mode.	Communications receive processing, program execution, and communications send processing

10-2-2 Operation of Safety Task

The following operation is performed for the safety task.
Input data processing for I/O refreshing, user program execution, and output data processing for I/O refreshing are performed repetitively, i.e., each safety task period.



The safety task period is the time interval at which the safety task is executed. The upper limit of the safety task period setting is 100 ms. A building error will occur for any safety program that requires a safety task period that is longer than 100 ms. If that occurs, change the safety program.

10-2-3 Minimum Safety Task Period

The minimum safety task period is automatically calculated by the Sysmac Studio and displayed in the **Minimum safety task period** in the **Task Settings**.

Precautions for Correct Use

If you change any of the following values, the minimum safety task period will change. Check the minimum safety task period again.

- Safety program execution time (This time depends on the sizes of the programs and the function blocks that are used.)
- Number of connections with Safety I/O Units
- Number of connections with CIP Safety devices

10-2-4 Setting the Safety Task Period

For the safety task period, specify a value that is equal to or greater than the minimum safety task period calculated by the Sysmac Studio but not greater than 100 ms.

Refer to *8-5-9 Safety Task Settings* on page 8-76 for information on setting the safety task period in the Sysmac Studio.

Additional Information

We recommend that you set the safety task period with plenty of leeway to allow for the possibility of expanding the safety control system or safety programs in the future.

10-3 FSoE Watchdog Timer

This section describes the FSoE watchdog timers.

10-3-1 FSoE Watchdog Timers

An FSoE watchdog timer is used for timeouts in safety process data between the Safety CPU Unit and Safety I/O Units.
The FSoE watchdog timers affect the safety reaction times.

The value of the FSoE watchdog timer is automatically calculated by the Sysmac Studio.

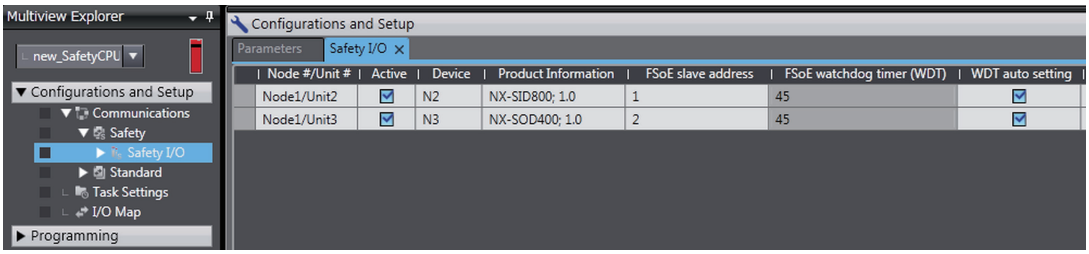
10-3-2 Checking FSoE Watchdog Timers

Use the following procedure to check the FSoE watchdog timers.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Double-click **Safety I/O** under **Configurations and Setup** – **Communications** – **Safety**.

The following Safety I/O Unit Setting Tab Page is displayed.



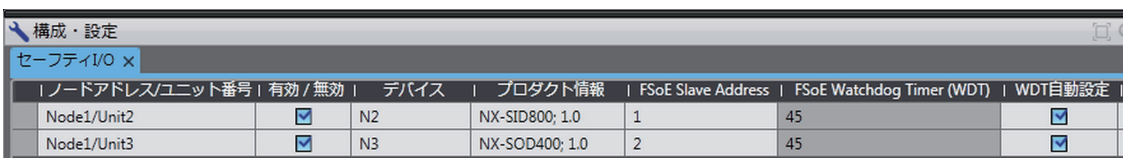
The values of the FSoE watchdog timers are displayed in the **FSoE watchdog timer** Column for the Safety I/O Units.

10-3-3 Changing FSoE Watchdog Timers

Use the following procedure to change a FSoE watchdog timer.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Double-click **Safety I/O** under **Configurations and Setup** – **Communications** – **Safety**.
The following Safety I/O Unit Setting Tab Page is displayed.



3 Clear the selection of the **WDT auto setting** Check Box for the Unit to change.
This enables changing the value of the **FSoE watchdog timer**.

Parameters | Safety I/O

Node #/Unit #	Active	Device	Product Information	FSoE slave address	FSoE watchdog timer (WDT)	WDT auto setting
Node1/Unit2	☑	N2	NX-SID800; 1.0	1	45	☐
Node1/Unit3	☑	N3	NX-SOD400; 1.0	2	45	☑

4 Double-click the cell in the **FSoE watchdog timer** Column for the Unit to change and set the desired FSoE watchdog timer value.

Node #/Unit #	Active	Device	Product Information	FSoE slave address	FSoE watchdog timer (WDT)	WDT auto setting
Node1/Unit2	☑	N2	NX-SID800; 1.0	1	2000	☐
Node1/Unit3	☑	N3	NX-SOD400; 1.0	2	45	☑

10-4 EPI (Data Packet Interval)

EPI stands for Expected Packet Interval and refers to the transmission interval of safety data packets in the CIP Safety communications.
The EPI affects the safety reaction time.

If you specify a smaller EPI, it shortens the network reaction time and the safety reaction time, but it increases the communications load on the EtherNet/IP communications port. For details on the communications load on the EtherNet/IP communications port, refer to *Section 11 Communications Load* on page 11-1.

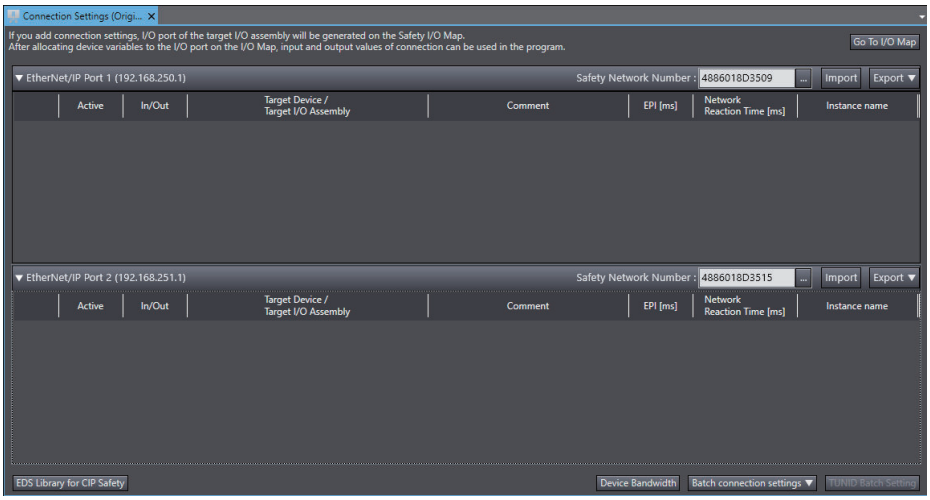
10-4-1 Changing the EPI

The EPI is set separately for each connection. Use the following procedure to change the EPI.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.

2 Go to **Configurations and Setup** – **Communications** – **Safety** – **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**.

The following Connection Settings (Originator) Tab Page is displayed.



3 Select a connection setting to change its EPI value and edit the **EPI** Column.

10-4-2 EPI Restrictions

The allowable range for EPI is automatically calculated and displayed by the Sysmac Studio.

11

Communications Load

This section describes how to adjust communications load in order to realize high-speed and stable communications.

11-1 Adjusting the Communications Load..... 11-2
11-1-1 Checking Bandwidth Usage for Tag Data Links 11-3
11-1-2 Checking the Device Bandwidth Usage of the CIP Safety Routing.....11-4
11-1-3 Relationship between the Number of Packets Used per Second and Packet Intervals.....11-5
11-1-4 Adjusting the Device Bandwidth Usage 11-5

11-1 Adjusting the Communications Load

In an Ethernet network using an Ethernet switch, the network bandwidth is not shared by all of the nodes, and independent transmission paths are established between individual nodes through the Ethernet switch.
A dedicated communications buffer is established in the Ethernet switch for communications between the nodes and full-duplex communications (simultaneous transmission and reception) are performed asynchronously with other transmission paths. The communications load in other transmission paths does not affect communications, therefore packet collisions do not occur, and stable high-speed communications can be performed.
The Ethernet switch functions shown in the following table determine the performance of the CIP Safety connections and tag data links.

Item	Description
Buffer capacity	This is the amount of data that can be buffered when the data packets accumulate at the Ethernet switch.
Multi-cast filtering	The function transfers multi-cast packets to specific nodes only.
QoS function	The function performs priority control of packet transfers.

The following table shows the specifications within which the CIP Safety Connection settings and the tag data link settings can be made for a built-in EtherNet/IP port.

Item	Meaning	Communication Control Unit
		NX-CSG320
Network bandwidth	Physical Ethernet baud rate	100 Mbps or 10 Mbps
Maximum number of packets per second	The maximum number of packets that can be processed in one second (pps: packet per second)	12,000 pps max (total of 12,000 pps with two ports)
Number of CIP Safety routing connections	Maximum safety I/O connections supported for routing	254 max (total of 254 with two ports)
Packet interval of CIP Safety connections (EPI: Expected Packet Interval)	Data refresh period of CIP Safety connections	1 to 500 ms in 1-ms increments. The allowable range depends on the target device.
Tag data link connection resources	The number of tag data link connections that can be opened	32 max (total of 64 with two ports)
Packet interval of tag data links (RPI: Requested Packet Interval)	Refresh period for tag data	1 to 10,000 ms in 1-ms increments

When the CIP Safety connection settings or the tag data link settings exceed the capabilities of the Ethernet switch, adjust (increase) the packet interval value (RPI/EPI).

Particularly when using an Ethernet switch that does not support multi-cast filtering, the settings must be made considering that multi-cast packets will be sent even to nodes without connection settings.

Additional Information

If the connection type is set to **Multi-cast connection** in the connection settings of the CIP Safety or the tag data links, multi-cast packets are used. If the connection type is set to **Point to Point connection**, multi-cast packets are not used.

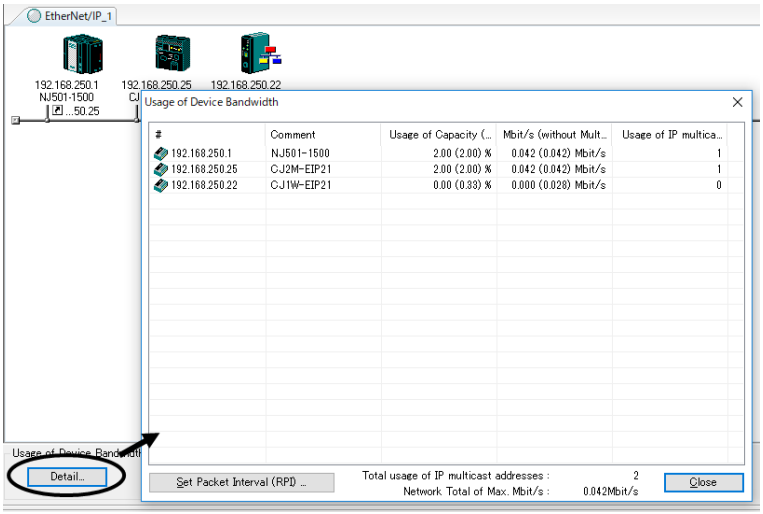
In addition, if the required CIP Safety performance or tag data link performance cannot be achieved within the specifications, reevaluate the overall network configuration and correct it by taking steps such as selecting a different Ethernet switch or splitting the network.
The following sections show how to check the device bandwidth to be used for the CIP Safety routings and the tag data links in the designed network, and how to change the values.

Additional Information

In order to provide stable communications, the connection settings need to be adjusted so that the total device bandwidth usage of tag data links and the CIP Safety routing will not exceed 80%.

11-1-1 Checking Bandwidth Usage for Tag Data Links

The Network Configurator can display the bandwidth actually used for tag data links at each built-in EtherNet/IP port, based on the connections set in the network configuration.
The device bandwidth used by tag data links can be checked by clicking the **Detail** Button in the **Usage of Device Bandwidth** Area at the bottom of the Network Configuration Pane.



Item	Description
#	The IP address of the device
Comment	A description of the device. The comment is displayed below the device icon. The model number of the device is displayed by default.

Item	Description
Usage of Capacity (without Multicast filter)	The ratio of the device's packet usage to the maximum number of packets per second. *Number of packets used per second* / *Number of maximum packets per second* The values outside parentheses are for when multi-cast filtering is used. The values inside parentheses are for when multi-cast filtering is not used.
Mbit/s (without Multicast filter)	The network bandwidth usage for tag data link communications with the device. The values outside parentheses are for when multi-cast filtering is used. The values inside parentheses are for when multi-cast filtering is not used.
Usage of IP multicast addresses	The number of IP multi-cast addresses actually used for communications with the device.
Total usage of IP multicast addresses	The number of IP multi-cast addresses used in the entire network. This value is used to estimate the number of multi-cast filters for switching.
Network Total of Max. Mbit/s	The total network bandwidth used for tag data link communications in the entire network. Tag data links will not operate normally if the network bandwidth that can be set is exceeded.

● Checking the Packet Usage Rate to the Maximum Number of Packets per Second and the Network Bandwidth Usage

The window displays the ratio of the packet usage to the maximum number of packets per second for each EtherNet/IP port, and the network bandwidth usage in Mbit/s.

The usage of capacity and used network bandwidth that are displayed in parentheses are for an Ethernet switch that does not use multicast filtering. In this case, multicast packets will be sent to even the nodes without connection settings, so the displayed values will include these packets as well.

These values can be adjusted by changing the RPI.

● Checking the Total Number of Multi-cast IP Addresses in the Network

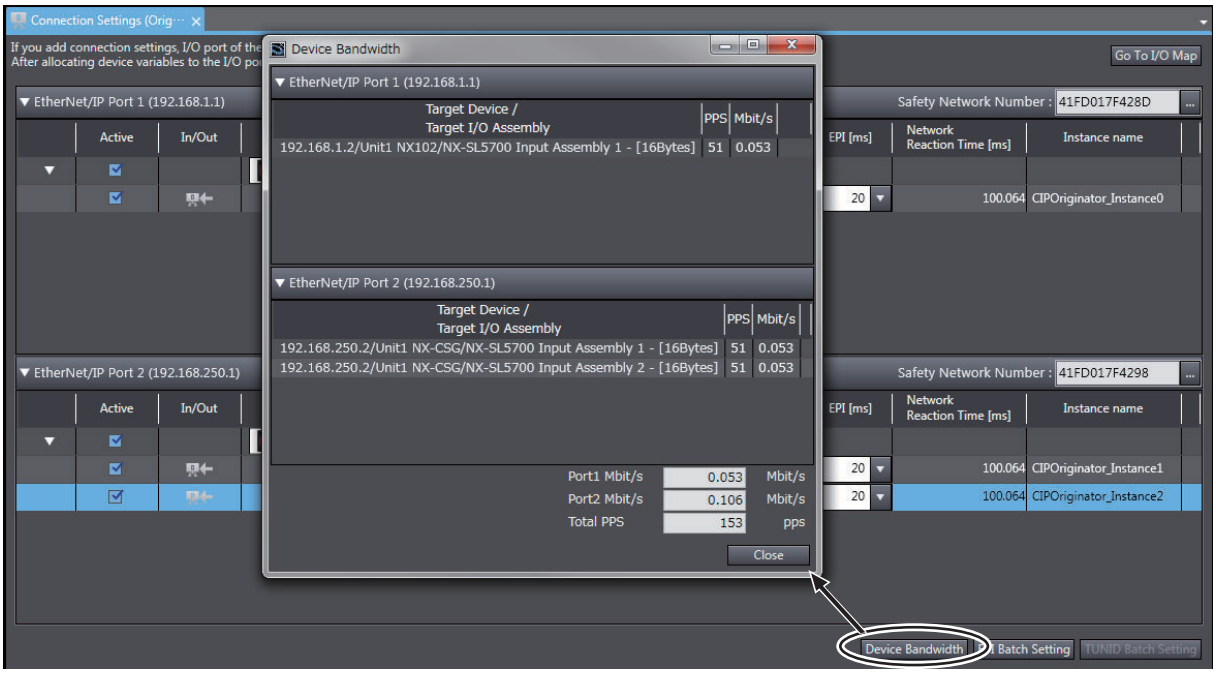
When using an Ethernet switch that provides multicast filtering, there must be enough multicast filters for the network to be used. The Network Configurator shows the number of multi-cast IP addresses used for the entire network based on the connection settings.

Make sure that the number of multicast IP addresses used in the entire network does not exceed the number of multicast filters supported by the Ethernet switch. If necessary, replace the Ethernet switch with another one that has the sufficient number of multi-cast filters, or adjust the usage rate to the maximum number of packets per second or the network bandwidth usage by using values given for Ethernet switches without multicast filtering (i.e., the values in parentheses). These values can be adjusted by changing the RPI.

11-1-2 Checking the Device Bandwidth Usage of the CIP Safety Routing

The Sysmac Studio displays the bandwidth used for the CIP Safety routing function for each CIP Safety connection configured on in the Safety CPU Unit.

You can verify the device bandwidth usage status for CIP Safety routing by clicking the **Device Bandwidth** Button located at the bottom of the Connection Settings (Originator) Tab Page.



Item	Meaning
PPS	Displays the number of packets used for each CIP Safety connection per second and the total sum of used packets
Mbit/s	Displays the network bandwidth used for each CIP Safety connection.

11-1-3 Relationship between the Number of Packets Used per Second and Packet Intervals

The usage rate to the maximum number of packets per second can be adjusted by modifying the settings for the packet interval (PRI) for the tag data link or the packet interval (EPI) for the CIP safety connection.

The shorter the packet interval is, the larger the usage rate to the maximum number of packets per second will become.

Conversely, the longer the packet interval is, the less the usage rate to the maximum number of packets per second will become.

11-1-4 Adjusting the Device Bandwidth Usage

This section describes how to adjust the device bandwidth usage.

Precautions for Correct Use

The Ethernet switch should support the maximum network bandwidth value that can be set for the Communication Control Unit. The maximum network bandwidth value of the Communication Control Unit is 100 Mbit/s.

Ethernet Switches without Multicast Filtering

- Does the total number of packets transmitted to the built-in EtherNet/IP port per second exceed the maximum number of packets allowed per second?
  If it exceeds the maximum number, check and modify the connection settings, including RPI and EPI values.
- Does the total network bandwidth usage of any transmission path exceed the network bandwidth that can be set for the path?
  If it exceed the bandwidth that can be set for the transmission path, the tag data link and CIP safety connection may not work properly. If the bandwidth is exceeded, rewire the network or increase the bandwidth between Ethernet switches (e.g., to 1 Gbps). If these countermeasures are not possible, change the connection settings, including the RPI settings.

Ethernet Switches with Multicast Filtering

- Does the total network bandwidth usage of any transmission path exceed the network bandwidth that can be set for the path?
  If it exceed the bandwidth that can be set for the transmission path, the tag data link and CIP safety connection may not work properly. If the bandwidth is exceeded, rewire the network or increase the bandwidth between Ethernet switches (e.g., to 1 Gbps). If these countermeasures are not possible, change the connection settings, e.g., the RPI settings.
- Does the total number of packets transmitted to the built-in EtherNet/IP port per second exceed the maximum number of packets allowed per second?
  If it exceeds the maximum number, check whether the multicast filtering on Ethernet switches is functioning correctly. Calculate the number of multicast filters required for each Ethernet switch on the network, and make sure that the resulting number does not exceed the number of multicast filters of any Ethernet switch. If the number of multicast filters of an Ethernet switch is not sufficient, replace it with another switch with enough multicast filters, or modify the connection settings, including the RPI and EPI settings.

12

Safety Unit Restore

This section describes the procedures to execute the Safety Unit Restore.

12-1 Safety Unit Restore 12-2
12-1-1 Generate Safety Unit Restore File Function 12-2
12-1-2 Safety Unit Restore Function 12-3
12-1-3 Specifications of a Safety Unit Restore File 12-5

12-1 Safety Unit Restore

The safety unit restore is a function designed to transfer safety programs and settings to Safety CPU Unit via an SD Memory Card.
You can use the Safety Unit Restore in the following instances.

Item	Application
Program and setting changes	When you change the safety program and settings for equipment that is currently in operation
Hardware replacement	When you replace the hardware for the Safety CPU Unit
Manufacture of equipment	When you want to manufacture the same equipment and need to transfer the data from the existing equipment to new equipment in its initial state.

Safety Unit Restore is executed combining the following functions.

Function	Description
Generate Safety Unit Restore File function	This function allows to generate the Safety Unit Restore File using the Sysmac Studio.
Safety Unit Restore function	This function allows to transfer the Safety Unit Restore File data stored in an SD Memory Card to a Safety CPU Unit.

Precautions for Correct Use

- To execute the Safety Unit Restore, you need to execute the restore function for the Communication Control Unit as well. In addition, you need to generate a safety backup file and a backup file of the Communication Control Unit from a same project or from a same project of a same physical unit where a project was transferred from. If the settings for the safety backup file and that for the backup file of the Communication Control Unit are not consistent, the safety control unit does not operate normally.
- Before executing the Safety Unit Restore, make sure to confirm the safety of the transfer destination.
- Before executing the Safety Unit Restore, verify that the operation target is correct.
- Before executing the Safety Unit Restore, verify that the signature displayed on the seven-segment indicator of the Safety CPU Unit is correct.
- To prevent accessing a wrong Safety Unit Restore File, make sure to control the file access and configuration properly.
- After executing the Safety Unit Restore, verify that the Unit is configured correctly and the Unit behaves as intended.
- To prevent executing the Safety Unit Restore by unauthorized person, make sure to keep under access control to SD Memory Cards and Safety Unit Restore Files.

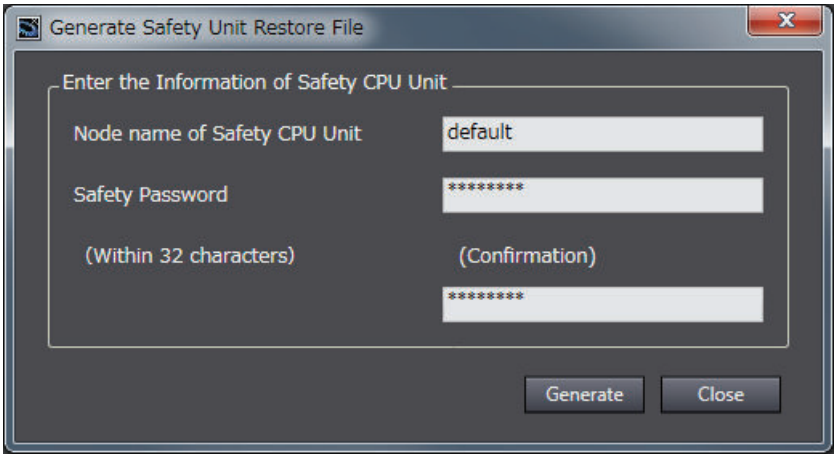
12-1-1 Generate Safety Unit Restore File Function

This function uses the Sysmac Studio to generate a Safety Unit Restore File from a project that includes safety application data.
Safety validation must be completed for the safety application data. Refer to *9-11 Performing Safety Validation and Operation* on page 9-59 for details on the safety validation of safety application data.

Procedure

1 Startup the Sysmac Studio. Open a project which contains the validated safety application data.

2 From the Controller selection in the Multiview Explorer, select Safety CPU Unit, then select **Tools** – **Generate Safety Unit Restore File** from the menu.
The Generate Safety Unit Restore File Dialog Box is displayed.



3 Enter the node name and the safety password that are set for the Safety CPU Unit to restore, and click the **Generate** Button.
The Browse Folder Dialog is displayed.

Item	Initial value	Description
Node Name	default	Enter a node name for Safety CPU Unit to restore data. If the node name does not match with the actual unit, the restore operation fails. If the node name of the actual unit is unchanged from the factory default settings, the node name you entered here will be reflected to the actual unit.
Safety Password	---	Enter a safety password for Safety CPU Unit to restore data. If the safety password does not match, the restore operation fails. If the safety password is not configured for the actual unit, the safety password you entered here will be reflected to the actual unit.

4 Specify the folder to save the files and click the **OK** Button.
The Safety Unit Restore File (file name: SLSystem.dat) will be generated to the specified folder.

5 Store the Safety Unit Restore File in the root directory on the SD Memory Card.

12-1-2 Safety Unit Restore Function

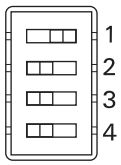
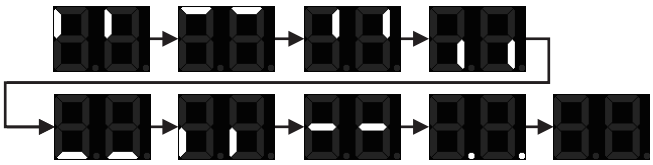
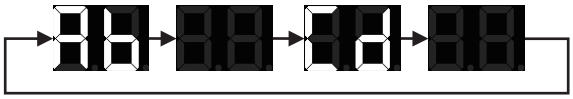
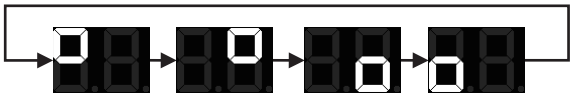
Insert an SD Memory Card to the Communication Control Unit connected to the Safety CPU Unit and then transfer data of the Safety Unit Restore File stored in the memory card to the Safety CPU Unit.

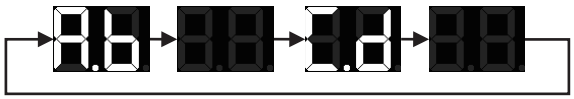
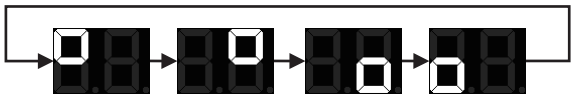
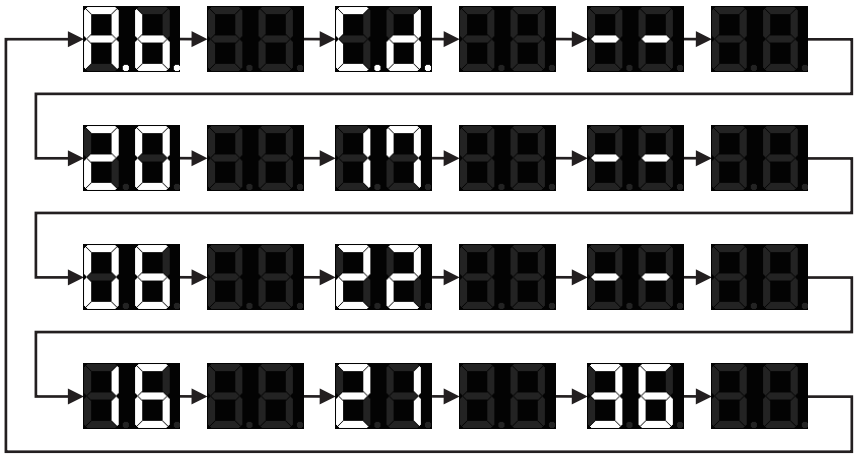
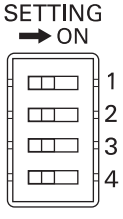
Change the DIP switch settings and start the Safety CPU Unit in the Restore mode then execute the Safety Unit Restore using the SD Memory Card.
The node name and safety password stored in the Safety CPU Unit to restore must be consistent with those stored in the Safety Unit Restore File or unchanged from the factory default settings.

Precautions for Correct Use

To execute the Safety Unit Restore, you need to execute the restore function for the Communication Control Unit as well. In addition, you need to generate a safety backup file and a backup file of the Communication Control Unit from a same project or from a same physical unit from which a project is transferred. If the settings for the safety backup file and that for the backup file of the Communication Control Unit are not consistent, the safety control unit does not operate normally.

Procedure

Processing stage	Procedure and Display
Insert an SD Memory Card	Insert the SD Memory Card where the Safety Unit Restore File are stored under the root directory into the Communication Control Unit.
Start RESTORE Mode	Set the pins 1 to 4 of the DIP switch on the Safety CPU Unit as follows: 1 to ON, 2 to OFF, 3 to OFF, and 4 to OFF, and turn ON the power supply to the Controller. The Safety CPU Unit starts in RESTORE mode. SETTING ON 
Initializing	Seven-segment indicators in the Safety CPU Unit repeat turning ON and OFF in sequence for each, to test if the devices are lit properly.  • If initialization ended in an error, an error code is shown in the seven-segment indicators in the Safety CPU Unit.
Wait for Start command	The safety signature of the Safety Unit Restore File stored in the SD Memory Card is repeatedly shown as a four-digit hexadecimal number in the seven-segment indicators in the Safety CPU Unit.  (Example: Supposing the safety signature is 0xABCD) Check the safety signature. If it is correct, press and hold the service switch for one second or more and release. Processing starts.
Processing	Seven-segment indicators in the Safety CPU Unit repeat turning ON and OFF in four at a time.  • If processing ended in an error, an error code is shown in the seven-segment indicators in the Safety CPU Unit.

Processing stage	Procedure and Display
Wait for Completion Command	The safety signature for the settings information transferred to the Safety CPU Unit is repeatedly shown as a four-digit hexadecimal number in the seven-segment indicators of the Safety CPU Unit.  (Example: Supposing the safety signature is 0xABCD) Check the safety signature. If it is correct, press and hold the service switch for one second or more and release. Completion processes starts.
Processing Completion	Seven-segment indicators in the Safety CPU Unit repeat turning ON and OFF in four at a time.  • If processing ended in an error, an error code is shown in the seven-segment indicators in the Safety CPU Unit.
Done	The safety signature including the date and time (UTC) is repeatedly shown in the seven-segment indicators of the Safety CPU Unit.  (Example: Supposing the safety signature is 0xABCD, and the date is 16:21:36 of June 22, 2017 (UTC))
Restart	After turning OFF the power supply to the Controller, set the pins 1 to 4 of the DIP switch on the Safety CPU Unit as follows: 1 to OFF, 2 to OFF, 3 to OFF, and 4 to OFF, and turn ON the power supply to the Controller. The Safety CPU Unit starts in RUN mode. 

Refer to *Section 15 Troubleshooting* on page 15-1 for errors that can occur while restoring the Safety Control Units.

12-1-3 Specifications of a Safety Unit Restore File

A Safety Unit Restore File is named as follows:

● File Name

File	File name
Safety Unit Restore File	SLSystem.dat

13

Backup Functions of the Communication Control Unit

This section describes the backup functions for the settings in an NX-series Communication Control Unit. There are different types of backup functions that handle different data or different storage locations. First an overall description of the backup functions is provided followed by descriptions of the individual functions.

13-1 The Backup Functions 13-2
- 13-1-1 Applications of Backup Functions 13-2
- 13-1-2 Examples of Operating Procedures for the Backup Functions 13-2
- 13-1-3 Data that Is Backed Up 13-4
- 13-1-4 Types of Backup Functions 13-5
- 13-1-5 Relation between the Different Types of Backup Functions and Data Groups 13-7
- 13-1-6 Applicable Range of the Backup Functions 13-8

13-2 SD Memory Card Backups 13-10
- 13-2-1 Backup (Controller to SD Memory Card) 13-10
- 13-2-2 Restore (SD Memory Card to Controller) 13-12
- 13-2-3 Verify (between Controller and SD Memory Card) 13-13

13-3 Disabling Backups to SD Memory Cards 13-15

13-4 Sysmac Studio Controller Backups 13-16
- 13-4-1 Backup (Controller to Computer) 13-16
- 13-4-2 Restore (Computer to Controller) 13-17
- 13-4-3 Verify (between Controller and Computer) 13-18

13-5 Importing and Exporting Sysmac Studio Backup File Data 13-20

13-6 Backup Functions when NX Units are Connected 13-21
- 13-6-1 Backing Up Data in NX Units on the Communication Control Unit 13-21
- 13-6-2 Backup Support Depending on the Controller Status 13-21
- 13-6-3 Conditions for Restoring NX Unit Data on the Communication Control Unit 13-22

13-7 Backup-related Files 13-23
- 13-7-1 Types of Backup-related Files 13-23
- 13-7-2 Specifications of a Backup File 13-23
- 13-7-3 Specifications of a Restore Command File 13-24
- 13-7-4 Specifications of a Controller Verification Results File 13-25
- 13-7-5 Specifications of an NX Unit Verification Results File 13-26

13-8 Compatibility between Backup-related Files 13-28
- 13-8-1 Compatibility between Backup Functions 13-28

13-9 Functions That Cannot Be Executed during Backup Functions 13-29

13-1 The Backup Functions

The following three functions are supported for data backup for an Communication Control Unit.
Note that these functions are not designed to back up the Safety Control Unit settings. Refer to *Section 12 Safety Unit Restore* on page 12-1 for details on the restore operations of the Safety Control Unit.

Function	Description
Backing up data	You can back up all of the data in the Communication Control Unit to an SD Memory Card or to a computer. The file that is saved is called a backup file.
Restoring data	You can transfer the contents of a backup file on the SD Memory Card or computer to the Communication Control Unit. The data in the Communication Control Unit is restored to the data at the time the backup file was made.
Verifying data	You can compare the contents of a backup file on the SD Memory Card or computer with the data in the Communication Control Unit to see if they are the same.

The following items are described for the backup functions.

Item	Description
Applications of backup functions	Effective usage of the backup functions is described.
Examples of operating procedures for the backup functions	The backup functions are executed with simple procedures. Examples are provided.
Data that is backed up	The data that can be saved with the backup functions from the connected Units and slaves is described.
Types of backup functions	There are different types of backup functions that differ in where the data is saved. The types of backup functions and the difference between them are described.
Relation between the different types of backup functions and data groups	Different types of backup functions handle different data groups. The relation between the different types of backup functions and data groups is described.
Applicable range of the backup functions	The connected Units and slaves for which you can save data with the backup functions are described.

13-1-1 Applications of Backup Functions

The backup function and the unit backup function are designed for the following purposes.

Item	Application
Setting changes	When you change the settings for equipment that is currently in operation.
Hardware replacements	When you replace the hardware of NX Units, except for Communication Control Units and Safety Control Units.
Manufacture of equipment	When you want to manufacture the same equipment and need to transfer the data from the existing equipment to new equipment in its initial state.

13-1-2 Examples of Operating Procedures for the Backup Functions

You can use the backup functions to easily back up, restore, and verify Communication Control Unit data.

This section describes the procedure for performing a backup, restore or compare operation of the SD Memory Card using Communication Control Unit front-panel switch.

Backup Procedure

● Preparations

1. Insert the SD Memory Card into the Communication Control Unit.
2. Set pins 1 to 4 on the DIP switch on the Communication Control Unit as follows: 1: OFF, 2: OFF, 3: ON, and 4: OFF.

● Executing the Backup

1. Press the SD Memory Card power supply switch for 3 seconds.
   The backup is started. The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds. When the backup operation is completed, the SD PWR indicator will stop flashing and remain lit.

● Ending the Backup Procedure

1. Set all of pins 1 to 4 on the DIP switch on the Communication Control Unit to OFF.
2. Press the SD Memory Card power supply switch to turn OFF the SD PWR indicator.
3. Remove the SD Memory Card.

Restoration Procedure

● Preparations

1. Turn OFF the power supply to the Communication Control Unit.
2. Insert the SD Memory Card that contains the backup file into the Communication Control Unit.
3. Set pins 1 to 4 on the DIP switch on the Communication Control Unit as follows: 1: OFF, 2: OFF, 3: ON, and 4: ON.

● Restoring Data

1. Turn ON the power supply to the Communication Control Unit.
   The restoration operation is started. The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds. When the restoration operation is completed, the SD PWR indicator will stop flashing and remain lit.

● Ending the Restoration Procedure

1. Press the SD Memory Card power supply switch to turn OFF the SD PWR indicator.
2. Turn OFF the power supply to the Communication Control Unit.

● Starting Normal Operation

1. Remove the SD Memory Card.
2. Set all of pins 1 to 4 on the DIP switch on the Communication Control Unit to OFF.
3. Turn ON the power supply to the Communication Control Unit.

Verification Procedure

● Preparations

1. Insert the SD Memory Card that contains the backup file into the Communication Control Unit.
2. Set all of pins 1 to 4 on the DIP switch on the Communication Control Unit to OFF.

● Verifying the Data

1. Press the SD Memory Card power supply switch for 3 seconds.
   Data comparison is started. The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds.
   If the verification operation is completed and the data is the same, the SD PWR indicator will stop flashing and remain lit.
   If the verification operation is completed and differences were found in the data, the SD PWR indicator will flash, lighting for 0.5 seconds and going out for 0.5 seconds.

● Ending the Verification Procedure

1. Press the SD Memory Card power supply switch to turn OFF the SD PWR indicator.
2. Remove the SD Memory Card.

13-1-3 Data that Is Backed Up

The following data is backed up.
This section describes the backup functions based on the following *data groups* for the backup data.

Data group	Data items
Data and settings	Unit Configuration and Unit Setup*1*2 I/O Map Controller Setup (Operation Settings and Built-in EtherNet/IP Port Settings) Tag Data Link Tables Controller name Operation authority verification Built-in clock (time zone setting) Data (global variables)
IP address of the built-in EtherNet/IP port*3*4	Of the TCP/IP Settings in the Built-in EtherNet/IP Port Settings, setting type, IP address, subnet mask, and default gateway
Present values of variables	Values of variables with a Retain attribute*5
Units and slaves settings	NX Unit Settings*2
X Bus Unit Settings*13-1-3 Data that Is Backed Up* on page 13-4	Settings in X Bus Unit
IP address of an EtherNet/IP port on an X Bus Unit*13-1-3 Data that Is Backed Up* on page 13-4	Of the TCP/IP Settings in the EtherNet/IP Port Settings for the NX-series EtherNet/IP Unit, setting type, IP address, subnet mask, and default gateway

*1. For the NX Units on the Communication Control Unit, data of configuration information, Unit operation settings and Unit application data is backed up.
*2. Safety Control Units are not included for the data backup function.
*3. IP address of the Built-in EtherNet/IP Port Settings can be used as a data group.
*4. Values of the IP address switch of Communication Control Unit are not backed up. Please set them manually as required.
*5. Of the system-defined variables with a Retain attribute, some variables are not applicable for the data backup function. Refer to the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for details on the specifications for individual system-defined variables.

13-1-4 Types of Backup Functions

The backup function supported for the Communication Control Unit allows you to save data to an SD Memory Card or to a computer. Also, there are two methods used to execute the backup functions: the Communication Control Unit front-panel DIP switches and the Sysmac Studio.

Functions that Save Data to SD Memory Cards

The SD Memory Card backup functions are used to back up, restore, and compare data on SD Memory Cards. Related functions include disabling backups to SD Memory Cards.

Function name		Description	Operating method		Reference
			Communication Control Unit Front-panel DIP Switch	Sysmac Studio	
SD Memory Card Backups	Backing up data	The Communication Control Unit data is saved in a backup file on the SD Memory Card.	Available	Available	*13-2-1 Backup (Controller to SD Memory Card)* on page 13-10
	Restoring data	The data in a backup file on the SD Memory Card is transferred to the Communication Control Unit.	Available		*13-2-2 Restore (SD Memory Card to Controller)* on page 13-12
	Verifying data	The Communication Control Unit data and the data in a backup file on the SD Memory Card are compared.	Available	Available	*13-2-3 Verify (between Controller and SD Memory Card)* on page 13-13
Disabling backups to SD Memory Cards		You can disable backing up data to SD Memory Cards.		Available	*13-3 Disabling Backups to SD Memory Cards* on page 13-15

Functions that Save Data to the Computer

The Sysmac Studio Controller backup functions are used to back up, restore, and compare the Communication Control Unit data on the computer.
Importing and exporting Sysmac Studio backup file data are used to save and read different types of data between the Sysmac Studio projects and backup files on the computer without using the Communication Control Unit.

Function name		Description	Operating method		Reference
			Communication Control Unit Front-panel DIP Switch	Sysmac Studio	
Sysmac Studio Controller backups	Backing up data	The Communication Control Unit data is saved in a backup file on the computer.		Available	*13-4-1 Backup (Controller to Computer)* on page 13-16
	Restoring data	The data in a backup file on the computer is transferred to the Communication Control Unit.		Available	*13-4-2 Restore (Computer to Controller)* on page 13-17
	Verifying data	The Communication Control Unit data and the data in a backup file on the computer are compared.		Available	*13-4-3 Verify (between Controller and Computer)* on page 13-18
Importing and exporting Sysmac Studio backup file data	Exporting data	The data is exported from the project on the Sysmac Studio to a backup file without using the Communication Control Unit.		Available	*13-5 Importing and Exporting Sysmac Studio Backup File Data* on page 13-20
	Importing data	The data in the backup file is imported into the Sysmac Studio project without using the Communication Control Unit.		Available	

13-1-5 Relation between the Different Types of Backup Functions and Data Groups

Different types of backup functions handle different data groups. The relation between the different types of backup functions and data groups is given in the following table.

(OK: Applicable NA: Not applicable)

Type of backup function		Data group			
		Data and Settings		Present values of variables	Units and slaves settings
			IP address of built-in EtherNet/IP port*1*2		
SD Memory Card Backups	Backing up data	OK	OK	OK*3	OK*4
	Restoring data	OK	OK	OK*3	OK*4
	Verifying data	OK	OK	NA	OK*4

Type of backup function		Data group			
		Data and Settings		Present values of variables	Units and slaves settings
			IP address of built-in EtherNet/IP port*1*2		
Sysmac Studio Controller backups	Backing up data	OK	OK	OK*3	OK*4
	Restoring data	OK	OK	OK*3	OK*4
	Verifying data	OK	OK	NA	OK*4
Importing and exporting Sysmac Studio backup file data	Exporting backup file data	OK*5	OK	NA	NA
	Importing backup file data	OK*5	OK	NA	OK

*1. IP address of the Built-in EtherNet/IP Port Settings can be used as a data group.
*2. Values of the IP address switch of Communication Control Unit are not included for the data backup function. Set these values manually as required.
*3. The backup data is processed only for the present values of variables that are specified for retention with the Retain attribute.
*4. Safety Control Units are not included for the data backup function.
*5. The following data is not processed. Tag data link settings for the built-in EtherNet/IP port, and operation authority verification.

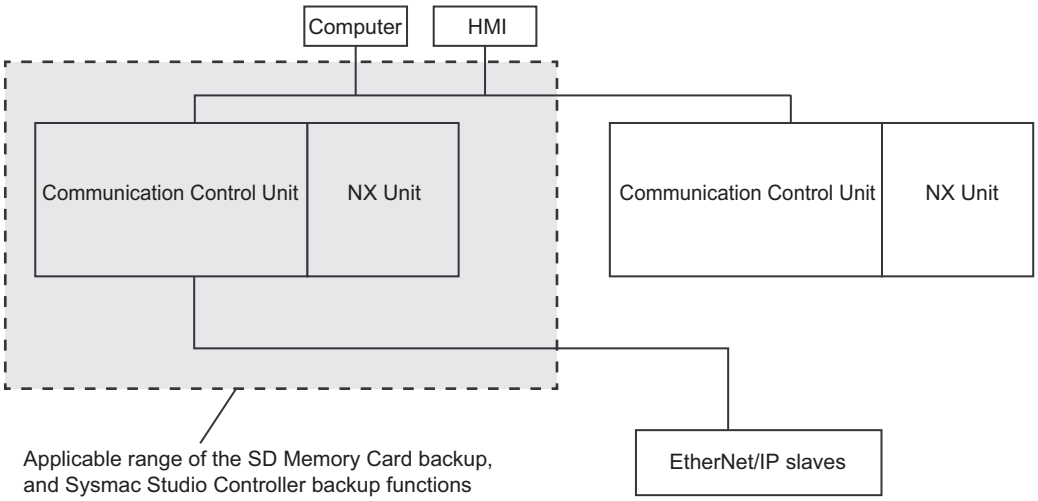
13-1-6 Applicable Range of the Backup Functions

Different types of backup functions handle data for different Units or slaves. The applicable Units and slaves for each backup function are given in the following table.

(OK: Applicable, NA: Not applicable)

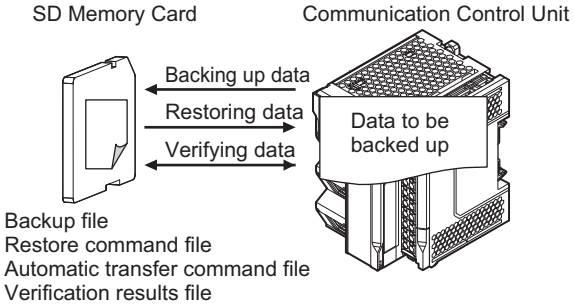
Type of backup function	Units/slaves			
	Communication Control Unit	NX Units on the Communication Control Unit	EtherNet/IP slaves	Computer and HMIs
SD Memory Card Backups	OK	OK	NA	NA
Sysmac Studio Controller backups	OK	OK	NA	NA
Importing and exporting Sysmac Studio backup file data	OK	OK	NA	NA

The Units and slaves that are shown in the following figure are covered by the SD Memory Card backup functions and Sysmac Studio Controller backup functions.


Computer
HMI
Communication Control Unit
NX Unit
Communication Control Unit
NX Unit
Applicable range of the SD Memory Card backup,
and Sysmac Studio Controller backup functions
EtherNet/IP slaves

13-2 SD Memory Card Backups

You can use SD Memory Cards to back up, restore, and verify the Communication Control Unit data.



When you back up data, the *Backup file*, *Restore command file*, and *Automatic transfer command file* are created in the specified directory on the SD Memory Card. When you verify data, the *Verification results files* are created in the specified directory.
All of these files are collectively referred to as *Backup-related files*.
The functions of the backup-related files are given in the following table.

File	Function			
	Description	Backing up data	Restoring data	Verifying data
Backup file	This file contains the Communication Control Unit data that is handled by the functions that are related to data backup.	Created.	Accessed.	Accessed.
Restore command file	This file specifies the data groups to restore when restoring data.You can edit this file with a text editor on a computer to specify the data groups to restore.	Created.	Accessed.	Accessed.
Automatic transfer command file	This file is not used with the Communication Control Unit.	Created.	Nothing is done.	Nothing is done.
Verification results files	These files contain the verification results after data is verified.	Nothing is done.	Nothing is done.	Created.

The execution method for the functions and applicable directory are given in the following table.

Procedure	Directory*1
Communication Control Unit Front-panel DIP switch *2	The root directory
SD Memory Card Window in Sysmac Studio	The directory that you specified in the tab page

*1. You can specify a directory only on the SD Memory Card.
*2. Before you restore or verify data, save the backup file and restore command file in the root directory.

13-2-1 Backup (Controller to SD Memory Card)

This operation is used to save data of the Communication Control Unit to the SD Memory Card in the Communication Control Unit.

Processing Contents

- This backup operation processes all data groups.
- When you back up data, the backup file, restore command file, and automatic transfer command file are created in the specified directory on the SD Memory Card.
- If the backup-related files are already in the specified directory, they are overwritten.
- If an error occurs while writing the backup-related files to the SD Memory Card, the previous back-up-related files will be deleted. Also, the new backup-related files will not be created.
- If an error occurs before the new backup-related files are created, the previous files are retained and the new files are not created.
- The power is continued to supply even if the SD Memory Card power supply switch is pressed when a backup is in progress.
- The SD Memory Card will remain mounted after completion of the backup.

Procedure

● Backing Up Data with the Communication Control Unit Front-panel DIP Switch

Processing stage	Procedure
Start command	The backup starts when the SD Memory Card power supply switch is pressed for 3 seconds with the DIP switch pins set as follows: 1: OFF, 2: OFF, 3: ON, and 4: OFF.
Executing	Immediately after Starting Backup*1 The SD PWR indicator will light, go out for 0.5 seconds, and then light again. While Backing Up Data The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds. The SD BUSY indicator will flash irregularly. The value of the *_BackupBusy* (Backup Function Busy Flag) system-defined variable will change to TRUE.
Execution results	Normal End: The SD PWR indicator will light. Error End: The SD PWR indicator will flash, lighting for 0.5 seconds and going out for 0.5 seconds. Press the SD Memory Card power supply switch so that the indicator will light.

*1. If an SD Memory Card is not inserted, the SD PWR indicator will not light.

● Backing Up Data from the SD Memory Card Window on the Sysmac Studio

Processing stage	Procedure
Start command	Click the **SD Memory Card Backup** Button on the SD Memory Card Window in the Sysmac Studio, specify the directory to save the backup file in, and execute the back-up.
Executing	The progress of the backup is displayed in the dialog box. The value of the *_BackupBusy* (Backup Function Busy Flag) system-defined variable will change to TRUE.
Execution results	A message will appear when the backup is completed. You will then be asked to confirm whether to verify the backup data.

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for specific procedures.

13-2-2 Restore (SD Memory Card to Controller)

You can transfer the data in a backup file on the SD Memory Card in the Communication Control Unit to the Communication Control Unit.
You can perform this operation using the Communication Control Unit front-panel DIP switch.

The transfer starts when the power supply is turned ON with the Communication Control Unit front-panel DIP switch. You can specify data to restore by the restore command file. You cannot specify the source directory for backup-related files. The backup file to restore must be stored in the root directory on the SD Memory Card.

Processing Contents

The following describes the processing contents of the operation when you use the Communication Control Unit front-panel DIP switch.

Restoring Data with the Communication Control Unit Front-panel DIP Switch

- The data in a backup file in the root directory on the SD Memory Card is transferred to the Communication Control Unit.
- The data groups that are processed by the *restoration operation* in the RestoreCommand.ini file (restore command file) that is stored in the root directory. Refer to *13-7-3 Specifications of a Restore Command File* on page 13-24 for details on the restore command file.
- If there is not a restore command file in the root directory of the SD Memory Card, all of the data from the backup files in the root directory that can be transferred to the Controller will be transferred.
- After the operation is completed, you cannot start operation in this state. To start operation, turn OFF all DIP switch pins and then cycle the power supply to the Communication Control Unit or *reset the Controller*.
- If an error occurs in the checks that are performed before starting to restore the data, the previous data will be retained in the Communication Control Unit.
- If the power supply to the Controller is interrupted while the data is being restored, a *User Program/ Controller Configurations and Setup Transfer Error (a major fault level Controller error)* will occur. If that occurs, the data in the Controller is not dependable. Use one of the following methods to clear the error.
  - Perform the restore operation again.
  - Clear all of memory and then download the project from the Sysmac Studio.
- If the unit configuration in the backup file is not consistent with the actual unit configuration of the restore destination, executing the restore results in a restore execution error.
- If the present values of variables that are set to be retained (with the Retain attribute) are not set to be restored, the previous present values of those variables will be retained. However, the values of any variables that do not meet the retain conditions are initialized. These are the retain conditions for the variable:
  - The variable name, data type name, and data type size must be the same before and after restoring the data.
- The SD Memory Card will remain mounted after completion of the restore operation.
- The write protection for the Communication Control Unitthat is set in the **Write Protection at Startup** setting is used after completion of the restore operation.

Procedure

● Backing Up Data with the Communication Control Unit Front-panel DIP Switch

Processing stage	Procedure
Start command	Turn ON the power supply to the Communication Control Unit with the DIP switch 1 to 4 set as follows: 1: OFF, 2: OFF, 3: ON, and 4: ON.
Executing	While Restoring Data The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds. The RUN indicator will flash, lighting for 0.5 seconds and going out for 0.5 seconds. The SD BUSY indicator will flash irregularly.
Execution results	Normal End: The SD PWR indicator will light. Error End: The SD PWR indicator will flash, lighting for 0.5 seconds and going out for 0.5 seconds. The indicator stop flashing and stay lit when the SD Memory Card power supply switch is pressed. *1

*1. If an SD Memory Card is not inserted, the SD PWR indicator will not light.

13-2-3 Verify (between Controller and SD Memory Card)

You can compare the Communication Control Unit data and the data in a backup file on the SD Memory Card in the Communication Control Unit.

Processing Contents

- The Communication Control Unit data and the data in the backup file that is saved in the specified directory of the SD Memory Card are compared.
- The data groups that are processed by the *restoration operation* are specified in the RestoreCommand.ini file (restore command file).
- The present values of variables are not compared because these values may change while the verification is in process.
- When you verify the data, the *verification results file (VerifyResult.log)* is created in the specified directory. The verification results are stored in this file. If a verification results file already exists in the specified directory, it will be overwritten. However, if the SD Memory Card is write-protected, the verification results files will not be created.
- If there is not a restore command file in the specified directory of the SD Memory Card, all of the data from the backup files in the specified directory that can be compared will be compared.
- If the unit configuration in the backup file is not consistent with the actual unit configuration of the verification destination, a verification error occurs.
- The SD Memory Card will remain mounted after completion of the verification operation.

Procedure

● Backing Up Data with the Communication Control Unit Front-panel DIP Switch

Processing stage	Procedure
Start command	The verification operation starts when the SD Memory Card power supply switch is pressed for 3 seconds with the DIP switch pins set as follows: 1: OFF, 2: OFF, 3: OFF, and 4: OFF.
Executing	Immediately after Starting Verification*1 The SD PWR indicator will light, go out for 0.5 seconds, and then light again. While Verifying Data The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds. The SD BUSY indicator will flash irregularly.
Execution results	Normal End with No Differences Found: The SD PWR indicator will light. Normal End with Differences Found: The SD PWR indicator will flash, lighting for 0.5 seconds and going out for 0.5 seconds. The indicator stop flashing and stay lit when the SD Memory Card power supply switch is pressed. Error End: The SD PWR indicator will flash, lighting for 0.5 seconds and going out for 0.5 seconds. Press the SD Memory Card power supply switch so that the indicator will light.

*1. If an SD Memory Card is not inserted, the SD PWR indicator will not light.

● Verifying Data from the SD Memory Card Window on the Sysmac Studio

Processing stage	Procedure
Start command	Click the **Compare SD Memory Card Backup** Button on the SD Memory Card Window in Sysmac Studio, specify the directory that contains the file to compare, and execute the verification.
Executing	A screen indicating the progress of verification is displayed. The SD PWR indicator will flash, lighting for 3 seconds and going out for 0.5 seconds. The SD BUSY indicator will flash irregularly.
Execution results	The results of the verification are displayed in the dialog box.

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for specific procedures.

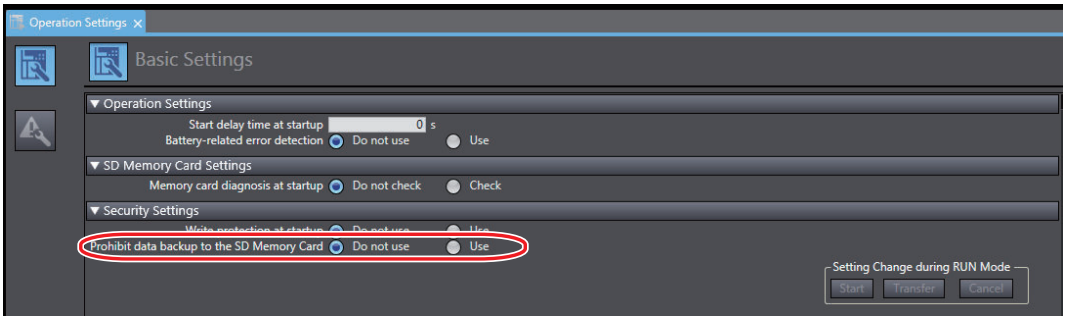
13-3 Disabling Backups to SD Memory Cards

You can disable the backup function from writing data to the SD Memory Card This function will help you protect user assets.

The function to disable backups to SD memory cards applies to the following two backup actions:

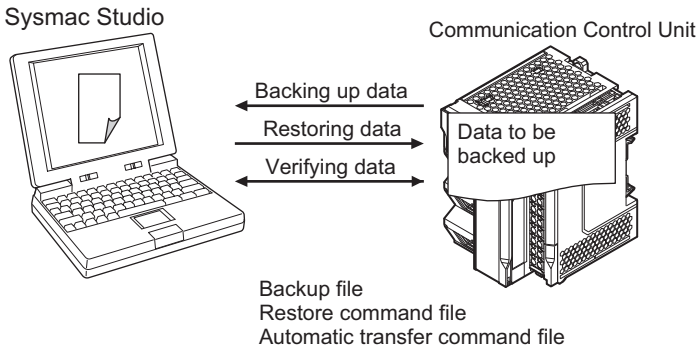
- Backup by using the front-panel DIP switch on the Communication Control Unit
- Backups from the SD Memory Card Window on the Sysmac Studio

Use the following procedure to set the Prohibit data backup to the SD Memory Card setting.
Select **Use** for the Prohibit data backup to the SD Memory Card setting in the Basic Settings Display of the Operation Settings Tab Page under Configurations and Setup - Controller Setup on the Sysmac Studio.



13-4 Sysmac Studio Controller Backups

You can use the Sysmac Studio to back up, restore, and verify the Communication Control Unit data from a computer.



When you back up data, the *backup file*, *restore command file*, and *automatic transfer command file* are created in the specified directory in the computer. The functions of the backup-related files are given in the following table.

File	Function			
	Contents	Backing up data	Restoring data	Verifying data
Backup file	This file contains the Communication Control Unit data that is handled by the backup-related functions.	Created.	Accessed.	Accessed.
Restore command file	This file specifies the data groups to transfer when restoring data. You can edit this file with a text editor on a computer to specify the data groups to transfer.	Created.	Accessed.	Accessed.
Automatic transfer command file	This file is not used with the Communication Control Unit.	Created.	Nothing is done.	Nothing is done.

13-4-1 Backup (Controller to Computer)

The Communication Control Unit data is saved in the specified directory on the computer.

Processing Contents

- For the Units and slaves settings in the backup data, you can select only NX Units that are connected to the Communication Control Unit.
- The backing up conditions for data groups are given in the following table.

Data group	Backing up condition
Data and Settings	**CPU Unit** must be selected.
IP address of the built-in EtherNet/IP port*1	**CPU Unit** must be selected.
Present values of variables	**CPU Unit** must be selected.

Data group	Backing up condition
Event logs	**CPU Unit** must be selected.
Units and slaves settings	**NX Units on the CPU Rack** must be selected.
X Bus Unit Settings	The *X Bus Unit* must be selected.*Processing Contents* on page 13-16
IP address of an EtherNet/IP port on an X Bus Unit	The *IP address of an EtherNet/IP port on an X Bus Unit* must be selected.*Processing Contents* on page 13-16

*1. Values of the IP address switch of Communication Control Unit are not included for the data backup function.

- When you back up data, the backup file, restore command file, and automatic transfer command file are created in the specified directory in the computer.
- If the backup-related files are already in the specified directory, they are overwritten.
- If an error occurs while writing the backup-related files to specified directory, the previous backup-related files will be deleted. Also, the new backup-related files will not be created.
- If an error occurs before the new backup-related files are created, the previous files are retained and the new files are not created.
- The value of the *_BackupBusy* (Backup Function Busy Flag) system-defined variable will be TRUE during the backup operation.

Procedure

1. Select **Backup** − **Backup Controller** from the Tools Menu on the Sysmac Studio.
2. Specify the folder in which to save the backup file, restore command file, and automatic transfer command file.
3. Click the **Execute** Button on the Backup Confirmation Dialog Box.
   The data is backed up and the backup file, restore command file, and automatic transfer command file are created.

13-4-2 Restore (Computer to Controller)

The data in a backup file in the specified directory on the computer is restored to the Communication Control Unit.

Processing Contents

- The data in a backup file in the specified directory on the computer is restored to the Communication Control Unit.
- You can select the data groups to restore from the Sysmac Studio. The conditions for restoring the data are given in the following table.

Data group	Restoring condition
Data and settings	The **CPU Unit** must be selected.

Data group	Restoring condition
The IP address of built-in EtherNet/IP port*1	The **IP address in Built-in EtherNet/IP Port Settings** must be selected.
Present values of variables	The **present values of variables with Retain attribute** must be selected.
Units and slaves settings	The **NX Units on the CPU Rack** must be selected.
X Bus Unit Settings	The *X Bus Unit* must be selected.*Processing Contents* on page 13-17
IP address of an EtherNet/IP port on an X Bus Unit	The *IP address of an EtherNet/IP port on an X Bus Unit* must be selected.*Processing Contents* on page 13-17

*1. Values of the IP address switch of Communication Control Unit are not backed up. Please set them manually as required.

- If an error occurs in the checks that are performed before starting to restore the data, the previous data will be retained in the Communication Control Unit.
- If the power supply to the Communication Control Unit is interrupted while the data is being restored, a User Program/Controller Configurations and Setup Transfer Error (a major fault level Controller error) will occur. If that occurs, the data in the Communication Control Unit is not dependable. Use one of the following methods to clear the error.
  - Perform the restore operation again.
  - Clear all of memory and then download the project from the Sysmac Studio.
- If the present values of variables that are set to be retained (with the Retain attribute) are not set to be restored, the previous present values of those variables will be retained. However, the values of any variables that do not meet the retain conditions are initialized. These are the retain conditions for the variable:
  - The variable name, data type name, and data type size must be the same before and after restoring the data.

Procedure

1. Select **Backup** − **Restore Controller** from the Tools Menu on the Sysmac Studio.
2. Specify the folder that contains the backup file and restore command file.
3. Click the **Execute** Button on the Restoration Confirmation Dialog Box.
   The restoration operation is executed.

13-4-3 Verify (between Controller and Computer)

The Communication Control Unit data and the data in a backup file in the specified directory on the computer are compared.

Processing Contents

- The Communication Control Unit data and the data in a backup file in the specified directory on the computer are compared. You can select the data groups to verify from the Sysmac Studio. The

conditions for verifying the data are given in the following table. If you specify all data, all of the following data will be compared.

Data group	Verification condition
Data and Settings	**CPU Unit** must be selected.
IP address of built-in EtherNet/IP port*1	**IP address in Built-in EtherNet/IP Port Settings** must be selected.
Units and slaves settings	**NX Units on the CPU Rack** must be selected.
X Bus Unit Settings	The *X Bus Unit* must be selected.*Processing Contents* on page 13-18
IP address of an EtherNet/IP port on an X Bus Unit	The *IP address of an EtherNet/IP port on an X Bus Unit* must be selected.*Processing Contents* on page 13-18

*1. Values of the IP address switch of Communication Control Unit are not included for the data backup function. Set these values manually as required.

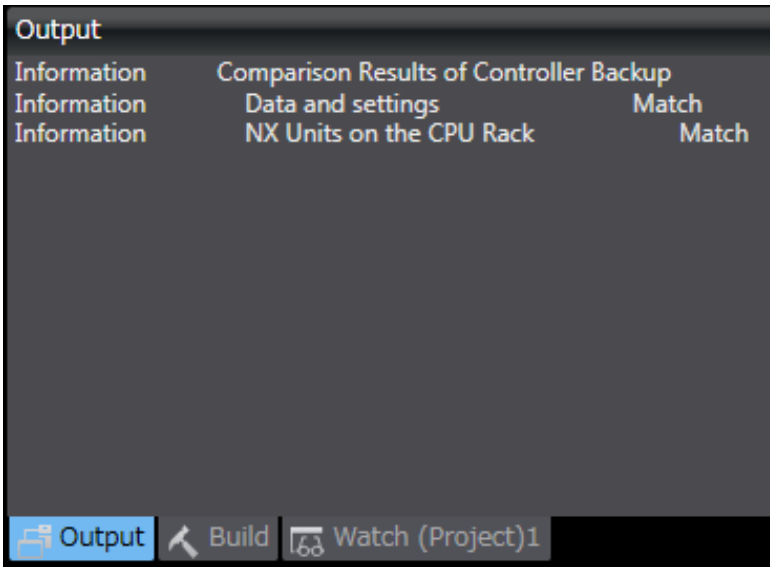
- The results of the verification are displayed in the dialog box on the Sysmac Studio.
- The value of the *_BackupBusy* (Backup Function Busy Flag) system-defined variable will be TRUE during the backup operation.

Operating Method

1 Select **Backup** − **Compare with Backup File** from the Tools Menu on the Sysmac Studio.

2 Specify the folder that contains the backup file.

3 Click the **Execute** Button on the dialog box.
The data is compared and the verification results are displayed in the Output Tab Page.



13-5 Importing and Exporting Sysmac Studio Backup File Data

You can create or read from a backup file in the specified directory on the computer from the Sysmac Studio project without using the Communication Control Unit.
This following data is processed:

Function		Data group			
		User program and settings		Present values of variables	Units and slaves settings
			IP address of built-in EtherNet/IP port*1*2		
Importing and exporting Sysmac Studio backup file data	Exporting backup file data	Possible*3	Possible	Not possible	Not possible
	Importing backup file data	Possible*4	Possible	Not possible	Possible

*1. IP address of the Built-in EtherNet/IP Port Settings can be used as a data group.
*2. Values of the IP address switch of Communication Control Unit are not included for the data backup function.
*3. The following data is not processed.
- The built-in EtherNet/IP port name in the Controller name
- The built-in EtherNet/IP tag data link settings in the Controller Setup
- Operation Authority Verification

*4. The following data is not processed.
- The built-in EtherNet/IP port name in the Controller name
- Operation Authority Verification

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for more information on these functions.

13-6 Backup Functions when NX Units are Connected

For NX Units on the Communication Control Unit, you can use the SD Memory Card backup functions and the Sysmac Studio Controller backup functions.
This section provides information on the data that is backed up, backup support according to the Communication Control Unit status, and restore conditions when NX Units are connected to the Communication Control Unit.

Precautions for Correct Use

You cannot back up, restore, or compare data for Safety Control Units on the Communication Control Unit. Refer to *Section 12 Safety Unit Restore* on page 12-1 for details on the restore operations of the Safety Control Unit.

13-6-1 Backing Up Data in NX Units on the Communication Control Unit

The data that is backed up for NX Units on the Communication Control Unit is given in the following table.

Unit	Data	Backup	Restore	Compare
NX Units	Configuration information*1	Possible	Possible	Possible
	Unit operation settings	Possible	Possible	Possible
	Unit application data*2	Possible	Possible	Possible

*1. The configuration information includes the Unit configuration information and I/O allocation information.
*2. This is the specific data for each NX Unit. Some NX Units do not have Unit application data.

13-6-2 Backup Support Depending on the Controller Status

The following table shows when backup, restore, and compare operations can be performed for NX Units based on the Controller status.

Controller status	Execution		
	Backing up data	Restoring data	Verifying data
Automatic creation of the Unit configuration information	Possible*1	Possible*2	Possible
Watchdog time error in NX Unit	Not possible*3	Not possible*4	Possible*5
During NX Bus Controller Error	Not possible*3	Not possible*4	Possible*5
During Unit Configuration Verification Error	Not possible*3	Possible	Possible*5
The Unit configuration information does not agree with the Unit configuration information in the backup data.	---	Not possible*4	Possible*5

*1. The backup contains information saying that the Unit configuration information does not exist.
*2. After the data is restored, automatic Unit configuration status continues.
*3. An NX Unit Backup Failed event is recorded in the event log.
*4. An NX Unit Restore Operation Failed event is recorded in the event log.
*5. The verification results will show differences.

13-6-3 Conditions for Restoring NX Unit Data on the Communication Control Unit

The following conditions must be met before you restore the backup data to the NX Units on the Communication Control Unit.

- The backup files must contain the data for the Communication Control Unit and NX Unit on the Communication Control Unit.
- The original Unit configuration in the backup must match the actual Unit configuration where data is being restored.
- The serial numbers of the NX Units from which the data was backed up and the serial numbers of the NX Units to which the data is restored must be the same. However, this assumes that the setting of the **Serial Number Check Method** in the **CPU Racks** in the backup file is set to *Setting = Actual device*.
- The unit version settings of the NX Unit from which the data was backed up and the unit versions of the actual NX Units to which the data is restored must be the same.

13-7 Backup-related Files

This section describes the specifications of the backup-related files.

13-7-1 Types of Backup-related Files

There are four types of files that are related to backup functions: backup files, restore command files, automatic transfer command files, and verification results files.

● Backup File

This file contains the Communication Control Unit data that is handled by the functions that are related to data backup. These files are created when data is backed up.

● Restore Command File

This file specifies the data groups to transfer by restoring data from an SD Memory Card. You can edit this file with a text editor on a computer to specify the data groups to transfer. These files are created when data is backed up.

● Automatic Transfer Command File

This file is not used for the Communication Control Unit.

● Verification Results Files

The verification results files contain the results of comparing the Communication Control Unit data and the data in a backup file on the SD Memory Card in the Communication Control Unit.
There are two different verification results files, as described below. These files are generated when you perform a verification using the SD Memory Card backup function.

Verification results files	Description
Controller verification results file	This file contains the verification results for all backup data specified by the restore command file.
NX Unit verification results file	This file contains the verification results for each NX Unit on the Communication Control Unit. It is generated when the Unit and slave settings are set to be restored in the restore command file and the backup file contains settings of the NX Unit on the Communication Control Unit.
X Bus Unit verification results file*Verification Results Files* on page 13-23	This file contains the verification results for each X Bus Unit. It is generated when the Unit and slave settings are set to be restored in the restore command file and the backup file contains settings of the X Bus Unit.

13-7-2 Specifications of a Backup File

This section describes the file name, creation timing, and created directory for a backup file.

File Name

File	File name
Backup file	NXBackup.dat

File Creation Timing and Created Directories

Function	Procedure	Creation timing	Created directory
SD Memory Card backups	Communication Control Unit Front-panel DIP Switch	When backup is executed	Root directory on the SD Memory Card
	SD Memory Card Window in Sysmac Studio	When backup is executed	Directory on the SD Memory Card that you specified with the Sysmac Studio
Sysmac Studio Controller backups	Sysmac Studio Controller Backup Dialog Box	When backup is executed	Directory in the computer that you specified with the Sysmac Studio
Importing and exporting Sysmac Studio backup file data	Sysmac Studio Backup File Export Dialog Box	When data is exported	Directory in the computer that you specified with the Sysmac Studio

13-7-3 Specifications of a Restore Command File

This section describes the file name, creation timing, created directory, and data group specification method for a restore command file.

File Name

File	File name
Restore command file	RestoreCommand.ini

File Creation Timing and Created Directories

Function	Procedure	Creation timing	Created directory
SD Memory Card backups	Communication Control Unit Front-panel DIP Switch	When backup is executed	Same directory as backup file
	SD Memory Card Window in Sysmac Studio	When backup is executed	Same directory as backup file
Sysmac Studio Controller backups	Sysmac Studio Controller Backup Dialog Box	When backup is executed	Same directory as backup file
Importing and exporting Sysmac Studio backup file data	Sysmac Studio Backup File Export Dialog Box	When data is exported	Same directory as backup file

Specifying the Data Groups to Restore

The restore command file allows you to specify the data groups to restore.
You can change the data group specifications by editing the file with a text editor on a computer.

For example, if you change *Variable=yes* on line 8 in the *File contents* that are shown in the following table to *Variable=no*, the *present values of variables* will not be restored.

File contents (defaults when the file is created)	Description
[Restore] ; --- User Program and Configuration. --- ; Always select "yes". UserProgram=yes	Not used in Communication Control Unit.
; --- IP Address of Built-in EtherNet/IP Port Settings. --- ; "yes":will be restored, "no":will not be restored IPAdr=yes	IP address of built-in EtherNet/IP port yes/no: Restore/Do not restore.
; --- Present values of variables (Retained variables only). --- ; "yes":will be restored, "no":will not be restored Variable=yes	Present values of variables (only variables that are set to be retained with the Retain attribute) yes/no: Restore/Do not restore.
:---Unit/Slave Parameters.--- ; "yes";will be restored."no";will not be restored UnitConfig=yes	Units and slaves settings yes/no: Restore/Do not restore.

Note 1. The default file contents when the restore command file is created are given above. All of the data groups that are listed in the file are set to be restored.

Note 2. The restore command file lists the restorable data groups that were in the backup file when the backup file was created.

Note 3. Only single-byte alphanumeric characters are used. The text is not case sensitive.

Precautions for Correct Use

When you edit the restore command file, do not change anything in the file except for the “yes” and “no” specifications for the selectable data groups. If you change anything else in the file, the Controller may perform unexpected operation when you restore the data.

13-7-4 Specifications of a Controller Verification Results File

This section describes the file name, creation timing, created directory, and verification results confirmation method for a Controller verification results file.

File Name

File	File name
Controller verification results file	VerifyResult.log

File Creation Timing and Created Directories

Function	Procedure	Creation timing	Created directory
SD Memory Card backups	SD Memory Card Window in Sysmac Studio	When verification is executed	Same directory as backup file
	Communication Control Unit Front-panel DIP Switch	When verification is executed	Same directory as backup file

Note However, if the SD Memory Card is write-protected, the verification results files will not be created.

How to Check the Verification Results

The verification results files contain the results of comparing the Communication Control Unit data and the data in a backup file on the SD Memory Card in the Communication Control Unit for each data group.
You can check the verification results in the portion that gives the verification results for each data group.
Result=Matched indicates a data group for which no differences were found. *Result=Not matched* indicates a data group for which differences were found.
In the file shown below, the user program and configuration data matched, and the Units and slave parameters did not match.

File contents	Description
[UserProgram] ; --- User Program and Configuration. --- Result=Matched	 User program and settings Matched: No differences were found, Not matched: Differences were found.
[UnitConfig] ; --- Unit/Slave Parameters. --- Result=Not matched	Units and slaves settings Matched: No differences were found, Not matched: Differences were found.

Note The verification results are given only for the data groups that were compared.

13-7-5 Specifications of an NX Unit Verification Results File

This section describes the file name, creation timing, created directory, and verification results confirmation method for an NX Unit verification results file.

File Name

File	File name
NX Unit verification results file	VerifyResult_NXUnit.log

File Creation Timing and Created Directories

Function	Procedure	Creation timing	Created directory
SD Memory Card backups	SD Memory Card Window in Sysmac Studio	When verification is executed	Same directory as backup file
	Communication Control Unit Front-panel DIP Switch	When verification is executed	Same directory as backup file

Note However, if the SD Memory Card is write-protected, the verification results files will not be created.

How to Check the Verification Results

The verification results files contain the results of comparing the Communication Control Unit data and the data in a backup file on the SD Memory Card in the Communication Control Unit for each data group.

You can check the verification results in the portion that gives the verification results for the NX Units. *Result=Matched* indicates a data group for which no differences were found. *Result=Not matched* indicates a data group for which differences were found.

The following table gives an example of the verification results for the following file contents.

- Matched: NX Unit N1
- Not matched: NX Unit N3
- Not verified: NX Unit N2

File contents	Description
[Verification Results] ; --- NX Parameters. --- [N1:UnitNo.1 NX-AD2203] Result=Matched [N2:UnitNo.2 NX-DA2203] Result=Not verified [N3:UnitNo.3 NX-TS3201] Result=Not matched Factor=Verification error	The Units are indicated in the following format: {Device name}:UnitNo.{Unit number}[blank]{Unit model} Device Name: The device name set by the user. Unit Number: Text string of decimal numbers. The value will be between 0 and 125. Unit Model: Text string that identifies the Unit model. Consecutive spaces at the end of the model number are deleted. The verification results are given as follows: Result=Matched Same Result=Not matched Different Result=Not verified No verification

13-8 Compatibility between Backup-related Files

The files may not be compatible if you back up and restore data under different conditions.
The files may not be compatible in these three cases:

- When the function that was used to back up data is different from the function that was used to restore it.
- When the model number of the Communication Control Unit where the data was backed up from does not match the model number where data is being restored.
- When the unit versions of the Communication Control Unit or units where the data was backed up from do not match the unit versions where data is being restored.

In this context, the term *restore* is used collectively for these backup functions: *restore* and *read* (back up).

13-8-1 Compatibility between Backup Functions

The following table shows the file compatibility when the function used to back up the data is different from the function used to restore it.

Function used to back up data	Function used to restore data			
	Restoring with SD Memory Card backup functions (SD Memory Card to Controller)	Automatic transfer and program transfer	Restoring with Sysmac Studio Controller backup functions (computer to Controller)	Importing Sysmac Studio backup file data (computer to project)
Backing up with SD Memory Card backup functions (Controller to SD Memory Card)	Compatible	Compatible	Compatible	Compatible*1
Backing up with Sysmac Studio Controller backup functions (Controller to computer)	Compatible	Compatible	Compatible	Compatible*1
Exporting from a Sysmac Studio backup file (Project to computer)	Compatible*1	Compatible*1	Compatible*1	Compatible

*1. The following data is not included.
- The built-in EtherNet/IP port name and built-in EtherNet/IP tag data link settings in the Controller Setup
- Operation Authority Verification
- Time Zone Setting
- Present Values of Variables

13-9 Functions That Cannot Be Executed during Backup Functions

The following functions cannot be executed at the same time as any of the backup functions. Do not execute any backup function while the Communication Control Unit is executing any of these functions. Also, do not execute any of these functions during execution of any of the backup functions.

- While a backup function is being performed
- Synchronization transfer from the computer to the Controller
- Execution of Memory All Clear operation
- Time zone changes
- Execution of Communication Control Unit name write operation

14

Safety Data Logging

This section describes the Safety Data Logging function.

14-1 Outline of the Safety Data Logging Function 14-2

14-2 Creating a Safety Data Logging Settings File with the Sysmac Studio 14-4

14-3 Safety Data Logging Operation Procedure 14-6

14-4 Checking the Logging Status 14-7

14-4-1 Checking the Seven-segment Indicator 14-7

14-4-2 Checking with System-defined Variables 14-7

14-5 Log File Specifications 14-9

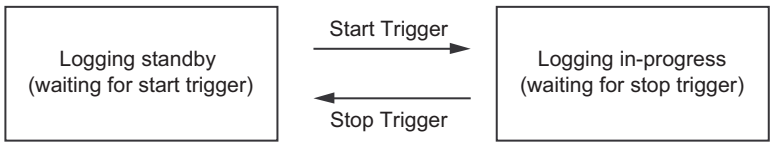
14-1 Outline of the Safety Data Logging Function

The safety data logging is a function that records exposed variables and device variables used in the safety program of the Safety CPU Unit in a chronological order. The function logs the specified variables in the volatile memory and saves the log data into the SD Memory Card before and after the trigger condition is met.

This section provides the specifications of the safety data logging.

Item	Specifications
Number of logging settings	2 max. Specify the respective settings including sampling interval, trigger conditions, and logging target.
Number of records	3000 records per setting
Sampling interval	Select any of the following per setting: 5 ms/10 ms/25 ms/50 ms/100 ms
Trigger condition	One variable can be specified as a trigger condition for each setting. BOOL variables: True or False Non-BOOL variables: Select any of the following and specify a constant: =: Equal to the constant ≠: Not equal to the constant >: Greater than the constant <: Less than the constant ≥: Equal to or greater than the constant ≤: Equal to or less than the constant
Logging target	Up to 100 exposed variables and devices variables can be specified for each setting.
Storage location of the safety data logging settings file and log files	The data is saved in the following folder of the SD Memory Card that is mounted in the Communication Control Unit. /SFLog/

The safety data logging function works as follows:



Status	Operation
Logging standby (waiting for start trigger)	The safety data logging is not in progress. When the start trigger is detected, it enters the "logging in-progress" state.
Logging in-progress (waiting for stop trigger)	The safety data logging is in progress. The log data is constantly recorded in the ring buffer of the volatile memory. When the buffer becomes full, the oldest log is discarded in order. When the unit enters the logging standby state with the stop trigger, logs in the buffer are saved into the SD Memory Card.

Start Trigger

When the following condition is met in the logging standby state, the start trigger is activated and the unit enters into the logging in-progress state.

- The service switch is pressed for operation after all the safety master connections were established.

However, if the logging settings file is configured to start logging at a startup, you do not need to press the service switch to start the logging in-progress state for the first logging.

Stop Trigger

The stop trigger is activated by the following factors:

Stop factors	Logging to be stopped	Log files to be saved
When the trigger condition specified in a safety data logging settings file is met	Stop only the logging for which the trigger condition is met	Save only log files recorded for the logging setting for which the trigger condition is met.
When the stop operation is performed with the service switch	Stop all the loggings in progress	Save log files for all the logging settings in progress.
When a communication error occurs in the safety master connections (FSoE master connection or CIP Safety originator connection)	Stop all the loggings in progress	Save log files for all the logging settings in progress.
When the operation to stop the FSoE or CIP Safety communications is performed • When the operating mode of the Safety CPU Unit changes • The setting is transferred to the Communication Control Unit • The NX bus restart is executed, etc.	Stop all the loggings in progress	Save log files for all the logging settings in progress.

When the unit enters the logging standby state with the stop trigger, logs into the buffer are saved into the SD Memory Card.

Precautions for Correct Use

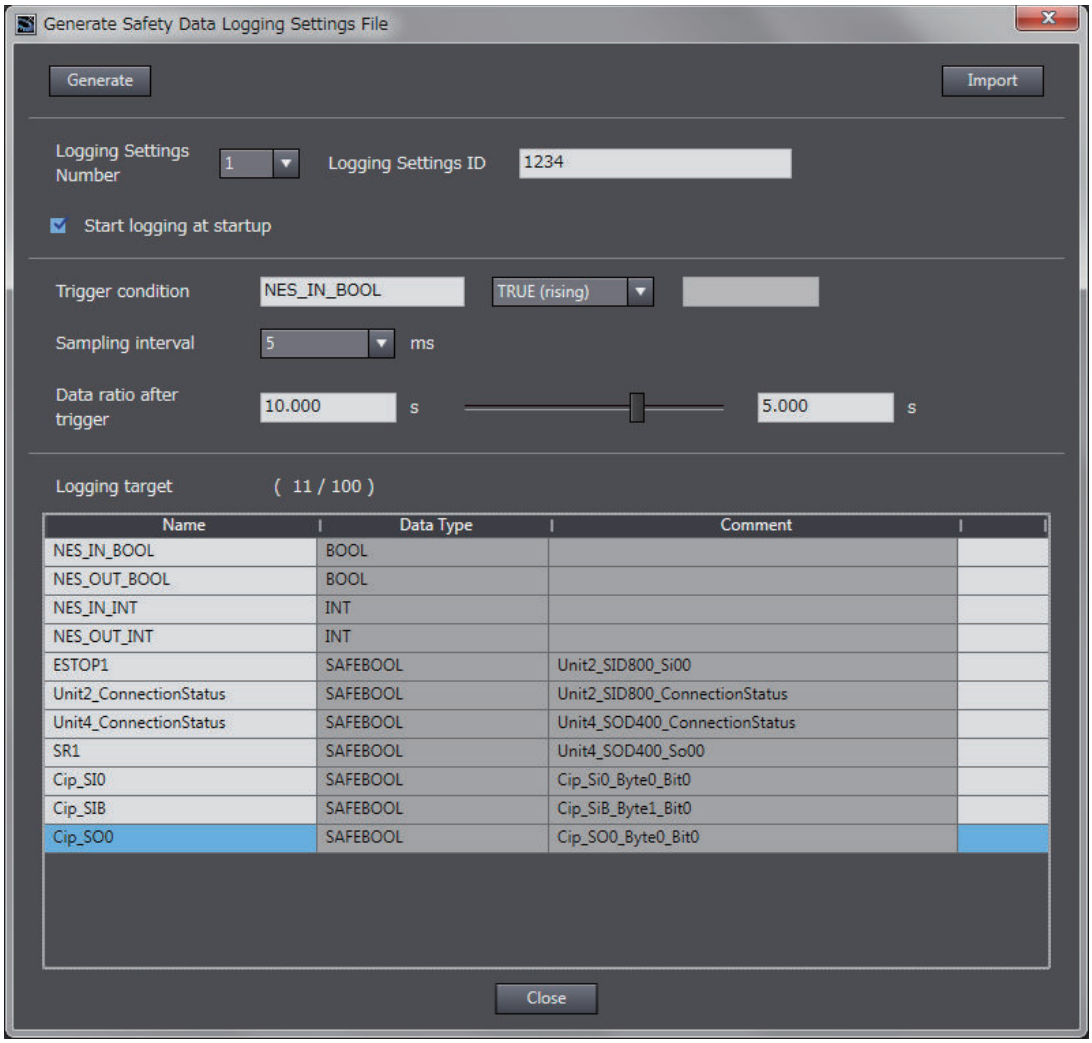
Do not turn OFF the power supply to the Communication Control Unit while data is being transferred. Otherwise, the files may be damaged.

14-2 Creating a Safety Data Logging Settings File with the Sysmac Studio

The Sysmac Studio allows you to create a safety data logging settings file.
Safety validation must be completed for the safety application data. Refer to *9-11 Performing Safety Validation and Operation* on page 9-59 for details on the safety validation of safety application data.

Use the following procedure to create a safety data logging settings file.

1 From the Controller selection in the Multiview Explorer, select the Safety CPU Unit and then go to **Tools** – **Generate Safety Data Logging Settings File**.
The **Generate Safety Data Logging Settings File** Window shown below appears.



The structure of the **Safety Data Logging Settings File** Window is as follows:

Item	Description
Logging Settings Number	Select 1 or 2. Up to two safety data logging settings files can be saved in the SD Memory Card. The logging settings ID for each file must be unique.

Item	Description
Logging Settings ID	An ID number is specified to associate a logging settings file with relevant log files as its logging result. This ID number is used as part of their file names so that the safety data logging settings file and the corresponding log files can be identified.
Start logging at startup	Selected: The safety data logging is executed at a startup without pressing the service switch. Not selected: The service switch operation is required for executing the safety data logging.
Trigger condition	Specify a variable and a condition expression as the trigger to stop the safety data logging. Left box: Specify a variable name. Right box: Specify a constant value to compare. List in the middle: Select from the following. For BOOL: Select either True or False. For other than BOOL: Select one of the following options: =: Equal to the constant ≠: Not equal to the constant >: Greater than the constant <: Less than the constant ≥: Equal to or greater than the constant ≤: Equal to or less than the constant
Sampling interval	Select a sampling interval.
Data ratio after trigger	Specify a ratio of the log data after the trigger to that before the trigger.
Logging target	Up to 100 variables can be registered for logging. Name: Specify the name of the variable is specified. Data Type: The data type of the variable is displayed. Comment: The comment for the variable is displayed.
Generate Button	This button allows you to save a safety data logging settings file into a folder you specify.
Import Button	This button allows you to import a safety data logging settings file.

2 Specify the settings and click the **Generate** Button.

When you specify a save destination in the displayed dialog box and click the **OK** Button, the following file will be generated.

File name*1	Application
SFLogConfig_<N>_<ID>_<SIGNATURE>.dat	Safety data logging settings file. This file is used for the safety data logging function.
SFLogConfig_<N>_<ID>_<SIGNATURE>.txt	Confirmation file for safety data logging settings. A text file in which the settings are visualized. This file is not used for the safety data logging function.

*1. The meaning of the extensions used for file names is as follows:
N: Logging Settings Number
ID: Logging Settings ID
SIGNATURE: Safety Signature

3 Store the safety data logging settings file in /SFLog/ on the SD Memory Card.

14-3 Safety Data Logging Operation Procedure

Use the following procedure to execute the safety data logging function:

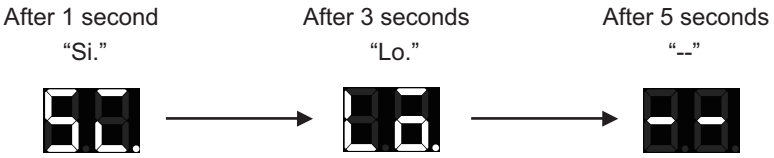
1 Find the SD Memory Card that contains the safety data logging settings file in the specified folder. Insert the SD Memory Card into the SD Card Slot of the Communication Control Unit to which the Safety CPU Unit is connected.

2 Set the DIP switch on the front panel of the Safety CPU Unit to turn ON SW2, and OFF SW1, SW3 and SW4.

3 Start or restart the Communication Control Unit and the Safety CPU Unit.

4 If the logging settings file is configured to start logging at a startup, the logging execution starts when all the safety master connections are established.
If the logging settings file is not configured to start logging at a startup, press the service switch on the front panel of the Safety CPU Unit after confirming that all the safety master connections are established.

If you hold down the service switch, the display of the seven-segment indicator will change as shown below.



Release the service switch while the indicator shows "Lo".
If you release the service switch while "--" is displayed, the function is not executed and the original state is restored.

5 Check the left dot of the seven-segment indicator on the Safety CPU Unit to see if the logging execution started normally.
If it starts normally, the left dot is lit. If it fails, the left dot is flashing.

6 Check the left dot of the seven-segment indicator on the Safety CPU Unit to see if the trigger condition was met and the log files were output.
When output of all the log files is completed, the left dot goes out and the right dot lights up.
If the log files are not saved successfully, the right dot starts flashing.

By following Step 4, you can manually stop the logging that is in progress.

7 Remove the SD Memory Card.

14-4 Checking the Logging Status

You can verify the logging status in the following methods:

- Checking the seven-segment indicator of the Safety CPU Unit.
- Checking with system-defined variables

14-4-1 Checking the Seven-segment Indicator

The logging status is displayed with the right and left dots of the seven-segment indicator of the Safety CPU Unit as shown below.

Display area	Display	Description
Left dot of the seven-segment indicator of the Safety CPU Unit	Not lit	No logging is in progress.
	Lit	Logging is in progress.
	Flashing (0.5-s interval)	Logging did not start.
Right dot of the seven-segment indicator of the Safety CPU Unit	Not lit	No log file was output.
	Lit	A log file was saved successfully.
	Flashing (0.5-s interval)	A log file was not saved successfully.

14-4-2 Checking with System-defined Variables

You can verify the logging execution status by checking the system-defined variables of the Communication Control Unit.

The Communication Control Unit has the following system defined variables for each logging setting. For details on the system-defined variables, refer to *System-defined Variables* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)*.

Variable Member name	Meaning	Function	Data Type	R/W
_PLC_SFLogSta	Safety Data Logging Status	Stores the status of safety data logging. Element number 0 corresponds to Logging Setting Number 1. Element number 1 corresponds to Logging Setting Number 2.	ARRAY[0..1] OF _sSFLOG_STA	R

Variable		Meaning	Function	Data Type	R/W
	Member name				
	.IsStart	Safety Data Logging Busy Flag	The value becomes 1 (ON) when starting the safety data logging, and 0 (OFF) when stopping the safety data logging.	BOOL	R
	.IsComplete	Safety Data Logging Completed Flag	The value becomes 1 (ON) when the logging stops. The value becomes 0 (OFF) when the next logging starts. When this flag is turned ON, it means that the logging is completed.	BOOL	R
	.IsOutput	Log File Output Completed Flag	The value becomes 1 (ON) when a log file is output. The value becomes 0 (OFF) when the next logging starts.	BOOL	R

14-5 Log File Specifications

Log files are stored in the SD Memory Card.

A log file is saved as a comma-delimited text file with a csv extension.
Log file specifications are described below.

Item	Specifications
Log file name*1 *2	SFLog_<N>_<ID>_<SIGNATURE>_<Date of output>_<Time of output>.csv
File location	/SFLog/

*1. N, ID, and SIGNATURE in a log file name are each set with the same text string set for the corresponding identifier in the file name of the relevant safety data logging settings file. The meaning of each identifier is as follows.
N: Logging Settings Number
ID: Logging Settings ID
SIGNATURE: Safety Signature

*2. As identifiers, the date of output is set as YYYYMMDD, and the time of output is as hhmmss.

The header row of a log record is output in the first row. The contents of the log record are output in the second and following rows.

Column	Item	Description
1st column	Record index (index)	Index number of the record. 0 to 2999
2nd column	Sampling time (time)	Sampling execution time. It is based on the time information configured in the Communication Control Unit. YYYY-MM-DD hh:mm:ss.ms
3rd column	Condition is met (condition)	When the trigger condition is met for the record, 1 is output. * If the logging is stopped by pressing the service switch, there may be no record with 1 for this value.
4th column and later	Sampling data (variable name)	It lists all the sampling data corresponding to the number of logging target variables. All data is expressed in decimal notation. BOOL/SAFEBOOL: 0 (FALSE), 1 (TRUE) BYTE: 0 to 255 WORD/SAFEWORD: 0 to 65535 INT/SAFEINT: -32768 to 32767 DINT/SAFEDINT: -2147483648 to 2147483647

After the final row of the record, the additional information (footer) shown below is output following a blank row.

Row No.	Item	Description
1st footer row	Trigger variable (condition)	The trigger condition used for the logging is output.
2nd footer row	Reason for logging stopped (StopType)	The reason for the stopped logging is provided. condition: The logging stopped because the trigger condition specified in the logging setting was met. other: The logging stopped due to any reason other than the trigger condition.

This is a log file example:
(condition)

Logging completion condition: VarX changes to FALSE
Logging target: Var1(SAFEBOOL), Var2(SAFEBOOL), Var3(WORD)
Reason for logging stopped: The trigger condition is met. (VarX changes to FALSE.) The condition was met when No2205 was read in the sampling.

```
"index","time","condition","Var1:SAFEBOOL","Var2:SAFEBOOL","Var3:WORD"
:
"2200","2017-06-16 11:16:40.443","0","1","1","153"
"2201","2017-06-16 11:16:40.448","0","1","0","153"
"2202","2017-06-16 11:16:40.453","0","1","0","153"
"2203","2017-06-16 11:16:40.458","0","1","0","153"
"2204","2017-06-16 11:16:40.463","0","1","0","153"
"2205","2017-06-16 11:16:40.468","1","1","0","153"
"2206","2017-06-16 11:16:40.473","0","1","0","153"
"2207","2017-06-16 11:16:40.478","0","1","0","153"
"2208","2017-06-16 11:16:40.483","0","1","0","150"
"2209","2017-06-16 11:16:40.488","0","1","0","150"
:
"2999","2017-06-16 11:16:40.488","0","1","0","150”

"condition:VarX=false"
"StopType:condition"
```

15

Troubleshooting

This section describes the event codes that are recorded when errors occur, and how to check and troubleshoot errors.

15-1 Operation after an Error 15-2
15-1-1 Overview of Communication Control Unit Status 15-2
15-1-2 Fatal Errors 15-4
15-1-3 Non-fatal Errors in the Communication Control Unit 15-6
15-1-4 Checking for Non-fatal Errors 15-15
15-1-5 Resetting Non-fatal Errors 15-17
15-1-6 Errors Related to the EtherNet/IP Function Module 15-19
15-1-7 Errors Related to Safety Control Units 15-20
15-1-8 Errors on CIP Safety Target Devices 15-21

15-2 Error Troubleshooting Methods 15-23
15-2-1 Troubleshooting Flowcharts 15-23
15-2-2 Troubleshooting Fatal Errors 15-24
15-2-3 Troubleshooting Non-fatal Errors 15-25
15-2-4 Troubleshooting When You Cannot Go Online from the Sysmac Studio 15-31
15-2-5 Troubleshooting Errors in the Safety Control Unit 15-35
15-2-6 Troubleshooting the CIP Safety Target Device Errors 15-43

15-3 Error Descriptions and Corrections 15-48
15-3-1 Interpreting Tables 15-48
15-3-2 Communication Control Unit Error 15-51
15-3-3 Safety CPU Unit Error 15-167
15-3-4 Safety I/O Unit Error 15-213
15-3-5 Other Troubles and Corrections 15-240

15-4 Checking Status with the Network Configurator 15-241
15-4-1 The Network Configurator's Device Monitor Function 15-241
15-4-2 Connection Status Codes and Troubleshooting 15-249
15-4-3 CIP Safety Connection Status Codes and Troubleshooting 15-257

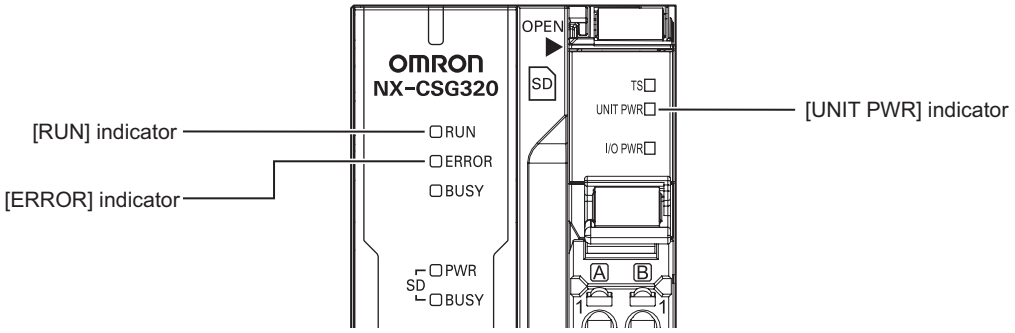
15-1 Operation after an Error

This section describes the error status of the Communication Control Unit and the Safety Control Unit, and the operation that occurs after an error is detected.
Refer to *15-2 Error Troubleshooting Methods* on page 15-23 for details on corrections for specific errors.

15-1-1 Overview of Communication Control Unit Status

You can check the operating status of the Communication Control Unit with the UNIT PWR, RUN, and ERROR indicators on the front panel of the Communication Control Unit.

Communication Control Unit



The following table shows the status of front-panel indicators and the ability to communicate with the Sysmac Studio or with an HMI during startup, during normal operation, and when errors occur.

(○: Lit / ●: Not lit / ⊙: Flashing)

Communication Control Unit operating status		Communication Control Unit			Communications with the Sysmac Studio or an HMI
		UNIT PWR (green)	RUN (green)	ERROR (red)	
Startup		○	⊙ (2-s intervals followed by 0.5-s intervals)	●	Not possible.
Normal operation		○	○	●	Possible.
Fatal error in Communication Control Unit	**Power Supply Error*1**	●	●	●	Not possible.
	Hardware Initialization Error*1*2	○	●	●	
	CPU Unit Error*1	○	● or ⊙ (2-s intervals or 0.5-s intervals)	○	
	System Initialization Error*1	○	⊙ (2-s intervals) for 30 s or longer	●	
Non-fatal error in Communication Control Unit	**Major fault*3**	○	●	○	Possible. (Communications can be connected from an HMI if EtherNet/IP is operating normally.)
	Partial fault*3	○	○	⊙ (1-s intervals)	
	Minor fault*3	○	○	⊙ (1-s intervals)	
	Observation*3	○	○	●	

*1. Refer to *15-1-2 Fatal Errors* on page 15-4 for information on individual errors.

*2. If the status of indicators shown above continues 30 seconds or longer, this error exists.

*3. Refer to *15-1-3 Non-fatal Errors in the Communication Control Unit* on page 15-6 for information on individual errors.



Precautions for Correct Use

A power shortage may occur at the CPU Rack depending on the configuration of the NX Units mounted to the Communication Control Unit. If one of the followings occurs, use the Sysmac Studio to check if the power consumed by the Units on the CPU Rack exceeds the supplied power.

- The Communication Control Unit is operating but the mounted NX Units do not operate.
- Power is supplied to the Communication Control Unit, but the Communication Control Unit does not turn ON.

Types of Errors

There are two main types of errors (events) depending on whether the Communication Control Unit can manage them or not.

● Fatal Errors in the Communication Control Unit

These errors are not detected by the event management function of the NX-series because the Communication Control Unit stops operation.
You cannot identify or reset these errors with the Sysmac Studio or an HMI.

Refer to *15-1-2 Fatal Errors* on page 15-4 for error types and confirmation methods of fatal errors in the Communication Control Unit.

● Non-fatal Errors in the Communication Control Unit

These errors are detected and managed with the event management function of the NX-series.
You can confirm these errors with the Sysmac Studio or an HMI.

Refer to *15-1-3 Non-fatal Errors in the Communication Control Unit* on page 15-6 for error types and confirmation methods of non-fatal errors in the Communication Control Unit.

15-1-2 Fatal Errors

Types of Fatal Errors in the Communication Control Unit

This section describes the errors that cause the operation of the NX-series Communication Control Unit to stop.
Communications with the Sysmac Studio or an HMI are not possible if there is a fatal error in the Communication Control Unit.

● Power Supply Error

Power is not supplied, the voltage is outside of the allowed range, or the Power Supply Unit or power supply section is faulty.

● Hardware Initialization Error

This error occurs for the NX-series Communication Control Unit. It indicates a data error in minimum programs required to initialize the hardware. Only the UNIT PWR indicator will be lit while the Communication Control Unit is starting, but if it is lit for 30 seconds or longer, then this error occurs.

● CPU Unit Error

This error can occur for the NX-series Communication Control Unit. It indicates that there is a hardware failure or that the CPU is running out of control due to temporary data corruption.

● System Initialization Error

This error can occur for the NX-series Communication Control Unit. It indicates a hardware failure or data error.

The RUN indicator will flash at 2-second intervals while the Communication Control Unit is starting, but if it flashes for 30 seconds or longer, then this error occurs.

Checking for Fatal Errors in the Communication Control Unit

You can identify fatal errors in the Communication Control Unit based on the status of the UNIT PWR, RUN and ERROR indicators, as well as by the ability to connect communications to the Sysmac Studio.
Refer to Section *15-2 Error Troubleshooting Methods* on page 15-23 for information on identifying errors and corrections.

(○: Lit / ●: Not lit / ⊙: Flashing)

Indicator			Communications with Sysmac Studio	Operating status of Communication Control Unit
UNIT PWR (green)	RUN (green)	ERROR (red)		
●	●	●	Not possible.	Power Supply Error
○	●	●		Hardware Initialization Error
○	● or ⊙ (2-s intervals or 0.5-s intervals)	○		CPU Unit Error
○	⊙ (2-s intervals) for 30 s or longer	●		System Initialization Error

15-1-3 Non-fatal Errors in the Communication Control Unit

Types of Non-fatal Errors in the Communication Control Unit

Non-fatal errors that occur in the Safety Network Controller are managed as events. You can check the event to find out what type of error occurred.

● Controller Events

The Controller automatically detects these events. Controller events include events for the function modules in the Communication Control Unit, Safety CPU Units, and Safety I/O Units.

Overview of Controller Events (Errors and Information)

You use the same methods to manage all of the events that occur on the Safety Network Controller. The events that occur are saved in the Communication Control Unit.
You can use the Sysmac Studio or an NA-series PT to confirm current Controller events and the log of events that occurred before. This log is called an event log.

To use an HMI to check events, connect the HMI to the built-in EtherNet/IP port on the Communication Control Unit.

Details on Controller Events (Errors and Information)

● Controller Event Times

The time of occurrence is recorded when an event occurs.
The time of occurrence for an event is displayed on the Sysmac Studio or HMI.

● Sources of Controller Events

The Event source information indicates the location where an event occurred.
The event source identifies the particular function module in the Communication Control Unit in which the event occurred.
For some function modules, there is more detailed information about the event source. This information is called the Source details.
The following information is provided as the event source details.

Event source	Source details
PLC Function Module	Power supply
NX Bus Function Module	Master or NX Unit
EtherNet/IP Function Module	Communications port 1, communications port 2, CIP1, CIP2, FTP, NTP, or SNMP

The event source is displayed on the Sysmac Studio or HMI.

Levels of Controller Events (Errors and Information)

The following table classifies the levels of Controller events according to the effect that the errors have on control. All events in impact levels as errors are collectively called Controller errors. All other events that are not classified into errors but mean information are called Controller information.

No.	Level	Level name	Classification
1	High	Major fault level	Controller errors
2		Partial fault level	
3		Minor fault level	
4		Observation	
5	Low	Information	Controller information

Errors with a higher level have a greater impact on the functions that the Safety Network Controller provides, and are more difficult to recover from.
When an event occurs, the Sysmac Studio or HMI will display the level name.

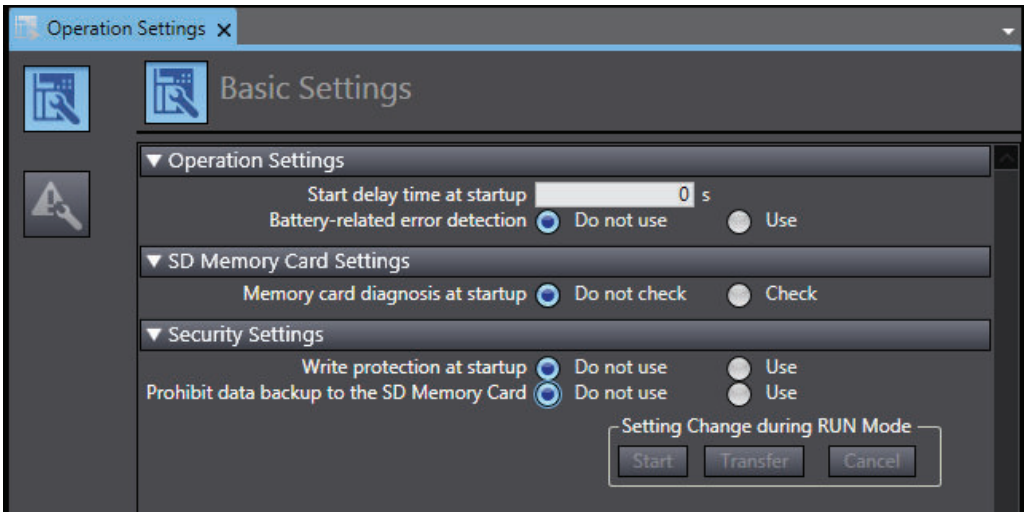
Each event level is described below.

Level	Description
Major fault level	These errors prevent control operations for the entire Controller. When the Controller detects a major fault, it turns OFF the loads of all slave, including remote I/O. You cannot reset major fault level errors from the Sysmac Studio or an HMI. To recover from a major fault level error, remove the cause of the error, and either cycle the power supply to the Controller, or reset the Controller from the Sysmac Studio.
Partial fault level	These errors prevent control operations in a certain function module in the Controller. After you remove the cause of the error, execute one of the following to return to normal status. • Reset the error from the Sysmac Studio or an HMI. • Cycle the power supply. • Reset the Controller from the Sysmac Studio.
Minor fault level	These errors prevent part of the control operations in a certain function module in the Controller. The troubleshooting for minor fault level errors is the same as the processing for partial fault level errors.
Observations	These errors do not affect the control operations of the Controller. The observation notifies you of potential problems before they develop into a minor fault level error or worse.
Information	Events that are classified as information provide information that do not indicate errors.

You can change the event level for some events.

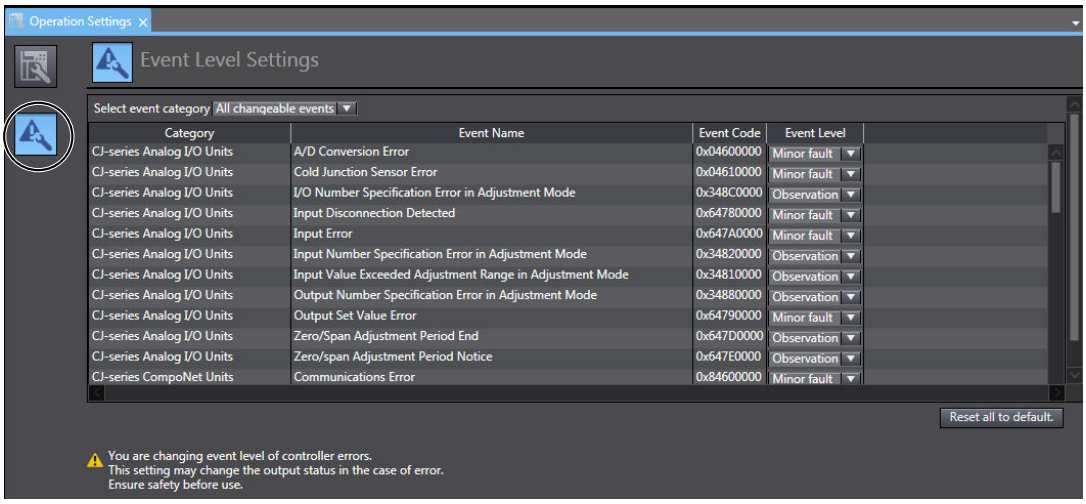
Procedure to Change an Event Level

1 Under **Configurations and Setup** - **Controller Setup** in the Sysmac Studio, double-click **Operation Settings**, or right-click and select **Edit** from the menu.
The **Basic Settings** Display is displayed on the Operation Settings Tab Page in the Edit Pane.



2 Click the **Event Level Settings** Button.

A list of the events for which you can change the event level is displayed.



3 Change the levels of the required events in the **Event Level** column.

Precautions for Correct Use

If you change an event level on the Sysmac Studio and download the event level setting to the Controller when the event already exists on the Controller, the event will be reset when the download is started. If the same event occurs again while the download is in progress, the Controller will operate according to the previous event level. If the same event occurs after the download is completed, the Controller will operate according to the new level.

Operation for Each Level

The operation that is performed when an error occurs depends on the error level of the Controller event.

Item		Level of event				
		Controller errors				Controller information
		Major fault level	Partial fault level	Minor fault level	Observation	Information
Definition		These errors are serious errors that prevent control operations for the entire Controller.	These errors prevent all of the control in a function module other than PLC Function Module.	Errors that prevent a portion of control in one of the function modules.	Errors that do not affect control.	Information level events are not errors, but information provided to the user in the event log.
Event examples		• Non-volatile Memory Data Corrupted (PLC Function)	• EtherNet/IP Processing Error (EtherNet/IP Function)	• Registered NX Unit Not Mounted (NX Bus Function)	• Packet Discarded Due to Full Reception Buffer (EtherNet/IP Function Module)	• Power Turned ON • Power Interrupted • Memory All Cleared
Front-panel indicators*1	UNIT PWR Indicator (green)	Lit.	Lit.	Lit.	Lit.	Lit.
	RUN (green)	Not lit.	Lit.	Lit.	Lit.	Lit.
	ERROR (red)	Lit.	Flashing (1-s intervals)	Flashing (1-s intervals)	Not lit.	Not lit.
Operation of Communication Control Unit	Outputs turned OFF	Yes	No	No	No	No
	Error reset	Not possible.	Depends on the nature of the error.	Depends on the nature of the error.	---	---
	Event logs	Recorded. (Some errors are not recorded.)	Recorded.	Recorded.	Recorded.	Recorded.

Item	Level of event				
	Controller errors				Controller information
	Major fault level	Partial fault level	Minor fault level	Observation	Information
Outputs from NX Units	Refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.	• Errors in NX Bus Function Module: Depends on the settings of the Unit • Errors in other function modules: Depends on the user program.	Depends on the user program.	Depends on the user program.	Depends on the user program.
Sysmac Studio display (when online)	The error status is automatically displayed in the Controller Status Pane. You can display detailed information in the Troubleshooting Dialog Box.			These items are not displayed on the error display of the Controller Status Pane.	

*1. If multiple Controller errors have occurred, the indicators show the error with the highest error level.

● Operation in the Function Module Where an Error Event Occurred

Function module	Level of current event			
	Major fault level	Partial fault level	Minor fault level	Observation
PLC Function Module	---	---	Operation continues.	
NX Bus Function Module	---	I/O refreshing for NX bus communications stops. (NX Unit operation depends on the NX Unit settings.)	Operation continues. If an NX Unit error occurs, operation depends on the Fail-soft Operation Setting of the NX bus function.	Operation continues.
EtherNet/IP Function Module	---	EtherNet/IP communications stop. (Online connections to the Sysmac Studio and communications connections with an HMI is not possible.)	Part of the EtherNet/IP communications stop. (Online connections to the Sysmac Studio and communications connections with an HMI is possible if the online connections or communications connection is not the cause of the error.)	EtherNet/IP communications continue.

Note Major fault level errors occur only in the PLC Function Module.

I/O Operation for Major Fault Level Controller Errors

The following table gives the operation of the Communication Control Unit and the I/O devices.

Unit	Communication Control Unit operation	Unit or slave operation
NX Unit mounted to the Communication Control Unit	• Input refreshing continues. • Updating the output values is stopped.	Depends on the settings for the NX Unit.
Devices connected with EtherNet/IP	• The variables and I/O memory addresses for input (consume) tags are not refreshed. • Operation depends on the settings of the tags sets for the output (produce) tags. • The CIP Safety routing is stopped.	Depends on the specifications of the connected devices.

*1. You can set whether to clear output or maintain the data from before the error occurred. Refer to *7-4-2 Setting Tag Data Links* on page 7-17 for details.

Event Code

Events that occur in a Controller have an event code.
When an event occurs, the Sysmac Studio or HMI will display the event code.
The event codes are 8-digit hexadecimal values.
The first digit of a Controller event represents its category. These categories are listed in the table below.

First digit of the code (hex)	Classification	Meaning
0	Hardware errors	An error caused by a hardware problem such as an internal part malfunction, contact failure, temperature error, undervoltage, overvoltage, or overcurrent.
1	Data errors	An error caused by incorrectly saved data or data corruption in the Controller.
2	Hardware setting errors	An error caused by incorrect handling of hardware settings (e.g., hardware switches) or restrictions (e.g., Unit assignment locations).
3	Configuration errors	An error caused by incorrect parameter values, parameters and hardware configurations that do not match, or configurations set by the user.
4	Software errors	An error caused by Controller software.
5	User software errors	An error that is caused by the user program. (For example, an input value to an instruction that is out of range.)
6	Observation errors	An error that was detected in monitoring operation that occurs due to user settings in the Controller. (For example, if the task period is exceeded or if a position outside of the motion range is detected.)
7	Control errors	An error caused by a control process. (For example, if the operating status does not meet the required conditions or if the timing is incorrect.)
8	Communications errors	An error caused by communications with an external device or host system.
9	Information	Events that are classified as information and provide information that do not indicate errors.

Exporting the Event Log

You can use the Sysmac Studio or an HMI to export the displayed event log to a CSV file.

15-1-4 Checking for Non-fatal Errors

Checking Methods

Use the following methods to check for non-fatal errors in the Communication Control Unit.

Checking method	What you can check
Checking the indicators	You can use the indicators to confirm the Controller error level and the error status of the EtherNet/IP Function Module.
Checking with the troubleshooting function of the Sysmac Studio	You can check for current Controller errors, a log of past Controller errors, error sources, error causes, and corrections.
Checking with the Troubleshooter of an HMI*1	You can check for current Controller errors, a log of past Controller errors, error sources, error causes, and corrections.
Checking the system-defined variables	You can check the current Controller error status for each function module.
Checking communications status with the Network Configurator	You can check the communications status (e.g., tag data link connection status) for each device on the EtherNet/IP network.

*1. To perform troubleshooting from an HMI, connect the HMI to the built-in EtherNet/IP port on the Communication Control Unit.

Checking the Indicators

● Checking the Level of a Controller Error

The following table shows the relationship between the Controller's indicators and the event level.

(○:Lit/●:Not lit/⊙:Flashing)

Indicators			Event level
UNIT PWR (green)	RUN (green)	ERROR (red)	
○	●	○	Major fault level
○	○	⊙ (1-s intervals).	Partial fault level
			Minor fault level
○	○	●	Observation

Checking with the Troubleshooting Function of Sysmac Studio

When an error occurs, you can connect the Sysmac Studio online to the Controller to check current Controller errors and the log of past Controller errors.

● Current Errors

Open the **Controller Error** Tab Page to check the current error's level, source, source details, event name, event code, username, occurrence number*1, details, attached information 1 to 4, action and correction.

Observation level errors are not displayed.

● Log of Past Errors

Open the **Controller Event Log** Tab Page to check the time, level, source, source details, event name, event code, username, occurrence number, details, attached information 1 to 4, action and correction of the past errors.

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on troubleshooting with the Sysmac Studio.

Checking with the Troubleshooter of an HMI

When an error occurs, if you can connect communications between an HMI and the Controller, you can check current Controller errors and the log of past Controller errors.
To perform troubleshooting from an HMI, connect the HMI to the built-in EtherNet/IP port on the Communication Control Unit.

● Current Errors

You can check the current error's event name, event code, level, source, source details, time, details, and attached information 1 to 4.
Also, observations are not displayed as errors.

● Log of Past Errors

You can check the time, level, source, source details, event name, event code, details, attached information 1 to 4 for past errors.

Refer to the relevant HMI manual for information on the HMI Troubleshooter.

Checking with System-Defined Variables

You can check the error status variables in the system-defined variables to determine the status of errors in a Controller.
You can read the Error Status variable from an external device by using communications.
Refer to the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for information on system-defined variables.

Checking Communications Status with the Network Configurator

You can use the Network Configurator to check the communications status (e.g., tag data link connection status) for each device on the EtherNet/IP network. Refer to *15-4 Checking Status with the Network Configurator* on page 15-241 for details.

15-1-5 Resetting Non-fatal Errors

Unless you reset an error, the Controller will retain the error status until you turn OFF the power supply to the Controller or reset the Controller.
To reset a Controller error, it is necessary to eliminate the cause of the error. The same error will occur again if you reset the error, but do not eliminate the cause of the error.

Precautions for Correct Use

Resetting an error is not the same as eliminating the cause of the error.
Always eliminate the cause of an error before you perform the procedure to reset the error.

Error Resetting Methods

Method	Operation	Errors that are reset	Description
Command from Sysmac Studio	Resetting Controller errors	Resetting all errors in the entire Controller	Reset the Controller errors from the Sysmac Studio's Troubleshooting Dialog Box.
		Resetting errors for individually specified NX Units	For NX Units connected to the NX bus of the Communication Control Unit, reset the Controller error individually from the Sysmac Studio's Troubleshooting Dialog Box.
	Downloading	Resetting all errors for a specific function module	After the causes of the Controller errors are removed, all Controller errors in the relevant function module are reset as a result. Errors are not reset when you download the Controller Configurations and Setup.
	Clear All Memory	Resetting all errors for all function modules	After the causes of the Controller errors are removed, all Controller errors in all function modules are reset as a result.
	Controller reset		After the causes of the Controller errors are removed, all Controller errors in all function modules are reset as a result.
Commands from an HMI*1	Resetting Controller errors	Resetting all errors in the entire Controller	Reset Controller errors from the Troubleshooter of an HMI. You can reset errors from an HMI that is not directly compatible with the NX-series Controller or another company's HMI if you use the HMI in combination with the reset error instruction for the function module in the user program.
Commands from a host computer	Resetting Controller errors with CIP messages	Resetting all errors for all function modules	Use a CIP message from a host computer to reset errors.
Cycling the Controller's power supply	---	Resets all errors.	After the causes of the Controller errors are removed, all Controller errors in all function modules are reset as a result.

*1. To reset errors from an HMI, connect the HMI to the built-in EtherNet/IP port on the Communication Control Unit.

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on clearing errors from the Sysmac Studio.

15-1-6 Errors Related to the EtherNet/IP Function Module

This section describes the errors that are related to the EtherNet/IP Function Module.

Classification

There are the following sources of errors in the EtherNet/IP Master Function Module.

Classification	Description
Communications port 1 errors	If an error is detected for EtherNet/IP communications port 1, the corresponding bit in the Communications Port1 Error status variable shows the error.
Communications port 2 errors	If an error is detected for EtherNet/IP communications port 2, the corresponding bit in the Communications Port2 Error status variable shows the error.
CIP communications 1 errors	If an error that is related to the tag data links or CIP message communications is detected for EtherNet/IP communications port 1, the corresponding bit in the CIP Communications1 Error status variable shows the error.*1
CIP communications 2 errors	If an error that is related to the tag data links or CIP message communications is detected for EtherNet/IP communications port 2, the corresponding bit in the CIP Communications2 Error status variable shows the error.*1
TCP application errors	If an error that is related to the FTP server, NTP, or SMNP client is detected, the corresponding bit in the TCP Application Communications Error status variable shows the error.

*1. Other Ethernet communications are not affected.

Event Source and Level

The following table gives sources and levels of the events that can occur in the EtherNet/IP Function Module.

Level	Source		
	Communications port	CIP communications	TCP application
Major fault	None	None	None
Partial fault	EtherNet/IP Processing Error	None	None
Minor fault	• Communications Controller Failure • MAC Address Error • IP Route Table Setting Error • Basic Ethernet Setting Error • IP Address Setting Error • DNS Setting Error • DNS Server Connection Error • IP Address Duplication Error • BOOTP Server Connection Error	• Identity Error • Tag Data Link Setting Error • Tag Name Resolution Error • Controller Insufficient Memory Warning • Tag Data Link Connection Failed • Tag Data Link Timeout • Tag Data Link Connection Timeout • Tag Data Link Equipment Total Allowable Bandwidth Exceeded	• FTP Server Setting Error • NTP Client Setting Error • SNMP Setting Error • NTP Server Connection Error
Observation	• Access Detected Outside Range of Variable • Packet Discarded Due to Full Reception Buffer • Link OFF Detected	None	None
Information	• Link Detected • Restarting Ethernet Port • IP Address Fixed • BOOTP Client Started	• Tag Data Link Download Started • Tag Data Link Download Finished • Tag Data Link Stopped • Tag Data Link Started • Tag Data Link All Run	• FTP Server Started • NTP Client Started • SNMP Started

15-1-7 Errors Related to Safety Control Units

Safety CPU Unit

The errors that can occur in the Safety CPU Unit and the operation that is performed for each are described in the following table.

Type	Overview	Operation
System error	Errors that occur in hardware self-diagnosis in the Safety CPU Unit	The Safety CPU Unit will stop. The Safety I/O Units will detect this and make the safety I/O data inactive (OFF).

Type	Overview	Operation
Communications errors	Errors that occur in safety process data communications with the FSoE slaves and the CIP Safety target devices	The Safety CPU Unit will continue operation. The relevant safety process data communications will stop. The Unit that detects the safety process data communications error will make the safety I/O data inactive (OFF).
Program execution error	Errors that occur in the safety function blocks in the Safety CPU Unit	The Safety CPU Unit will continue operation. Refer to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)* for the operation of function blocks in which errors occur.
Other errors	Errors other than those given above	The Safety CPU Unit will continue operation. Refer to the list of errors for details.

Events are recorded in the log when the Safety CPU Unit is accessed by the Sysmac Studio.

Type	Overview	Operation
User access log	The Safety CPU Unit was accessed by the Sysmac Studio.	The Safety CPU Unit will continue operation.

Safety I/O Units

The errors that can occur in the Safety I/O Units and the operation that is performed for each are described in the following table.

Type	Overview	Operation
System error	Errors that occur in hardware self-diagnosis in the Safety I/O Units	The Safety I/O Unit will stop.
Communications errors	Errors that occur in safety process data communications with the Safety CPU Units	The Safety I/O Unit will continue operation. The Safety I/O Unit will make the safety I/O data inactive (OFF).
Safety I/O errors	Errors that occur in safety I/O in the Safety I/O Units	The Safety I/O Unit will continue operation. Safety process data communications will continue. The safety I/O data will become inactive (OFF).
Other errors	Errors other than those given above	The Safety I/O Unit will continue operation. Refer to the list of errors for details.

Events are recorded in the log when the Safety I/O Unit is accessed by the Sysmac Studio.

Type	Overview	Operation
User access log	The Safety I/O Unit was accessed by the Sysmac Studio.	The Safety I/O Unit will continue operation.

15-1-8 Errors on CIP Safety Target Devices

You can check errors that have occurred on the CIP Safety target devices by using the following methods.

Checking method	What you can check
Checking the Indicators of the CIP Safety Target Device	Device status and error status, etc.
Checking with the CIP Safety Monitor Function of Sysmac Studio	• Device status • Connection status • Parameter monitor value • Event logs (for OMRON CIP Safety target devices only)

Checking the Indicators of the CIP Safety Target Device

Refer to the manuals for the corresponding CIP Safety target devices.

Checking with the CIP Safety Monitor Function of Sysmac Studio

By establishing online connection between Sysmac Studio and a Safety CPU Unit, you can check the device status, connection status, and parameter monitor values.
With OMRON CIP Safety target devices, you can also checked the event logs.

- Device status
  The device status can be checked.
- Connection status
  The connection status between the Safety CPU Unit and the CIP Safety target device can be checked.
- Parameter monitor value
  The supported parameters defined in the EDS file can be monitored.
- Event logs (for OMRON CIP Safety target devices only)
  Errors occurred in the past can be checked.

Refer to *15-2-6 Troubleshooting the CIP Safety Target Device Errors* on page 15-43 for details on the CIP Safety Monitor function of Sysmac Studio.

15-2 Error Troubleshooting Methods

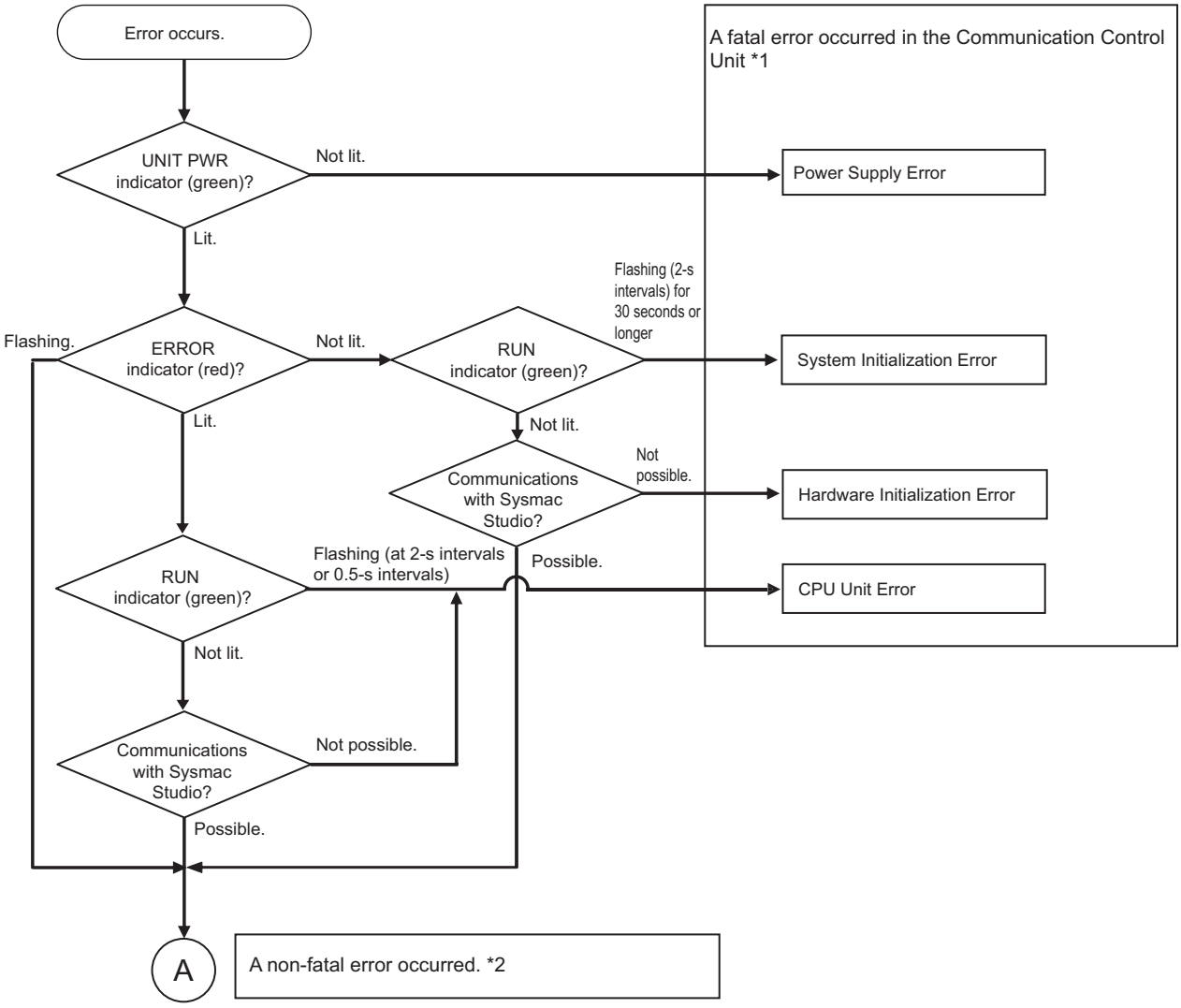
This section describes troubleshooting methods for specific errors.

15-2-1 Troubleshooting Flowcharts

This section provides basic error identification and troubleshooting flowcharts. Use them when an error occurs in the NX-series Controller.

Checking to See if the Communication Control Unit Is Operating

When an error occurs in the Communication Control Unit, use the following flowchart to determine whether the error is a "fatal error" or a "non-fatal error".
If a communications connection from the Sysmac Studio is not possible, perform *15-2-4 Troubleshooting When You Cannot Go Online from the Sysmac Studio* on page 15-31 before you assume that the error is a fatal error of the Communication Control Unit.



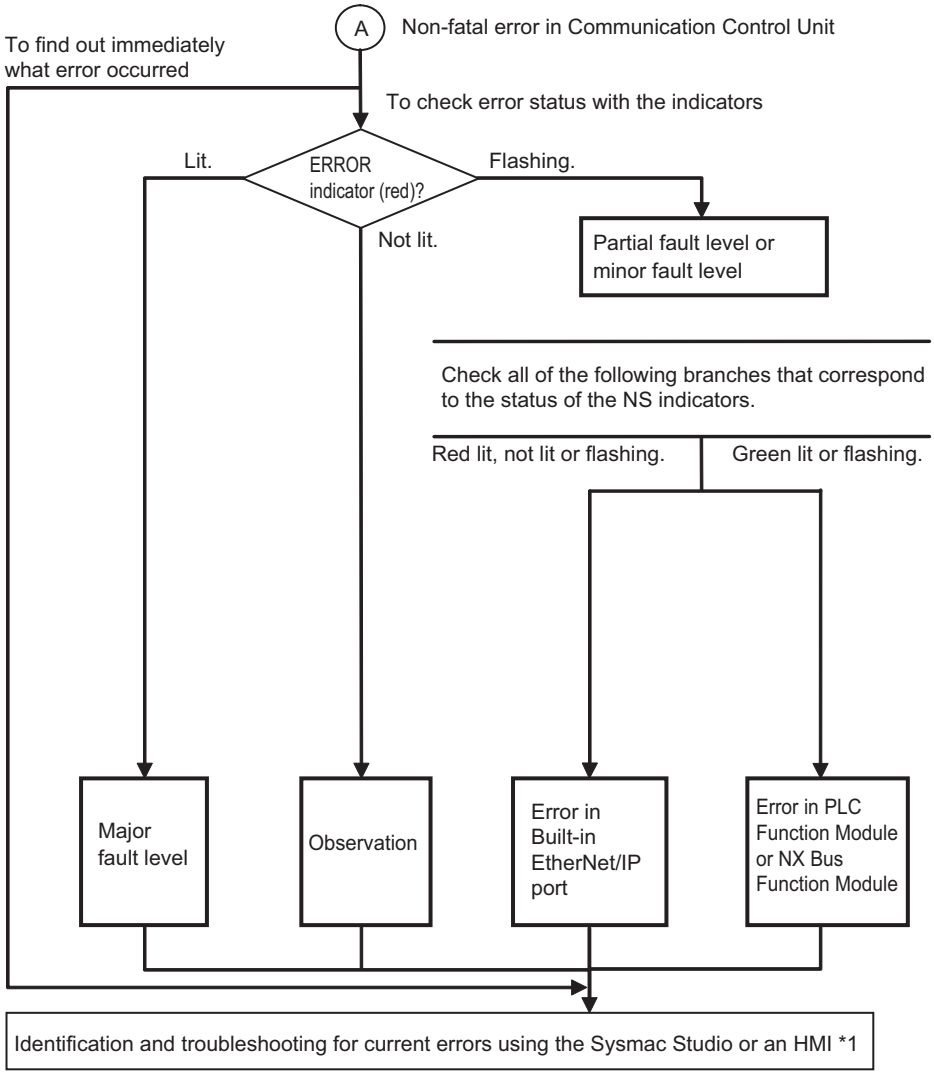
*1. Refer to *15-2-2 Troubleshooting Fatal Errors* on page 15-24.
*2. Refer to *Troubleshooting Flowchart for Non-fatal Errors* on page 15-24.

Troubleshooting Flowchart for Non-fatal Errors

For a non-fatal error, use the Sysmac Studio or an HMI to troubleshoot the error with the following flowchart.

You can use the indicators to check the following.

- Level
- Whether the error is in the EtherNet/IP port
- If the sources of the error is the EtherNet/IP port, whether you can restore normal status yourself



*1. Refer to *15-2-3 Troubleshooting Non-fatal Errors* on page 15-25.

15-2-2 Troubleshooting Fatal Errors

● Power Supply Error

Cause	Correction
Power is not being input.	Turn ON the power.
The voltage is outside of the allowable range for the power supply.	Check the Controller's power supply system, and correct it so that the voltage is within the allowable range.

● System Initialization Error

Cause	Correction
A conductive object has gotten inside.	If there is conductive material nearby, blow out the Communication Control Unit with air.
Noise	If the error did not result from the above causes, cycle the power to the Controller and see if that resets the error. If the error occurs frequently, check the FG and power supply lines to see if noise is entering on them. Implement noise countermeasures as required.

● Hardware Initialization Error

Cause	Correction
A conductive object has gotten inside.	If there is conductive material nearby, blow out the Communication Control Unit with air.
Noise	If the error did not result from the above causes, cycle the power to the Controller and see if that resets the error. If the error occurs frequently, check the FG and power supply lines to see if noise is entering on them. Implement noise countermeasures as required.
Communication Control Unit failure	If the error persists even after you make the above corrections, replace the Communication Control Unit.

● CPU Unit Error

Cause	Correction
A conductive object has gotten inside.	If there is conductive material nearby, blow out the Communication Control Unit with air.
Noise	If the error did not result from the above causes, cycle the power to the Controller and see if that resets the error. If the error occurs frequently, check the FG and power supply lines to see if noise is entering on them. Implement noise countermeasures as required.

15-2-3 Troubleshooting Non-fatal Errors

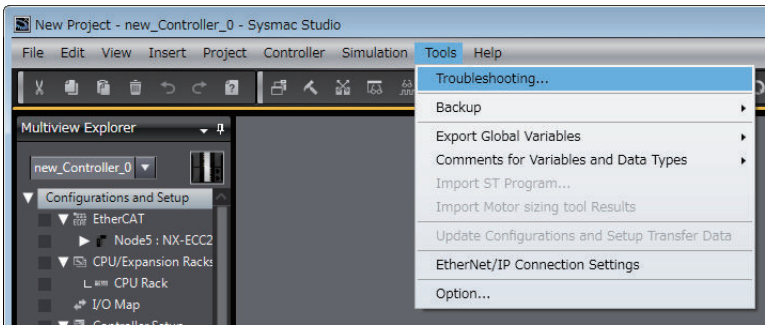
Identifying and Resetting Errors with the Sysmac Studio

Troubleshooting functions are provided by the Sysmac Studio.
You can use the troubleshooting functions to identify errors that occur in a Controller, and reset the errors.

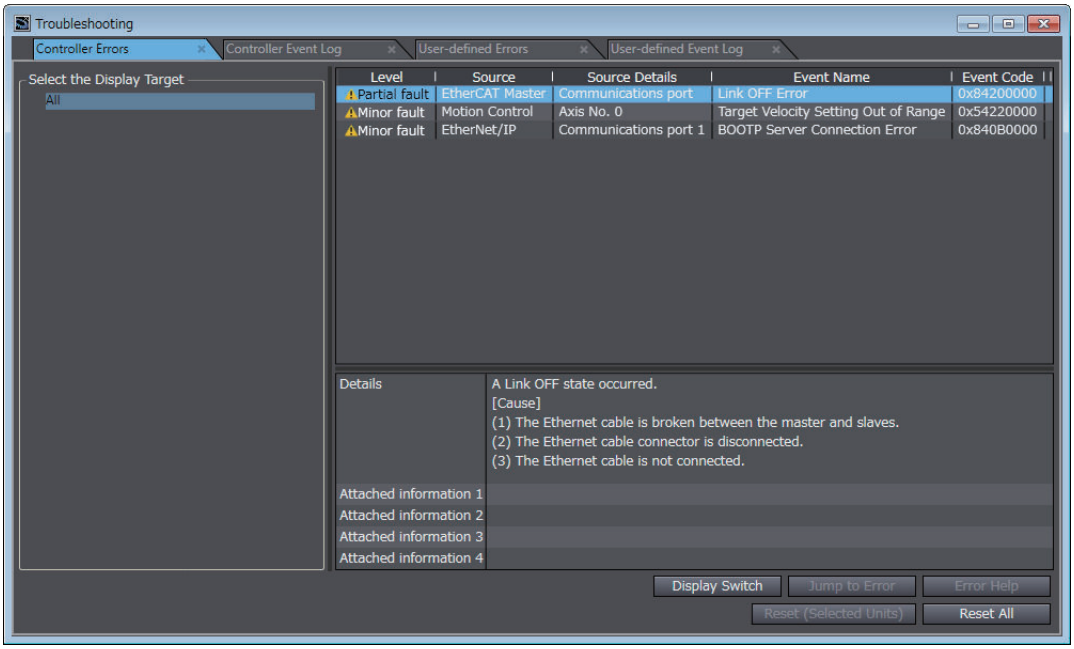
● Displaying Errors on the Sysmac Studio

If an error occurs while the Sysmac Studio is online with the Controller, the Sysmac Studio notifies the user of the error in the Controller Status Pane. From there, you can open the Troubleshooting and Event Logs Window to read detailed error information and troubleshooting methods.

Click the **Troubleshooting** Button in the toolbar, or select **Troubleshooting** from the **Tools** Menu.



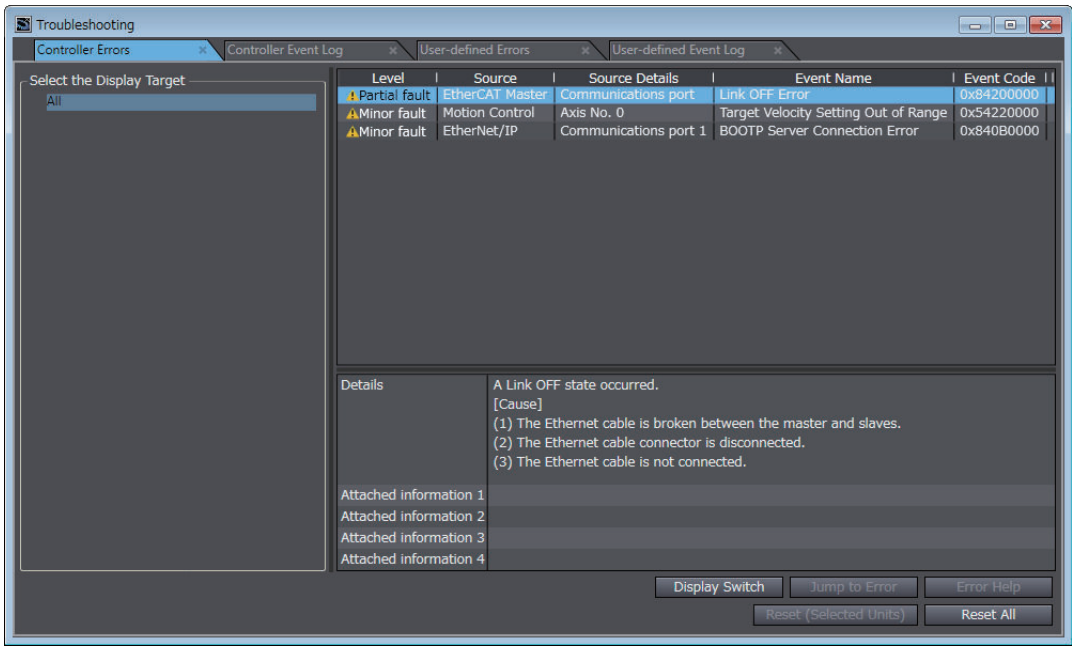
The Sysmac Studio automatically collects the Controller's error information, and opens the **Troubleshooting** Dialog Box.



● Checking Current Errors with the Sysmac Studio

You can click the **Controller Errors** Tab in the **Troubleshooting** Dialog Box to read information on current errors in the Controller.

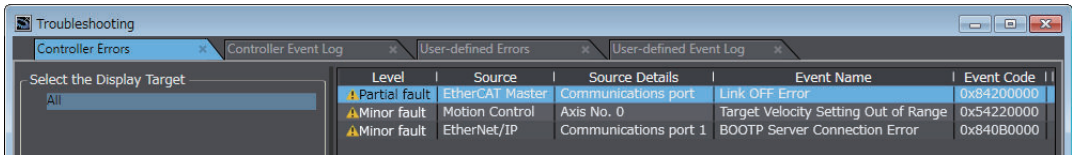
The **Controller Errors** Tab Page lists the current errors in order of their levels.



Displayed Item	Description
Level	This is the event level of the error.
Source and Source Details	This is the physical location and functional location of the error.
Event Name	Error name
Event Code	This is the code of the error.

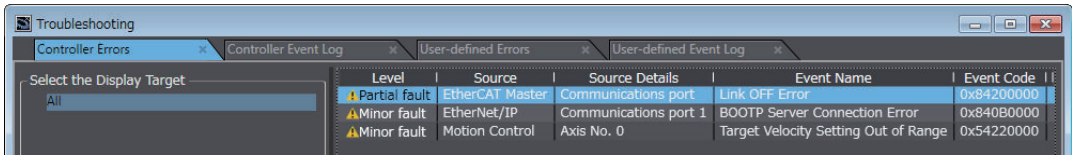
You can click the column headings in the Controller error list, such as the **Level** or **Source**, to reorder the table rows according to that heading.
For example, the following change occurs when you click the **Source** heading.

Before **Source** heading is clicked.



↓

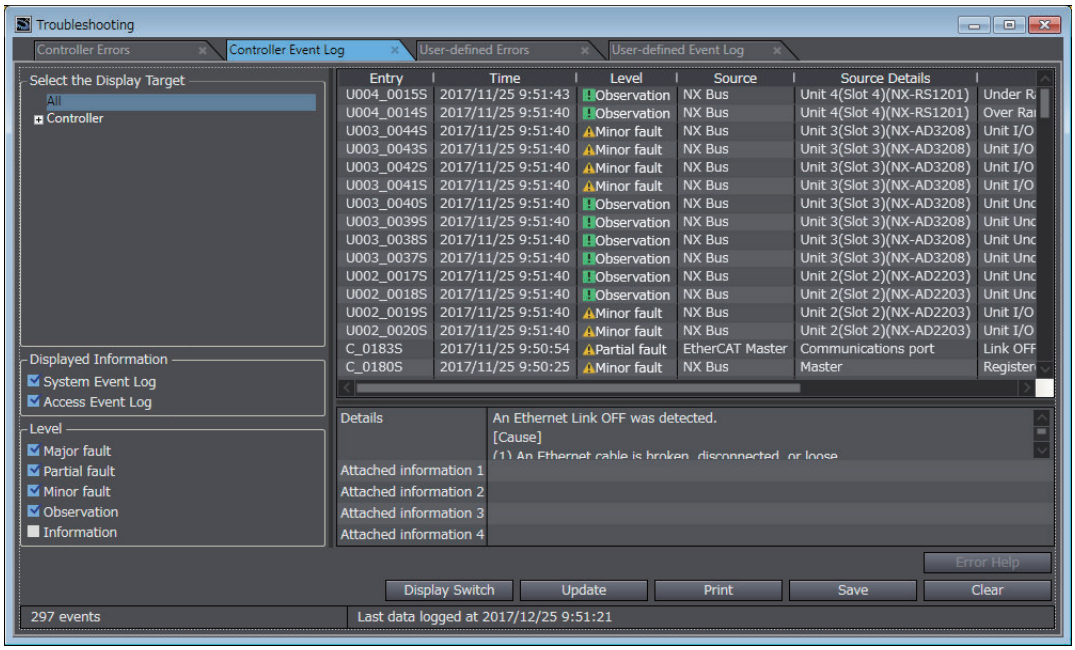
After **Source** heading is clicked.



● Displaying Event Logs with the Sysmac Studio

With Sysmac Studio, you can check a log of the Controller events that previously occurred on the **Controller Event Log** Tab Page.

You can select the event logs and levels to display in the Display Settings Area.
Information on the event that you specified are displayed in the Details Pane.



● Resetting Errors with the Sysmac Studio

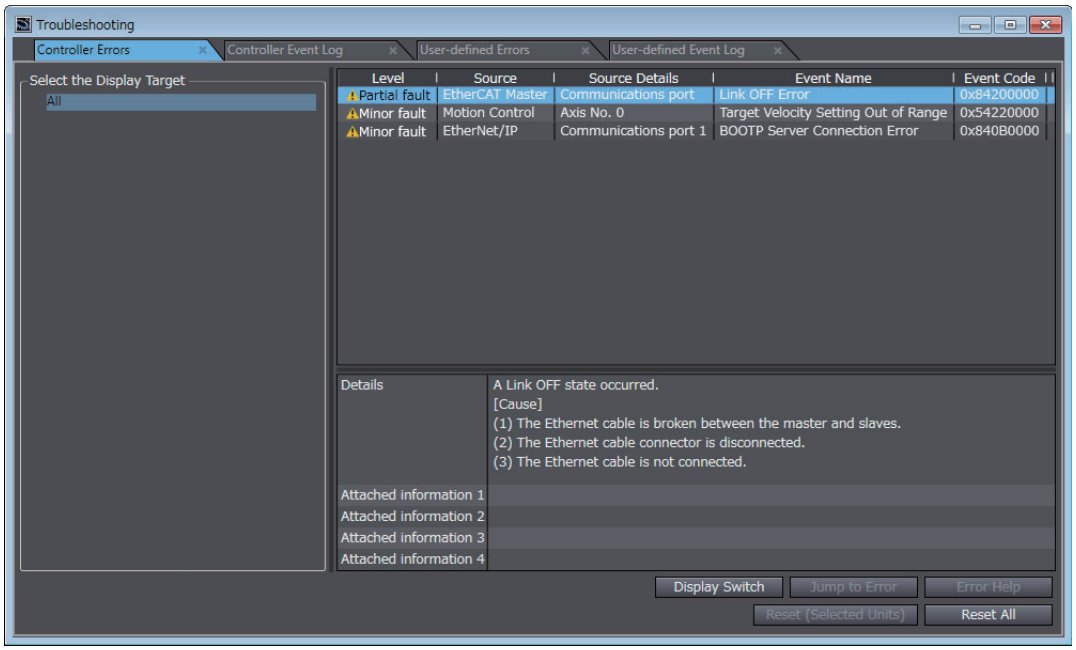
You can use the Sysmac Studio to reset errors that occur in a Controller.

Before you attempt to reset a Controller error, isolate and remove the cause of the error.

The Troubleshooting Dialog Box displays the cause, source, and corrections for the error. You can select any of the items from the error list to display the following information about that error.
Click the **Display Switch** Button to switch between displaying details and attached information and displaying actions and corrections.

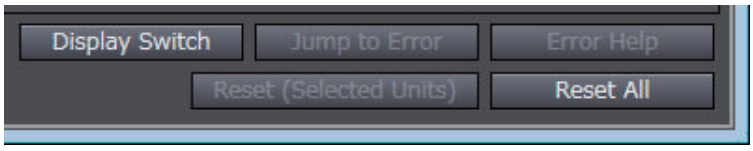
Displayed item	Description
Details	Detailed information on the error is displayed, such as the probable causes.
Attached information 1 through 4	Detailed information about the source of the error is displayed.
Action and Correction	Methods to correct the probable causes of the error are displayed.

After confirming the cause of the displayed error and the conditions in which it occurred, perform the displayed error corrections to eliminate the cause of the error.



To eliminate the cause of the error, first select the item to perform from the Action and Correction list.
When you select the appropriate step in the Action and Correction list, either the **Jump to Error** or **Error Help** Button is enabled, depending on the contents. In some cases, neither button will operate.
Click the enabled button, and proceed with the displayed troubleshooting steps.

After you complete all of the troubleshooting steps for the current errors, click the **Reset (Selected Units)** or **Reset All** Button to reset all of the current errors.
If the cause of the error is not removed, or if the power supply is not cycled or the Controller is not reset as required after resetting the error, the error will occur again.



Button	Description
Jump to Error	This button is enabled when the error correction involves a change in the Sysmac Studio settings. When you click the button, the Sysmac Studio will automatically switch to the Editing Pane.
Error Help	The correction methods or the attached information is displayed if it is not possible to jump to the settings display.
Reset (Selected Units)	This button resets the current errors in the selected Unit.
Reset All	This button resets all of the current errors, and reads errors again.

It is necessary to synchronize the data between the Sysmac Studio and the connected Communication Control Unit before you use the **Jump to Error** Button.

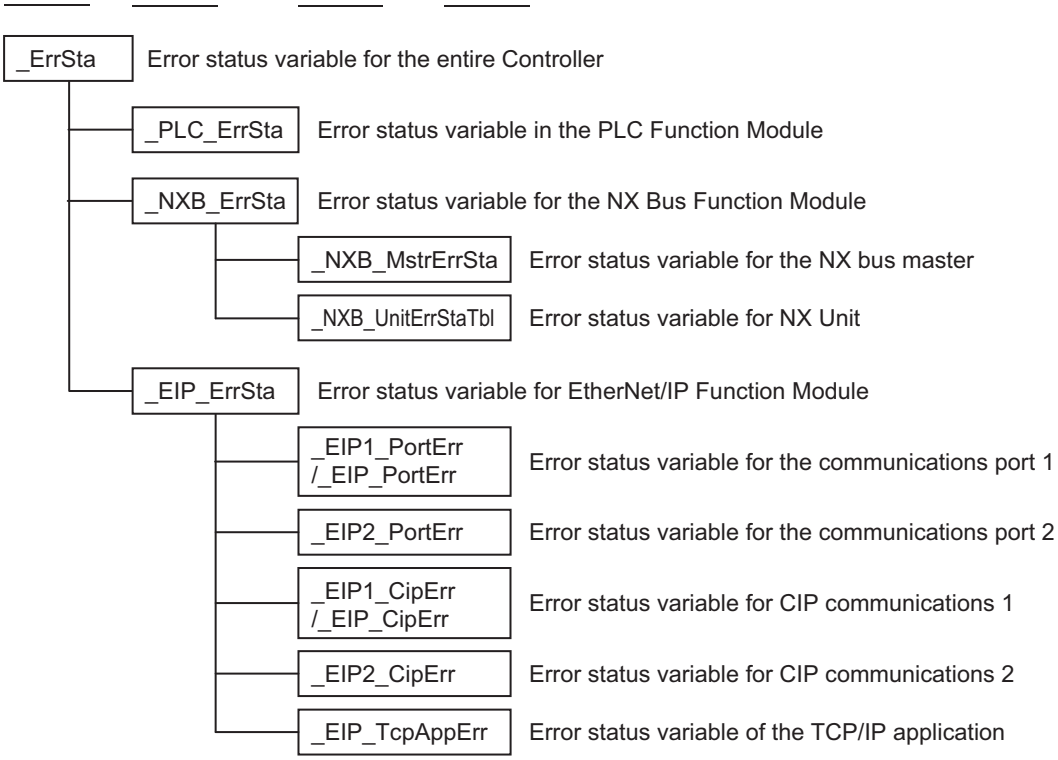
For details on synchronization, refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)*.

If you have enabled the verification of operation authority, it is necessary to confirm your authority before you can reset Controller errors.
The Operator, Maintainer, Designer, and Administrator have the authority to reset errors. For an Operator, however, verification is required each time.
Refer to the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for information on operation authority.

The Controller errors in all function modules are reset when you reset the Controller from the Sysmac Studio.
If the cause of the error is not removed, the error will occur again.

Checking for Errors with System-defined Variables

The system-defined variables include an Error Status variable, which shows the error status in a hierarchical structure. The system determines the error status of each level by logically ORing the error status information of the next lower level.
You can read the error status variables from an external device through communications.



15-2-4 Troubleshooting When You Cannot Go Online from the Sysmac Studio

The section describes the procedure to troubleshoot when you cannot go online with the Communication Control Unit from the Sysmac Studio.

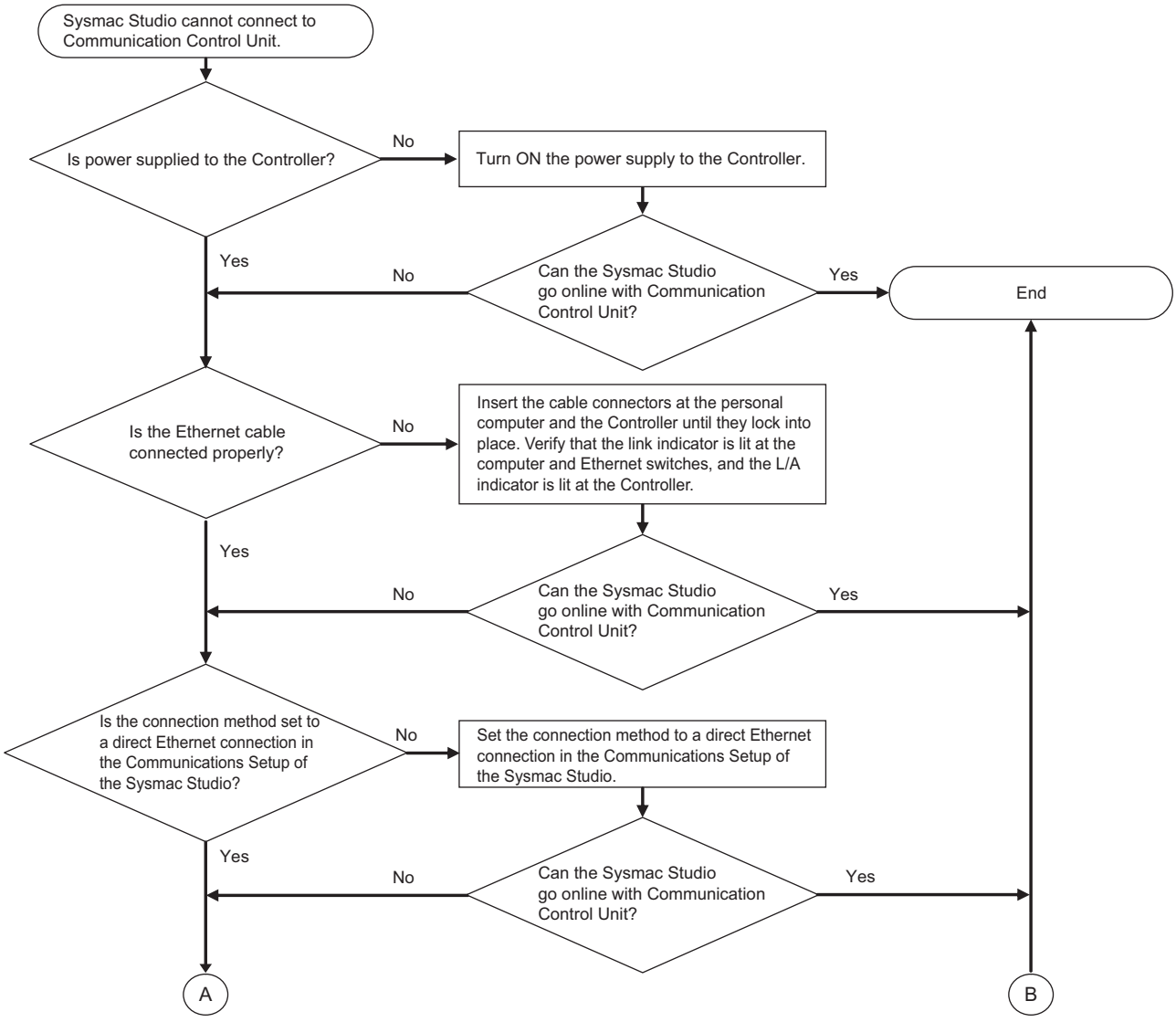
Causes and Correction When You Cannot Go Online from the Sysmac Studio

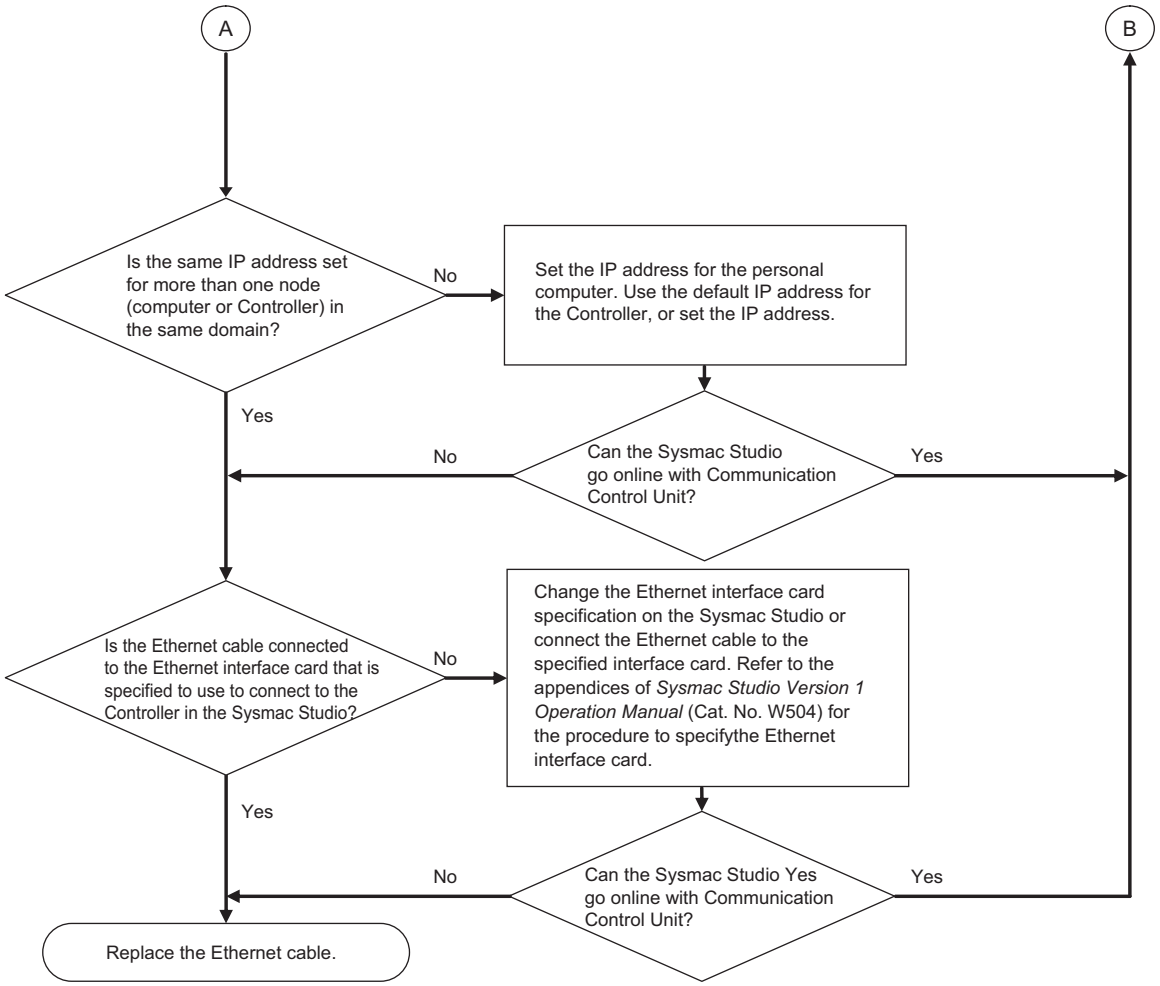
The following table lists the possible causes when you cannot go online with the Communication Control Unit from the Sysmac Studio.

Causes	Description	Correction
Incorrect settings or faulty communications path	There is a mistake in the settings that the Sysmac Studio uses to go online with the Communication Control Unit. Or, the communications path is faulty.	Refer to *Troubleshooting Incorrect Settings and Faulty Communications Path* on page 15-32.
Fatal error in the Communication Control Unit	A fatal error occurred in the Communication Control Unit.	Refer to *Checking to See if the Communication Control Unit Is Operating* on page 15-23.

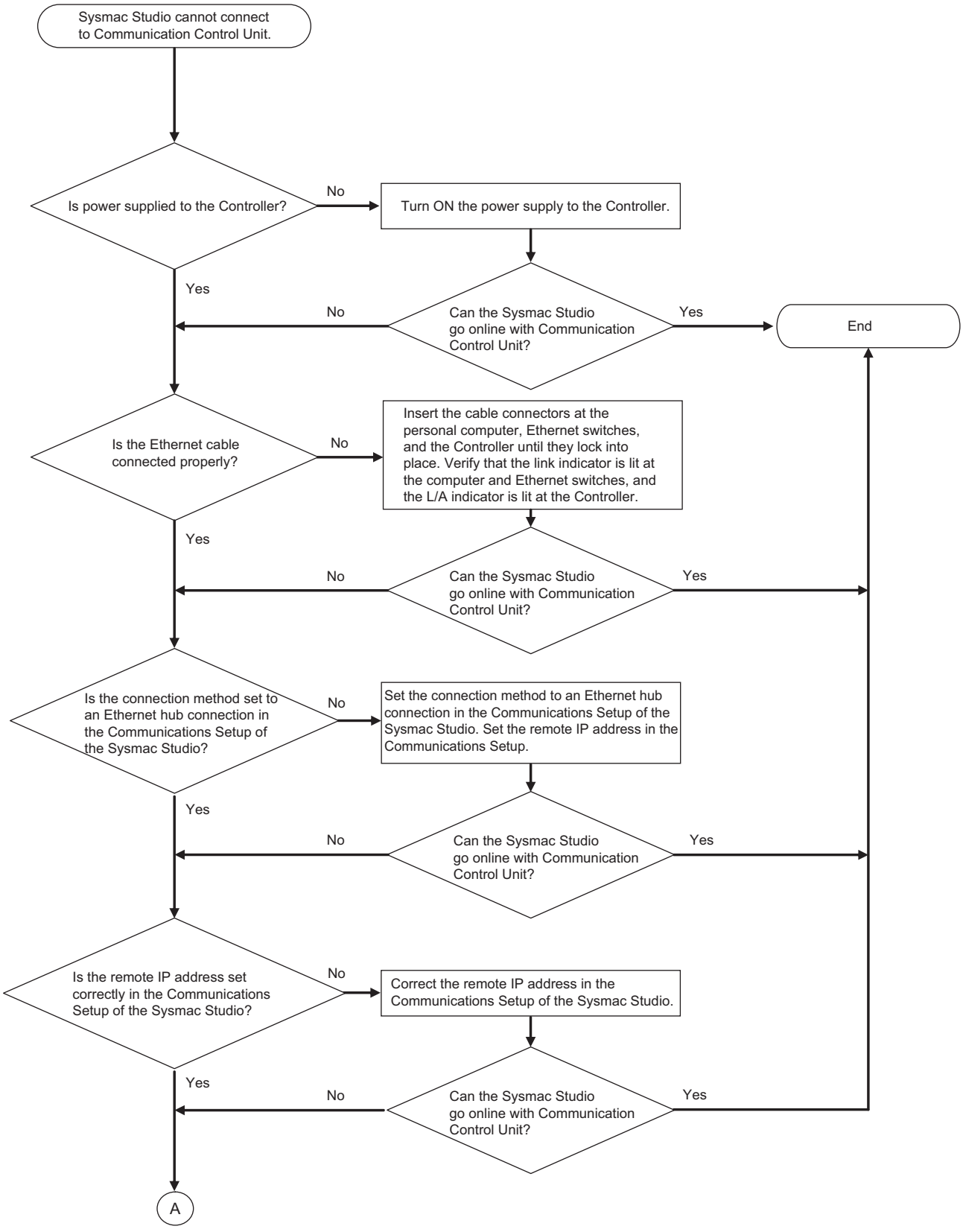
Troubleshooting Incorrect Settings and Faulty Communications Path

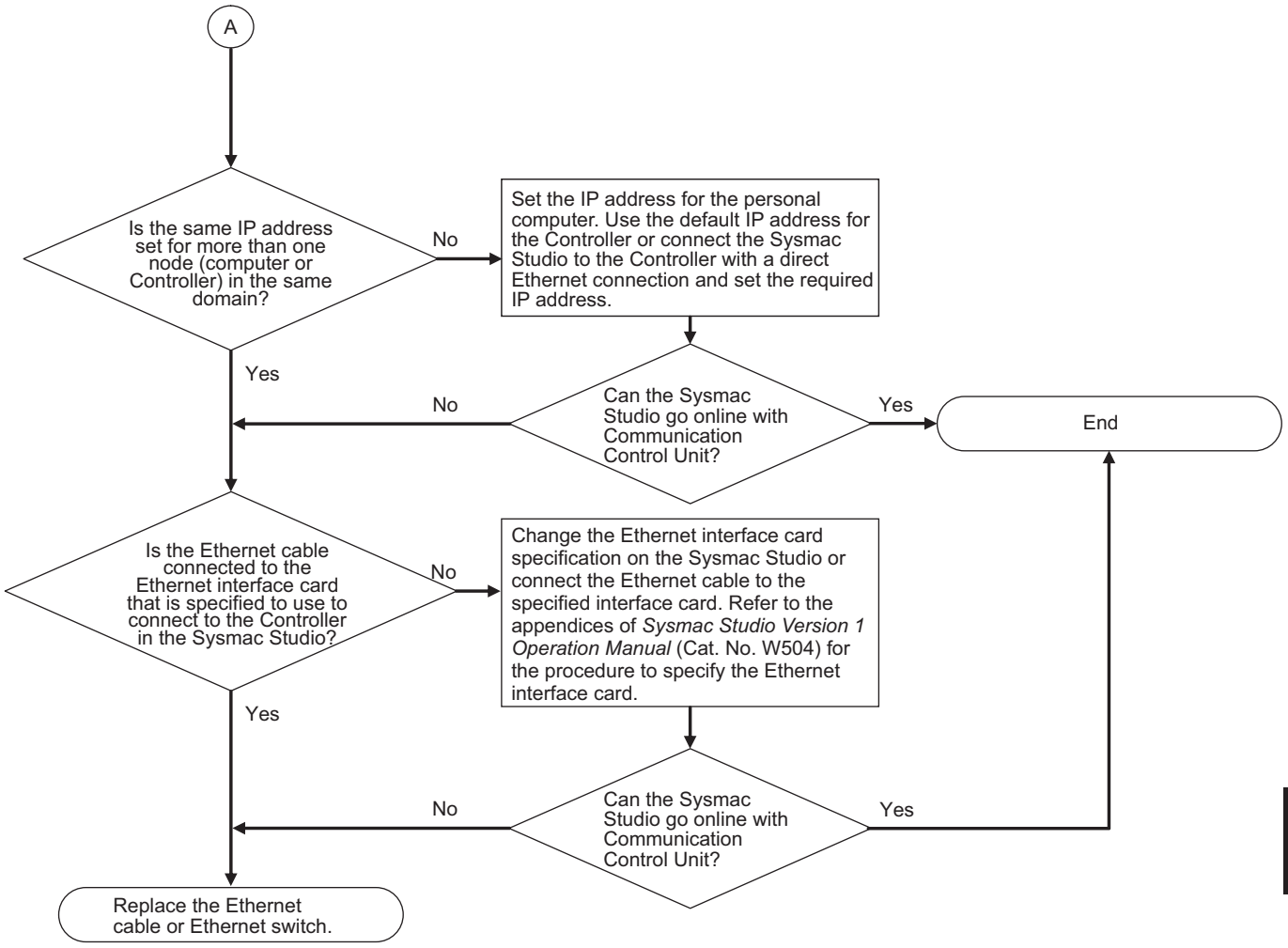
● Direct Connection with EtherNet/IP Port




A
B
Is the same IP address set for more than one node (computer or Controller) in the same domain?
No
Set the IP address for the personal computer. Use the default IP address for the Controller, or set the IP address.
Yes
No
Can the Sysmac Studio go online with Communication Control Unit?
Yes
Is the Ethernet cable connected to the Ethernet interface card that is specified to use to connect to the Controller in the Sysmac Studio?
No
Change the Ethernet interface card specification on the Sysmac Studio or connect the Ethernet cable to the specified interface card. Refer to the appendices of *Sysmac Studio Version 1 Operation Manual* (Cat. No. W504) for the procedure to specifythe Ethernet interface card.
Yes
No
Can the Sysmac Studio Yes go online with Communication Control Unit?
Yes
Replace the Ethernet cable.

● Ethernet Hub Connection





15-2-5 Troubleshooting Errors in the Safety Control Unit

Checking for Errors with the Indicators

You can use the [TS], [FS], [NS], and [P ERR] indicators on the Safety Control Unit to check the Safety Control Unit status and errors.
This section describes the meanings of errors that the [TS], [FS], [NS], and [P ERR] indicators show and the troubleshooting procedures for them.

● Troubleshooting the Main Errors in the Safety CPU Unit

TS Indicator	NS Indicator	FS Indicator	P ERR Indicator	Seven-segment Indicator	Cause	Corrective action
				---	---	Status is normal.
				[H3]	System Error	Refer to System Error (page 15-178).

TS Indicator	NS Indicator	FS Indicator	P ERR Indicator	Seven-segment Indicator	Cause	Corrective action
				[L3]	An error has occurred in the software.	Cycle the power supply. If the error reoccurs, contact your OMRON distributor.
	---	---	---	---	NX Bus I/O Communications Stopped	Refer to NX Bus I/O Communications Stopped (page 15-188).
 1-second interval	---	---	---	---	NX Unit I/O Communications Error	Refer to NX Unit I/O Communications Error (page 15-180).
 2-second interval	---	---	---	---	• Initializing • Downloading	Status is normal. Wait until processing is completed.
	---	---	---	---	No power is supplied by the Unit power supply.	Check the following items and make sure that power is correctly supplied from the Unit power supply. Checks Related to the Power Supply • Make sure that the power supply cable is wired properly. • Make sure that there are no breaks in the power supply cable. • Make sure that the power supply voltage is within the specified range. • Make sure that the power supply has enough capacity. • Make sure that the power supply has not failed. If you cannot resolve the problem after you check the above items and cycle the Slave Terminal power supply, the Unit may have a hardware failure. In that case, replace the Safety CPU Unit.
	---	---	---	---	• Waiting for initialization to start • Restarting the Unit	Status is normal. Wait until processing is completed.

TS Indicator	NS Indicator	FS Indicator	P ERR Indicator	Seven-segment Indicator	Cause	Corrective action
---	 1-second interval	---	---	[d6] --> [iP] --> Remote IP address	CIP Safety Originator Connection Not Established Error	Refer to CIP Safety Originator Connection Not Established Error (page 15-183).
---	 1-second interval	---	---	[dA] --> [iP] --> Remote IP address	CIP Safety Originator Connection Timeout	Refer to CIP Safety Originator Connection Timeout (page 15-185).
---	 1-second interval	---	---	[d5] --> [iP] --> Remote IP address	CIP Safety Target Does Not Exist	Refer to CIP Safety Target Does Not Exist (page 15-186).
---	 1-second interval	---	---	[A0] --> Assembly No. Upper Byte --> Assembly No. Lower Byte	CIP Safety Target Connection Timeout	Refer to CIP Safety Target Connection Timeout (page 15-187).
---	---	 1-second interval	---	---	FSoE Master Connection Not Established Error	Refer to FSoE Master Connection Not Established Error (page 15-179).
---	---	 1-second interval	---	---	FSoE Master Connection Timeout	Refer to FSoE Master Connection Timeout (page 15-182).

TS Indicator	NS Indicator	FS Indicator	P ERR Indicator	Seven-segment Indicator	Cause	Corrective action
---	---	 1-second interval	---	---	The safety connections are not established (including when they are currently being established).	Wait until processing is completed.
---	---	---		---	NX Bus Communications Settings Read Error	Refer to NX Bus Communications Settings Read Error (page 15-201).
---	---	---		---	Safety Application Data Read Error	Refer to Safety Application Data Read Error (page 15-201).
---	---	---		---	NX Bus Communications Settings and Safety Application Data Mismatch	Refer to NX Bus Communications Settings and Safety Application Data Mismatch (page 15-202).
---	---	---		---	Non-volatile Memory Access Error	Refer to Non-volatile Memory Access Error (page 15-203).
---	---	---		---	Division by Zero	Refer to Division by Zero (page 15-198).
---	---	---		---	Cast Error	Refer to Cast Error (page 15-199).
---	---	---		---	MUX Error	Refer to MUX Error (page 15-200).
---	---	---	 1-second interval	---	SF_Antivalent Error	Refer to SF_Antivalent Error (page 15-189).
---	---	---	 1-second interval	---	SF_EDM Error	Refer to SF_EDM Error (page 15-189).
---	---	---	 1-second interval	---	SF_EmergencyStop Error	Refer to SF_EmergencyStop Error (page 15-190).
---	---	---	 1-second interval	---	SF_EnableSwitch Error	Refer to SF_EnableSwitch Error (page 15-190).
---	---	---	 1-second interval	---	SF_Equivalent Error	Refer to SF_Equivalent Error (page 15-191).

TS Indicator	NS Indicator	FS Indicator	P ERR Indicator	Seven-segment Indicator	Cause	Corrective action
---	---	---	 1-second interval	---	SF_ESPE Error	Refer to SF_ESPE Error (page 15-191).
---	---	---	 1-second interval	---	SF_GuardLocking Error	Refer to SF_GuardLocking Error (page 15-192).
---	---	---	 1-second interval	---	SF_GuardMonitoring Error	Refer to SF_GuardMonitoring Error (page 15-192).
---	---	---	 1-second interval	---	SF_ModeSelector Error	Refer to SF_ModeSelector Error (page 15-193).
---	---	---	 1-second interval	---	SF_MutingPar Error	Refer to SF_MutingPar Error (page 15-193).
---	---	---	 1-second interval	---	SF_MutingPar_2Sensor Error	Refer to SF_MutingPar_2Sensor Error (page 15-194).
---	---	---	 1-second interval	---	SF_MutingSeq Error	Refer to SF_MutingSeq Error (page 15-194).
---	---	---	 1-second interval	---	SF_OutControl Error	Refer to SF_OutControl Error (page 15-195).
---	---	---	 1-second interval	---	SF_SafetyRequest Error	Refer to SF_SafetyRequest Error (page 15-195).
---	---	---	 1-second interval	---	SF_TestableSafetySensor Error	Refer to SF_TestableSafetySensor Error (page 15-196).
---	---	---	 1-second interval	---	SF_TwoHandControlTypeII Error	Refer to SF_TwoHandControlTypeII Error (page 15-196).

TS Indicator	NS Indicator	FS Indicator	P ERR Indicator	Seven-segment Indicator	Cause	Corrective action
---	---	---	 1-second interval	---	SF_TwoHandControlTypeIII Error	Refer to SF_TwoHandControlTypeIII Error (page 15-197).
---	---	---	---	---	NX Message Communications Error	Refer to NX Message Communications Error (page 15-204).
---	---	---	---	[E1] --> [01]	Safety Unit Restore Operation Failed to Start (SD Memory Card Access Failed)	Refer to Safety Unit Restore Operation Failed to Start (SD Memory Card Access Failed) (page 15-207).
---	---	---	---	[E1] --> [02]	Safety Unit Restore Operation Failed to Start (Safety Unit Restore File Read Error)	Refer to Safety Unit Restore Operation Failed to Start (Safety Unit Restore File Read Failure) (page 15-208).
---	---	---	---	[E1] --> [03]	Safety Unit Restore Operation Failed to Start (Model Mismatch)	Refer to Safety Unit Restore Operation Failed to Start (Model Mismatch) (page 15-209).
---	---	---	---	[E1] --> [04]	Safety Unit Restore Operation Failed to Start (Version Mismatch)	Refer to Safety Unit Restore Operation Failed to Start (Version Mismatch) (page 15-210).
---	---	---	---	[E1] --> [05]	Safety Unit Restore Operation Failed to Start (Node Name Mismatch)	Refer to Safety Unit Restore Operation Failed to Start (Node Name Mismatch) (page 15-211).
---	---	---	---	[E1] --> [06]	Safety Unit Restore Operation Failed to Start (Safety Password Mismatch)	Refer to Safety Unit Restore Operation Failed to Start (Safety Password Mismatch) (page 15-212).
---	---	---	---	[E1] --> [10]	Safety Unit Restore Operation Failed	Refer to Safety Unit Restore Operation Failed (page 15-213).
---	---	---	---	[E8]	Incorrect DIP Switch Setting	Refer to Incorrect DIP Switch Setting (page 15-203).

● Troubleshooting the Main Errors in the Safety I/O Units

TS Indicator	FS Indicator	Cause	Corrective action
		---	Status is normal.
	 1-second interval	Safety Process Data Communications Not Established - Incorrect Unit Parameter Error	Refer to Safety Process Data Communications Not Established - Incorrect Unit Parameter Error (page 15-220).

TS Indicator	FS Indicator	Cause	Corrective action
	 1-second interval	Safety Process Data Communications Not Established, Incorrect FSoE Slave Address Error	Refer to Safety Process Data Communications Not Established, Incorrect FSoE Slave Address Error (page 15-221).
	 1-second interval	Safety Process Data Communications Not Established, Incorrect Frame Error	Refer to Safety Process Data Communications Not Established, Incorrect Frame Error (page 15-222).
	 1-second interval	I/O Power Supply Voltage Error	Refer to I/O Power Supply Voltage Error (page 15-230).
	 1-second interval	Output Power Interrupt Circuit Error	Refer to Output Power Interrupt Circuit Error (page 15-231).
	 1-second interval	External Test Signal Failure at Safety Input	Refer to External Test Signal Failure at Safety Input (page 15-232).
	 1-second interval	Internal Circuit Error at Safety Input	Refer to Internal Circuit Error at Safety Input (page 15-227).
	 1-second interval	Discrepancy Error at Safety Input	Refer to Discrepancy Error at Safety Input (page 15-233).
	 1-second interval	Overload Detected at Test Output	Refer to Overload Detected at Test Output (page 15-234).
	 1-second interval	Stuck-at-high Detected at Test Output	Refer to Stuck-at-high Detected at Test Output (page 15-235).
	 1-second interval	Internal Circuit Error at Test Output	Refer to Internal Circuit Error at Test Output (page 15-228).
	 1-second interval	Short Circuit Detected at Safety Output	Refer to Short Circuit Detected at Safety Output (page 15-236).
	 1-second interval	Stuck-at-high Detected at Safety Output	Refer to Stuck-at-high Detected at Safety Output (page 15-237).
	 1-second interval	Internal Circuit Error at Safety Output	Refer to Internal Circuit Error at Safety Output (page 15-229).

TS Indicator	FS Indicator	Cause	Corrective action
 2-second interval	---	Initializing	Status is normal. Wait until processing is completed.
		System Error	Refer to System Error (page 15-219).
	 1-second interval	NX Bus I/O Communications Stopped	Refer to NX Bus I/O Communications Stopped (page 15-226).
 1-second interval	 1-second interval	NX Unit I/O Communications Error	Refer to NX Unit I/O Communications Error (page 15-223).
	---	No power is supplied by the Unit power supply.	Check the following items and make sure that power is correctly supplied from the Unit power supply. Checks Related to the Power Supply • Make sure that the power supply cable is wired properly. • Make sure that there are no breaks in the power supply cable. • Make sure that the power supply voltage is within the specified range. • Make sure that the power supply has enough capacity. • Make sure that the power supply has not failed. If you cannot resolve the problem after you check the above items and cycle the Slave Terminal power supply, the Unit may have a hardware failure. In that case, replace the Safety I/O Unit.
	---	• Waiting for initialization to start • Restarting the Unit	Status is normal. Wait until processing is completed.
---	 1-second interval	The safety connections are not established (including when they are currently being established).	Wait until processing is completed.
---	 1-second interval	Safety Process Data Communications Timeout	Refer to Safety Process Data Communications Timeout (page 15-225).
---	---	NX Message Communications Error	Refer to NX Message Communications Error (page 15-238).

● Checking for Errors with the Sysmac Studio

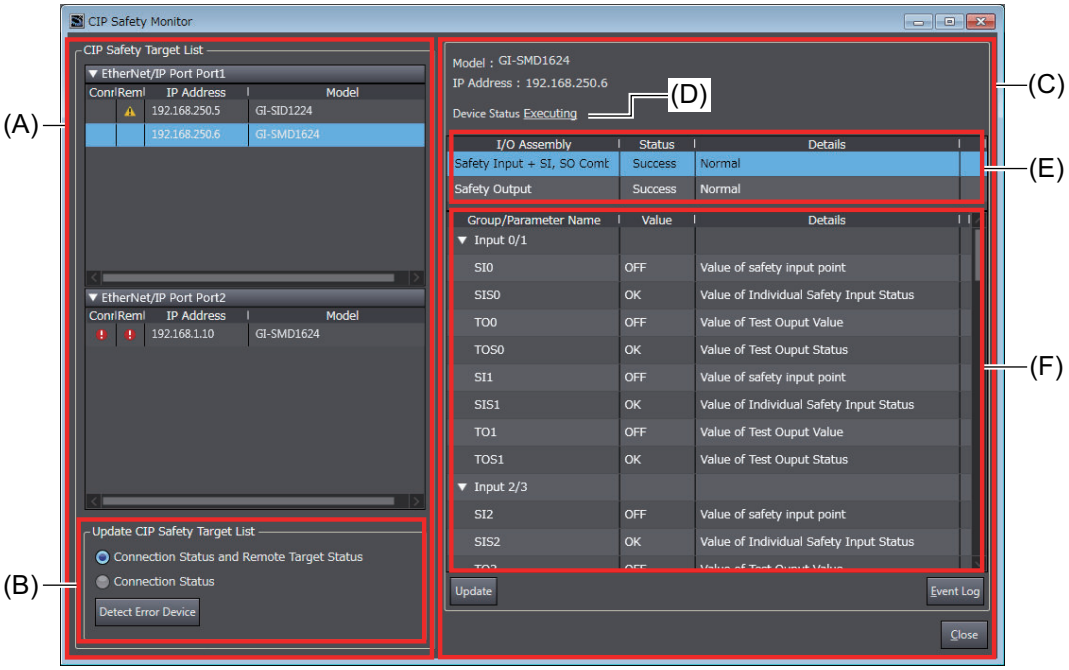
Refer to *15-2-3 Troubleshooting Non-fatal Errors* on page 15-25 for the procedure to check errors with the Sysmac Studio.

15-2-6 Troubleshooting the CIP Safety Target Device Errors

Sysmac Studio has the CIP Safety Monitor function.
The CIP Safety Monitor function allows you to monitor the device status of the CIP Safety target devices, the connection status with the Safety CPU Unit, as well as the parameter monitor values. If you are using an OMRON CIP Safety target device, the event logs can also be checked.

Part Names and Functions of the CIP Safety Monitor

This section describes the names and functions of the components on the CIP Safety Monitor.



Letter	Name	Function
(A)	CIP Safety Target List	A list of CIP Safety target devices registered in the Safety CPU Unit.
(B)	Update CIP Safety Target List	Updates the status of the CIP Safety Target List.
(C)	Monitor Information	Monitor information of the CIP Safety target device selected in the CIP Safety Target List.
(D)	Device Status	Device status information of the CIP Safety target device.
(E)	Connection Status	Status information of the connections configured for the CIP Safety target device.
(F)	Parameter Monitor Value	Information of monitored parameters of the CIP Safety target device.

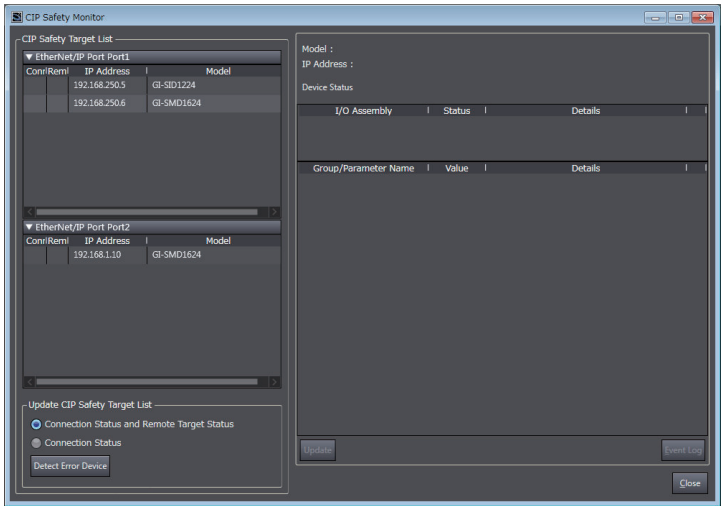
Starting the CIP Safety Monitor

Use the following procedure to start the CIP Safety Monitor.

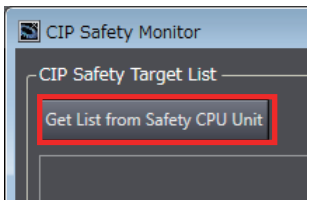
1 Select **Online** from the **Controller** Menu. Or, click the **Go Online** Button ( ) in the toolbar.

2 In the Multiview Explorer, select the Safety CPU Unit in the Controller Selection Box.

3 Select **Tools** - **CIP Safety Monitor**. Or, click the **CIP Safety Monitor** Button ( ) in the tool-bar.
If the information of the CIP Safety target device matches between the Safety CPU Unit and Sysmac Studio, **CIP Safety Target List** displays CIP Safety target devices that are registered in the Safety CPU Unit as shown below.



If the list of CIP Safety target devices does not appear, click the **Get List from Safety CPU Unit** Button. This will retrieve the connection settings from the Safety CPU Unit and display the device data in the list.



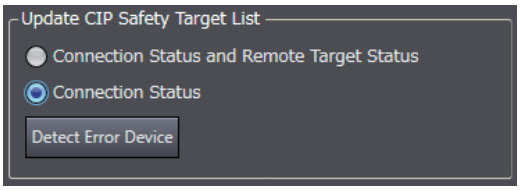
Precautions for Correct Use

The CIP Safety Monitor function is available only when the Safety CPU Unit is in the RUN or DEBUG mode.

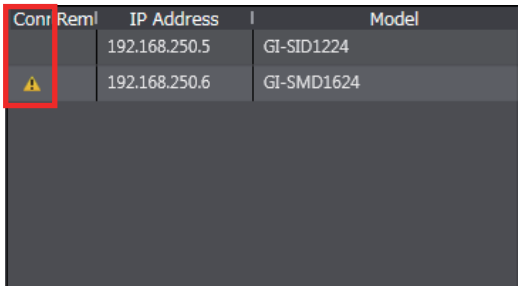
Identifying a Target Device with the Connection Error and its Cause

In the CIP Safety Target List, you can identify a CIP Safety target device with a connection error and its cause.

1 Go to **Update CIP Safety target list** and select the checkbox for **Connection Status**, and then click the **Detect Error Device** Button.

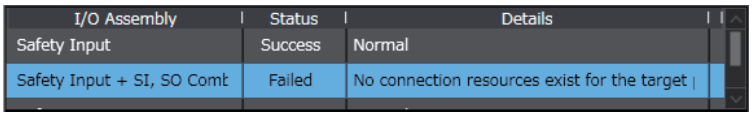


In the **CIP Safety Target List**, the display of the connection status error icon is refreshed.
If an error is present in the connection, an error icon is displayed.



Icon	Description
	A connection between the target device cannot be established.
	No target device is found.

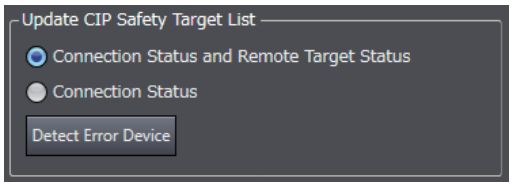
2 In the **CIP Safety Target List**, click a CIP Safety target device where a connection error is present.
The monitor information of the selected CIP Safety target is updated.
The connections configured to the CIP Safety target device and their statuses are displayed in the list. You will be able to identify the cause of the error by checking the details.



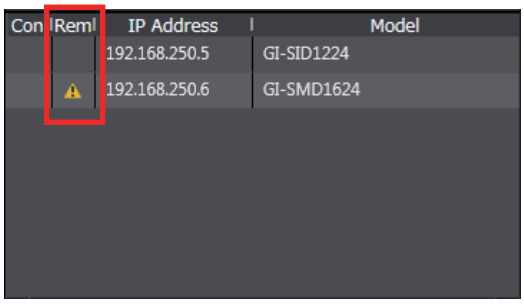
Checking the Parameter Monitor Values

The supported parameters defined in the EDS file can be monitored.
The cause of the error can be identified by monitoring the CIP Safety device-specific I/O data and status information.

1 Go to **Update CIP Safety target list** and select the checkbox for **Connection Status and Remote Target Status**, and then click the **Detect Error Device** Button.

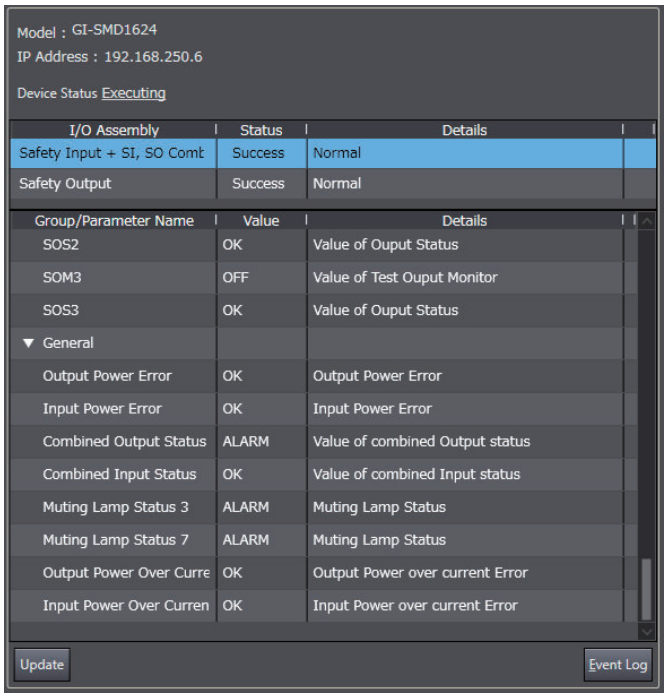


In the **CIP Safety Target List**, the display of the remote target status error icon is refreshed.
If an error is present in the device status of the CIP Safety target devices, an error icon is displayed.



Icon	Description
	An error is present in the device status.
	No target device is found.

2 In the **CIP Safety Target List**, click a CIP Safety target device where an error is present.
In the monitor information of the selected CIP Safety target, the device status, connection status, and parameter monitor values are displayed.



For details on the parameter monitor values, refer to the manuals for the corresponding CIP Safety target devices.

Precautions for Correct Use

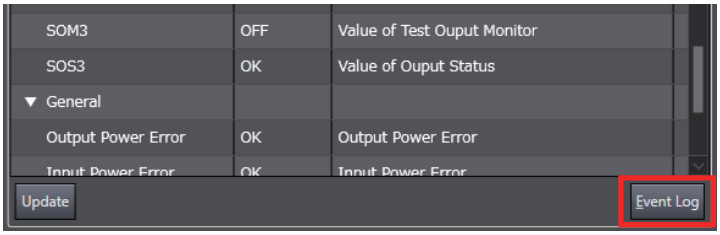
The monitor values of CIP Safety Monitor are not automatically refreshed. Click the Update Button to refresh the values.

Checking the Event Logs

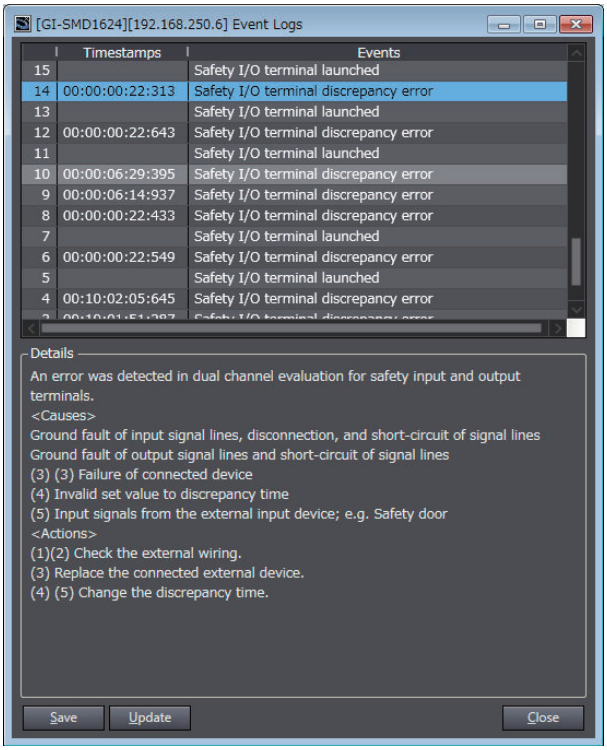
You can check event logs of the OMRON CIP Safety target devices.

1 Go to **CIP Safety Target List** and select an OMRON CIP Safety target device that you want to check the event logs.

2 Click the **Event Log** Button.



The event logs are displayed.



For details on the event logs, refer to the manuals for the corresponding CIP Safety target devices.

15-3 Error Descriptions and Corrections

This section lists all of the errors (events) that can occur.

15-3-1 Interpreting Tables

Within each source, errors (events) are given by functional classifications. Also, events that are not errors are given.

● Interpreting Description of Events When Using the Communication Control Unit

On the Sysmac Studio, the descriptions of events that are common to the Communication Control Unit and NJ/NX-series Controllers are displayed as the descriptions of NJ/NX-series Controller. Therefore, it is necessary to interpret the displayed contents when you use the Communication Control Unit. Observe the following precautions.

- In explanation of the errors, replace the term "CPU Unit" with the term "Communication Control Unit".
- Replace the NJ/NX-series manuals with the Communication Control Unit manuals in the Reference.
- The Communication Control Unit does not have the followings. Skip items that are related to them.
  a) Sequence controls (such as user programs and instructions)
  b) Online editing
  c) Motion Control Function Module (such as Axes and Cam Table)
  d) EtherCAT Function Module
  e) DB connection
  f) Robot
  g) USB
  h) Battery
- The unit version of the Communication Control Unit is different from the unit versions of the NJ/NX-series Controllers. If the description of an event contains information on the relevant unit versions, refer to the following correspondence table and read the relevant part.
  The following table shows the correspondence between the unit versions of the Communication Control Unit and the NJ/NX-series Controllers.

NJ/NX-series Controller	Communication Control Unit
Ver.1.17 or earlier	Not applicable
Ver.1.30	Ver.1.00
Ver.1.31	Ver.1.01

Interpreting Error Table

The contents of the error tables are described below.

Item	Description
Event code	The event code of the error in the NX-series Controller is given. The codes are given in eight hexadecimal digits. A version in parentheses in the Event code column is the unit version of a Communication Control Unit where an event with the relevant event code occurs. A model name in square brackets in the Event code column is the Communication Control Unit when the event occurs. The model name is not described if the event occurs in all Communication Control Unit.
Event name	The name of the error is given
Meaning	A short description of the error is given.
Assumed cause	The assumed cause of the error is given
Level	The level of influence on control is given. The abbreviations have the following meanings. Maj: Major fault level Prt: Partial fault level Min: Minor fault level Obs: Observation Info: Information The symbols have the following meanings. ○: Event levels that are defined by the system. ⊙: Event levels that can be changed by the user. *1
Reference	The catalog number of the manual that provides details on the event is given. The manual name that corresponds to the manual number is given before each error table.

*1. This symbol appears only for events for which the user can change the event level.

Interpreting Error Descriptions

The items that are used to describe individual errors (events) are described in the following copy of an error table.

<table>
<tr><td>Event name</td><td colspan="3">Gives the name of the error.</td><td>Event code</td><td colspan="2">Gives the code of the error.</td></tr>
<tr><td>Meaning</td><td colspan="6">Gives a short description of the error.</td></tr>
<tr><td>Source</td><td colspan="2">Gives the source of the error.</td><td>Source details</td><td>Gives details on the source of the error.</td><td>Detection timing</td><td>Tells when the error is detected.</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Tells the level of influence on control. *1</td><td>Recovery</td><td>Gives the method to return to normal state after eliminating the cause of the error.</td><td>Log category</td><td>Tells which log the error is saved in. *2</td></tr>
<tr><td>Effects</td><td>User program</td><td>Tells what will happen to execution of the user program. *3</td><td>Operation</td><td colspan="3">Provides special information on the operation that results from the error.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="6">Lists the variable names, data types, and meanings for system-defined variables that provide direct error notification, that are directly affected by the error, or that contain settings that cause the error. *4</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="6">Lists the possible causes, corrections, and preventive measures for the error.</td></tr>
<tr><td>Attached information</td><td colspan="6">This is the attached information that is displayed by the Sysmac Studio.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">Provides precautions, restrictions, and supplemental information. If the user can set the event level, the event levels that can be set, the recovery method, operational information, and other information is also provided.</td></tr>
</table>

*1. One of the following:
Major fault: Major fault level
Partial fault: Partial fault level
Minor fault: Minor fault level
Observation
Information

*2. One of the following:
System: System event log
Access: Access event log

*3. One of the following:
Continues: Execution of the user program will continue.
Stops: Execution of the user program stops.
Starts: Execution of the user program starts.

*4. Device variables are also contained in this section.
The differences between system-defined variables and device variables are as follows:
System-defined variable: The variable name starts with an underbar (_).
Device variable: The variable name stars with a character other than an underbar (_).

15-3-2 Communication Control Unit Error

The section provides tables of the errors (events) that can occur in the Communication Control Unit. They are divided into the following functional classifications for each function module.

Function module	Functional classification
PLC Function Module	Self-diagnosis
	Controller operation
NX Bus Function Module	NX Bus
EtherNet/IP Function Module	Built-in EtherNet/IP Port on CPU Unit

PLC Function Module Error Table

● Errors for Self Diagnosis

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
00090000 hex	DIP Switch Setting Error	An error was detected in the DIP switch setting.	• There is an error in the DIP switch setting.	○					page 15-74
000D0000 hex	Internal Bus Check Error	A fatal error was detected on the internal bus.	• A conductive material has gotten inside. • Noise • The CPU Unit has failed.	○					page 15-75
000E0000 hex	Non-volatile Memory Life Exceeded	The specified number of deletions for non-volatile memory was exceeded. Or, the number of bad blocks in memory exceeded the specified value.	• Non-volatile memory life expired.	○					page 15-76
00130000 hex	Main Memory Check Error	An error was detected in the memory check of the main memory in the CPU Unit.	• A conductive material has gotten inside. • Noise • There is a soft error. • The CPU Unit has failed.	○					page 15-77
10010000 hex	Non-volatile Memory Restored or Formatted	An error was detected in the non-volatile memory check and file system recovery or formatting was executed. Previous files may have been deleted.	• The Controller power supply was turned OFF while the BUSY indicator was lit. • The power supply to the Controller was interrupted momentarily while the BUSY indicator was lit.	○					page 15-78

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10020000 hex	Non-volatile Memory Data Corrupted	A file that must be in non-volatile memory is missing or corrupted.	• The Controller power supply was turned OFF while the BUSY indicator was lit. • The power supply to the Controller was interrupted momentarily while the BUSY indicator was lit. • The CPU Unit has failed.	○					page 15-79
10080000 hex	Main Memory Check Error	An error was detected in the memory check of the main memory in the CPU Unit.	• A conductive material has gotten inside. • Noise • There is a soft error. • The CPU Unit has failed.	○					page 15-80
100B0000 hex	Non-volatile Memory Data Corrupted	A file that must be in non-volatile memory is missing or corrupted.	• The Controller power supply was turned OFF while the BUSY indicator was lit. • The power supply to the Controller was interrupted momentarily while the BUSY indicator was lit. • The CPU Unit has failed.	○					page 15-81
100C0000 hex	Event Level Setting Error	The settings in the event level setting file are not correct.	• The event level settings are not correct because the power supply to the Controller was interrupted or communications with the Sysmac Studio were disconnected during a download of the event level settings. • The event level settings are not correct because the power supply to the Controller was interrupted during a Clear All Memory operation. • Non-volatile memory failed.	○					page 15-82
100F0000 hex	Present Values of Retained Variables Restoration Error	The present values of retained variables could not be restored at startup and the values were initialized.	• An error occurred in the software. • Backup memory failure	○					page 15-83
10100000 hex	Present Values of Retained Variables Not Saved	The process of saving the current value of the retained variable during power interruptions could not be performed because an error occurred in the software.	• An error occurred in the software.	○					page 15-84
40020000 hex	PLC System Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.	○					page 15-85

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
40030000 hex	PLC System Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.	○					page 15-85
40040000 hex	PLC System Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.	○					page 15-86
40050000 hex	PLC System Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.	○					page 15-86
00070000 hex	Real-Time Clock Stopped	The oscillation of the real-time clock stopped. The real-time clock is set to an illegal time.	• The battery voltage is low. • The battery connector has come loose. • The Battery is missing.			○	⊙		page 15-87
00080000 hex	Real-Time Clock Failed	The real-time clock in the CPU Unit failed.	• The CPU Unit clock has failed.			○			page 15-87
000F0000 hex	SD Memory Card Invalid Type	The current SD Memory Card is not supported.	• An SD Memory Card that is not supported was inserted into the CPU Unit.				○		page 15-88
00100000 hex	SD Memory Card Life Exceeded	The specified number of deletions for the SD Memory Card was exceeded. Or, the number of bad blocks exceeded the specified value.	• The service life of the SD Memory Card was exceeded.			⊙	○		page 15-88
10030000 hex	SD Memory Card Invalid Format	The file format of the SD Memory Card is not FAT16 or FAT32.	• The file format of the SD Memory Card inserted in the CPU Unit is not FAT16 or FAT32.				○		page 15-89
10040000 hex	SD Memory Card Restored or Formatted	An error was detected during the file system check and the file system was restored. Files may have been deleted.	• The Controller power supply was turned OFF while the SD BUSY indicator was lit. • The power supply to the Controller was interrupted momentarily while the SD BUSY indicator was lit. • The SD Memory Card was removed while the SD PWR indicator was lit. • The SD Memory Card is damaged.			⊙	○		page 15-90

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10060000 hex	SD Memory Card Data Corrupted	A file that must be in the SD Memory Card is missing or corrupted.	• The Controller power supply was turned OFF while the SD BUSY indicator was lit. • The power supply to the Controller was interrupted momentarily while the SD BUSY indicator was lit. • The SD Memory Card was removed while the SD PWR indicator was lit. • The SD Memory Card is damaged.			⊙	○		page 15-91
10070000 hex	SD Memory Card Access Power OFF Error	The power supply to the Controller was interrupted during access to the SD Memory Card.	• The Controller power supply was turned OFF while the SD BUSY indicator was lit. • The power supply to the Controller was interrupted momentarily while the SD BUSY indicator was lit.				○		page 15-92
10130000 hex	PLC System Information	This event provides internal information from the PLC Function Module.	• This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.				○		page 15-92
10310000 hex	Incorrect SD Memory Card Removal	SD Memory Card removal processing failed.	• The SD Memory Card was removed while the SD PWR indicator was lit.				○		page 15-93

● Errors Related to Controller Operation

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10200000 hex	User Program/ Controller Configurations and Setup Transfer Error	The user program or Controller Configurations and Setup were not transferred correctly.	• The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during a download of the user program or the Controller Configurations and Setup. • The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during online editing. • The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during a Clear All Memory operation. • The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during a restore operation. • Non-volatile memory failed.	○					page 15-94
10250000 hex	Illegal User Program/ Controller Configurations and Setup	The upper limit of the usable memory was exceeded or the user program or Controller Configurations and Setup is corrupted.	• The upper limit of the data size was exceeded. • The main memory capacity was exceeded. • Non-volatile memory is deteriorating or has failed.	○					page 15-95
40110000 hex	PLC Function Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.	○					page 15-96
44420000 hex	PLC Function Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.	○					page 15-96
40120000 hex	PLC Function Processing Error	A fatal error was detected in the PLC Function Module.	• An error occurred in the software.		○				page 15-97
40130000 hex	PLC Function Processing Error	A fatal error was detected in part of the PLC Function Module.	• An error occurred in the software.			○			page 15-97
10230000 hex	Event Log Save Error	Saving the event log failed.	• Data in the event log area are invalid.				○		page 15-98

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10290000 hex	Backup Failed to Start	An error was detected in pre-execution checks for a backup operation.	• An SD Memory Card is not inserted. • The SD Memory Card type is not correct. • The format of the SD Memory Card is not correct. • The SD Memory Card is write protected. • The **Prohibiting backing up data to the SD Memory Card** parameter is set to **prohibit** backing up data to an SD Memory Card. • Another backup operation is in progress. • Synchronization, online editing, or the Clear All Memory operation is in progress. • The backup was canceled by the user. • The online connection with the Sysmac Studio was disconnected. • The SD Memory Card is damaged. • An unexpected error has occurred.				○		page 15-99

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
102A0000 hex	Backup Failed	The backup operation ended in an error.	• The capacity of the SD Memory Card is insufficient. • It was not possible to save the data that was specified for backup. • The SD Memory Card was removed during a backup operation. • Failed to back up Unit or slave. • The backup was canceled by the user. • Execution of the Save Cam Table instruction or changing the CPU Unit name is in progress. • The online connection with the Sysmac Studio was disconnected. • It was not possible to save the data that was specified for backup to the computer. • The SD Memory Card is damaged. • An unexpected error has occurred. Also check the following when you use the Robot Integrated CPU Unit. • The SD Memory Card format is invalid • The SD Memory Card is write protected. • The /D folder, which is the data to be backed up, does not exist on the SD Memory Card.				○		page 15-101

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
102B0000 hex	Restore Operation Failed to Start	An error was detected in pre-execution checks for a restore operation.	• An SD Memory Card is not inserted. • The SD Memory Card type is not correct. • The format of the SD Memory Card is not correct. • There are no backup files on the SD Memory Card. • Either the backup files on the SD Memory Card are corrupted or required data is not in the backup files on the SD Memory Card. • The unit version of the CPU Unit to which to restore the files is older than the unit version of the backup files on the SD Memory Card. • The model of the CPU Unit to which to restore the files is not the same as the model of the CPU Unit of the backup files on the SD Memory Card. • Recovery was executed for the SD Memory Card. • The CPU Unit is write-protected. • The settings in the restore command file (RestoreCommand.ini) are not correct. • A backup operation is in progress. • Synchronization, online editing, or the Clear All Memory operation is in progress. • The online connection with the Sysmac Studio was disconnected. • Reading the data for restoration failed because the SD Memory Card is faulty or not formatted correctly. • The SD Memory Card is damaged. • The database connection service version of the CPU Unit to which to restore the files is older than the database connection service version of the backup files on the SD Memory Card.				○		page 15-103

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
			• The robot version of the CPU Unit to which to restore the files is older than the robot version of the backup files on the SD Memory Card. • The CPU Unit failed to process the power OFF during the last power interruption. • An unexpected error has occurred. Check the followings for specification with system-defined variables. • Restore by system-defined variable is set to Do not use in the Controller Setup. • Password of Restore by system-defined variable in the Controller Setup does not agree with the _Card1RestoreCmd.Password system-defined variable. • The DIP switch on the CPU Unit is not set to allow starting the restore of SD Memory Card backups by specification with system-defined variables. • There is no such folder as specified by the system-defined variable. • Required files are not set to transfer in the setting of the system-defined variable. Also check the following when you use the Robot Integrated CPU Unit. • The SD Memory Card is write protected. • The capacity of the SD Memory Card is insufficient.						

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
102C0000 hex	Restore Operation Failed	The restore operation ended in an error.	• It was not possible to read the data to restore. • The SD Memory Card was removed during a restore operation. • Failed to restore Unit or slave. • The SD Memory Card is damaged. • An unexpected error has occurred. Also check the following when you use the Robot Integrated CPU Unit. • The SD Memory Card is write protected. • The capacity of the SD Memory Card is insufficient. • The number of files or directories in the SD Memory Card exceeded the maximum number supported by the file system of the SD Memory Card.				○		page 15-106
103F0000 hex	Online Edits Transfer Failure	Transferring the online edits failed.	• The number of variables exceeded the upper limit of variables. • The variable setting for Initial Value Specified/No Initial Value Specified was changed.				○		page 15-107
10630000 hex	Safety Data Logging Failed to Start	Starting the safety data logging failed.	• An SD Memory Card is not inserted. • There are no logging setting files. • The logging settings number of the logging setting file is duplicated. • The logging settings number of the logging setting file is outside of the specifications. • The logging setting files are invalid. • Not all of safety master connections are established. • Impossible to access a logging target variable that is specified in the logging setting file.				○		page 15-108

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10640000 hex (Ver. 1.60 or later)	Safety Data Log File Save Failed	Saving the log file for safety data logging failed.	• The SD Memory Card was removed after the start of logging. • The SD Memory Card is write-protected. • The capacity of the SD Memory Card is insufficient. • The maximum number of files for an SD Memory Card was exceeded. • The SD Memory Card is damaged.				○		page 15-109
40140000 hex	PLC System Information	This event provides internal information from the PLC Function Module.	• This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.				○		page 15-109
40170000 hex	Safe Mode	The Controller started in Safe Mode.	• The Controller started in Safe Mode.				○		page 15-110
80230000 hex	NX Message Communications Error	An error has occurred in message communications.	• The communications cable is broken. • The communications cable connector is disconnected. • The NX message communications load is high.				○		page 15-110
90470000 hex	Safety Data Logging Aborted	The execution of safety data logging was aborted.	• The execution of safety data logging was aborted by a service switch operation. • Either a communication error on the safety master connections occurred or the Safety CPU Unit entered a operating mode where it could not continue safety process data communications. • The NX bus was restarted. • The Controller Setup or program was changed.				○		page 15-111
40150000 hex	PLC System Information	This event provides internal information from the PLC Function Module.	• This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.					○	page 15-112
44430000 hex	PLC System Information	This event provides internal information from the PLC Function Module.	• This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.					○	page 15-112
90010000 hex	Clock Changed	The clock time was changed.	• The clock time was changed.					○	page 15-113

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
90020000 hex	Time Zone Changed	The time zone was changed.	• The time zone was changed.					○	page 15-113
90050000 hex	User Program/ Controller Configurations and Setup Downloaded	The user program and the Controller configurations and setup were downloaded.	• The user program and the Controller configurations and setup were downloaded.					○	page 15-114
900B0000 hex	Memory All Cleared	All memory was cleared.	• A user with Administrator rights cleared all of the memory.					○	page 15-114
900C0000 hex	Event Log Cleared	The event log was cleared.	• The event log was cleared by the user.					○	page 15-115
90110000 hex	Power Turned ON	The power supply was turned ON.	• The power supply was turned ON.					○	page 15-115
90120000 hex	Power Interrupted	The power supply was interrupted.	• The power supply was interrupted.					○	page 15-116
90150000 hex	Reset Executed	A reset was executed.	• A reset command was received.					○	page 15-116
90180000 hex	All Controller Errors Cleared	All current errors were cleared.	• The user cleared all current errors.					○	page 15-116
901A0000 hex	Backup Started	A backup operation was started.	• A backup operation was started.					○	page 15-117
901B0000 hex	Backup Completed	The backup operation ended normally.	• The backup operation ended normally.					○	page 15-117
901C0000 hex	Restore Operation Started	A restore operation started.	• A restore operation started.					○	page 15-118
901D0000 hex	Restore Operation Completed	The restore operation ended normally.	• The restore operation ended normally.					○	page 15-118
90370000 hex	Web UI Authentication Failed	Web UI authentication failed.	Attempts to log in to Web UI failed consecutively.					○	*Errors Related to Controller Operation* on page 15-94
90460000 hex	Safety Data Logging Started	Safety data logging was started.	Safety data logging was started because the start conditions were met.					○	page 15-119
90480000 hex	Safety Data Logging Completed	The execution of safety data logging was completed because the trigger conditions were met.	The trigger condition that is specified in the Safety Data Logging Settings is met, and safety data logging ends.					○	page 15-119

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
95A70000 hex	Cameras Settings Imported/ Exported	Camera settings were imported or exported.	Camera settings were imported or exported via Web UI.					○	*Errors Related to Controller Operation* on page 15-94
95A80000 hex	Network Storage Connection Successful	Connection to the network storage was successful.	Connection to the output destination network storage was successful.					○	*Errors Related to Controller Operation* on page 15-94

NX Bus Function Module Error Table

● Errors Related to the NX Bus

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
04100000 hex	NX Bus Controller Error	An error occurred in the NX bus.	• An I/O communications error occurred between the CPU Unit and the NX Unit.		○				page 15-120
04110000 hex	NX Bus Hardware Error	A hardware error was detected in the NX Bus Function Module.	• A hardware error related to the NX bus was detected.		○				page 15-121
10600000 hex	NX Bus Memory Check Error	An error was detected in the internal memory check for the NX Bus Function Module.	• An error was detected in the memory check for the internal protection circuit.		○				page 15-121
10610000 hex	Failed to Read NX Unit Operation Settings	Reading the NX Unit operation settings failed. Cycle the power supply to the CPU Unit to restore the previous normally-saved settings.	• The NX Unit operation settings are not saved normally in the CPU Unit.		○				page 15-122
24D00000 hex	Number of Mountable NX Units Exceeded	The number of mounted NX Units exceeds the specified value for the CPU Unit.	More than the maximum number of NX Units are mounted on the CPU Unit.		○				page 15-123
24D20000 hex	Total I/O Data Size in NX Units Excessive	The total size of I/O data in the mounted NX Units exceeds the maximum specified value for the CPU Unit.	• The total size of I/O data in the mounted NX Units exceeds the maximum specified value for the CPU Unit.		○				page 15-124
35900000 hex	NX Unit Version Not Matched	There is a mounted NX Unit with a unit version earlier than that in the Unit configuration information registered in the CPU Unit.	The unit version of an NX Unit mounted in the actual configuration is earlier than that in the Unit configuration information registered in the CPU Unit.		○				page 15-125

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
35910000 hex	Unregistered NX Unit Mounted	There is a mounted NX Unit that does not exist in the Unit configuration information registered in the CPU Unit. If there are more than one NX Unit relevant to this event, only the NX Unit that is nearest to the CPU Unit is registered with the event.	• There is a mounted Unit that does not exist in the Unit configuration information registered in the CPU Unit. • There is a mounted Unit in which the NX Unit Mounting Setting is set to *Disabled*.		○				page 15-126
35930000 hex	NX Unit Serial Number Mismatch	There is a mounted NX Unit with a serial number different from that in the Unit configuration information registered in the CPU Unit.	• One or more NX Units with the serial number set in the Unit configuration information registered in the CPU Unit are not mounted.		○				page 15-127
44440000 hex	NX Bus Function Processing Error	A fatal error was detected in the NX Bus Function Module.	An error occurred in the software.		○				page 15-128
85540000 hex	NX Bus I/O Communications Stopped Due to Another Event	The I/O communications on the NX bus were stopped because an error that prevents I/O communications on the NX bus occurred.	• The I/O refreshing was stopped because a minor fault error (another event) that triggers fail-soft operation occurred when the Fail-soft Operation Setting is *Stop*. • The I/O communications was stopped because the *Registered NX Unit Not Mounted* event occurred and the actual configuration prevents I/O communications from starting.		○				page 15-128
35920000 hex	Registered NX Unit Not Mounted	One or more NX Units set in the Unit configuration information registered in the CPU Unit are not mounted. If there are more than one NX Unit relevant to this event, only the NX Unit that is nearest to the CPU Unit is registered with the event.	• There is no mounted NX Unit that exists in the Unit configuration information registered in the CPU Unit. • The power supply to the Additional NX Unit Power Supply Unit is not turned ON.			○			page 15-129

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
85500000 hex	NX Bus Communications Error	A communications error that prevents normal NX bus communications was detected. If there are more than one NX Unit relevant to this event, only the NX Unit that is nearest to the CPU Unit is registered with the event.	• The NX bus connector contact is faulty due to vibration or shock. • Excessive noise is applied to the NX bus connector. • An NX Unit was removed. • An error occurred in an NX Unit.			○			page 15-130
85510000 hex	NX Unit Communications Timeout	An error occurred in I/O data communications with the NX Units.	• An NX Bus Communications Error has occurred. • An error occurred in an NX Unit.			○			page 15-130
85520000 hex	NX Unit Initialization Error	Initializing an NX Unit failed.	• Initialization with the Unit configuration information registered in the CPU Unit failed. • An NX Bus Communications Error has occurred. • The Channel Enable/Disable Setting for all channels of the Analog Unit are set to Disable. • Initialization of an NX Unit failed.			○			page 15-131
85530000 hex	NX Unit Startup Error	Starting an NX Unit failed.	A startup error occurred in an NX Unit.			○			page 15-132
103C0000 hex	NX Unit Backup Failed	The backup operation for an NX Unit ended in an error.	• There is also another error related to the NX Bus Function Module. • An NX Bus Communications Error has occurred. • Backup data cannot be received from an NX Unit.				○		page 15-132
103D0000 hex	NX Unit Restore Operation Failed	The restore operation for an NX Unit ended in an error.	• There is also another error related to the NX Bus Function Module. • An NX Bus Communications Error has occurred. • The backup data cannot be sent to an NX Unit. • The Unit configuration in the backup file does not agree with the actual Unit configuration.				○		page 15-133

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10620000 hex	NX Unit Event Log Save Error	Saving or reading the NX Unit event log failed. Continuing to operate with this error may result in no event log saved at CPU Unit power OFF although it has no effect on the control function.	• Data in the NX Unit event log area are invalid.				○		page 15-134
44450000 hex	NX Bus System Information	This event provides internal information from the NX Bus Function Module.	• This event provides internal information from the NX Bus Function Module.					○	page 15-134
95800000 hex	NX Bus Restart Executed	An NX bus restart was executed.	An NX bus restart command was received.					○	page 15-135
95810000 hex	NX Unit Memory All Cleared	The NX Unit operation settings were initialized.	A Clear All Memory operation for an NX Unit was received.					○	page 15-135

EtherNet/IP Function Module Error Table

● Errors Related to the Built-in EtherNet/IP Port on Communication Control Unit

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
14220000 hex	EtherNet/IP Processing Error	A fatal error was detected in the EtherNet/IP Function Module.	• Hardware has failed.		○				page 15-136
04210000 hex	Communications Controller Error	A hardware error was detected in the communications controller of the built-in EtherNet/IP port.	• Hardware error in the communications controller			○			page 15-136
14210000 hex	Identity Error	The CIP identity information in non-volatile memory was not read correctly.	• Non-volatile memory failure			○			page 15-137
14230000 hex	MAC Address Error	The MAC address in non-volatile memory was not read correctly.	• Non-volatile memory failure			○			page 15-137
28040000 hex	IP Address Switch Settings Error	An error was detected in the IP address switch settings.	• The built-in EtherNet/IP port settings (TCP/IP settings)are set to obtain from BOOTP server, but the IP address switch is not set correctly. • Communications port 1 and communications port 2 of the built-in EtherNet/IP ports belong to the same network. • All bits for the host address of the built-in EtherNet/IP port are 0 or 1.			○			page 15-138
34200000 hex	Tag Data Link Setting Error	An error was detected in the communications settings for tag data links.	• Power was interrupted when a download was in progress for the data link settings. • Memory error			○			page 15-139
34230000 hex	IP Route Table Setting Error	An IP routing setting error was detected.	• Setting error • Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings. • Memory error			○			page 15-140
34240000 hex	FTP Server Setting Error	An error was detected in the FTP server settings.	• Setting error • Power was interrupted when a download was in progress for the FTP server settings. • Memory error			○			page 15-141

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
34250000 hex	NTP Client Setting Error	An error was detected in the NTP client settings.	• Setting error • Power was interrupted when a download was in progress for the NTP client settings. • Memory error			○			page 15-142
34260000 hex	SNMP Setting Error	An error was detected in the SNMP agent/trap settings.	• Setting error • Power was interrupted when a download was in progress for the SNMP agent/trap settings. • Memory error			○			page 15-143
34270000 hex	Tag Name Resolution Error	Resolution of a tag used in a tag data link failed.	• The size of the network variable is different from the tag settings. • The I/O direction set for a tag data link and the I/O direction of the Controller variable do not match. • There are no network variables for the Controller tag settings. • A variable in the Controller that is set for a tag data link has the Network Publish attribute set to Input but also has the Constant attribute.			○			page 15-144
34280000 hex	Basic Ethernet Setting Error	An error was detected in the Ethernet settings.	• Parameter error • Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings. • A memory error occurred.			○			page 15-145
34290000 hex	IP Address Setting Error	An error was detected in the IP address settings.	• Parameter error • Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings. • The IP address acquired from BOOTP or DHCP server is illegal. • A memory error occurred.			○			page 15-146
342A0000 hex	DNS Setting Error	An error was detected in the DNS settings or Hosts settings.	• Parameter error • Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings. • A memory error occurred.			○			page 15-147

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
50010000 hex	Controller Insufficient Memory Warning	The amount of data for the EtherCAT slave configuration, network-published information, or other data exceeds the value that is specified for the CPU Unit. You may not be able to perform online editing or other operations.	• The amount of data for the EtherCAT slave configuration, network-published information, or other data exceeds the value that is specified for the CPU Unit.			○			page 15-148
84030000 hex	DNS Server Connection Error	Connection with the DNS server failed.	• Parameter error • The server went down. • An error occurred in the communications path.			○			page 15-148
84040000 hex	NTP Server Connection Error	Connection with the NTP server failed.	• Parameter error • The server went down. • An error occurred in the communications path.			○	⊙		page 15-149
84070000 hex	Tag Data Link Connection Failed	Establishing a tag data link connection failed.	• The tag data link connection information is not the same for the originator and target. • Insufficient connections			○			page 15-150
84080000 hex	Tag Data Link Timeout	A timeout occurred in a tag data link.	• The power supply to the target node is OFF. • Communications at the target node are stopped. • The Ethernet cable for EtherNet/IP is disconnected. • The Ethernet cable for EtherNet/IP is broken. • The link to the built-in EtherNet/IP port is OFF. • The packet loss occurred on the path due to the network communications load. • Noise			○			page 15-151
84090000 hex	Tag Data Link Connection Timeout	A timeout occurred while trying to establish a tag data link connection.	• The power supply to the target node is OFF. • Communications at the target node are stopped. • The Ethernet cable connector for EtherNet/IP is disconnected. • The Ethernet cable for EtherNet/IP is broken. • An error occurred in the communications path.			○	⊙		page 15-152

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
840A0000 hex	IP Address Duplication Error	The same IP address is used more than once.	• The IP address of the built-in EtherNet/IP port is also used as the IP address of another node.			○			page 15-153
840B0000 hex	BOOTP Server Connection Error	Connection with the BOOTP server failed.	• Server setting error • The server went down. • An error occurred in the communications path.			○			page 15-154
840C0000 hex	Allowed Communications Bandwidth per Unit Exceeded	The total bandwidth for the connections that are set or established exceeded the allowed communications bandwidth of tag data links and CIP Safety communications per Unit for all of the built-in EtherNet/IP ports.	• An attempt was made to establish a connection that would cause the used bandwidth (PPS) total of the packet transfer rates of the tag data links and CIP Safety communications that use all of the built-in EtherNet/IP ports to exceed the allowed communications bandwidth per Unit.			○			page 15-155
840D0000 hex	IP Address Switch Change during Operation Error	The IP address switch setting was changed during the operation.	• The IP address switch setting was changed during the operation.			○			page 15-156
840E0000 hex	Number of Tag Sets for Tag Data Links Exceeded	The total number of tag sets for tag data links for all ports of the built-in Ethernet/IP port exceeds the upper limit.	• The total number for all ports of tag sets for tag data links that are set for each built-in Ethernet/IP port exceeds the total number the product allows.			○			page 15-157
54E00000 hex	Access Detected Outside Range of Variable	Accessing a value that is out of range was detected for a tag variable that is used in a tag data link.	• An out-of-range value was written by an EtherNet/IP tag data link for a variable with a specified range. A value that does not specify an enumerator was written by an EtherNet/IP tag data link for an enumeration variable.				○		page 15-158
84050000 hex	Packet Discarded Due to Full Reception Buffer	A packet was discarded.	• A network convergence occurred.				○		page 15-158

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
84060000 hex	Link OFF Detected	An Ethernet link OFF was detected.	• An Ethernet cable is broken, disconnected, or loose. • The Ethernet switch's power supply is turned OFF. • Communications speed mismatched. • Noise • The Identity object was reset. • Settings for EtherNet/IP were downloaded from the Network Configurator or Sysmac Studio, or the Clear All Memory operation was performed. • EtherNet/IP was restarted. • If an Ethernet link off is detected on port 2, the **Use Port 2** check box is not selected.			⊙	○		page 15-159
94010000 hex	Tag Data Link Download Started	Changing the tag data link settings started.	• Changing the tag data link settings started.					○	page 15-160
94020000 hex	Tag Data Link Download Finished	Changing the tag data link settings finished.	• Changing the tag data link settings finished.					○	page 15-160
94030000 hex	Tag Data Link Stopped	Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.	• Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.					○	page 15-161
94040000 hex	Tag Data Link Started	Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.	• Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.					○	page 15-162
94050000 hex	Link Detected	Establishment of an Ethernet link was detected.	• Establishment of an Ethernet link was detected.					○	page 15-163

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
94060000 hex	Restarting Ethernet Port	The built-in EtherNet/IP port was restarted.	• The built-in EtherNet/IP port was restarted.					○	page 15-163
94070000 hex	Tag Data Link All Run	Tag data link connections to all nodes have been normally established.	• Tag data link connections to all target nodes have been normally established.					○	page 15-164
94080000 hex	IP Address Fixed	The correct IP address has been determined and Ethernet communications can start.	• The correct IP address has been determined and Ethernet communications can start.					○	page 15-164
94090000 hex	BOOTP Client Started	The BOOTP client started requesting an IP address.	• The BOOTP client started requesting an IP address.					○	page 15-165
940A0000 hex	FTP Server Started	The FTP agent started normally.	• The FTP agent started normally.					○	page 15-165
940B0000 hex	NTP Client Started	The NTP client started normally and a request for the NTP server to obtain the time started.	• The NTP client started normally and a request for the NTP server to obtain the time started.					○	page 15-165
940C0000 hex	SNMP Started	The SNMP agent started normally.	• The SNMP agent started normally.					○	page 15-166

PLC Function Module Error Descriptions

● Errors for Self Diagnosis

Event name	DIP Switch Setting Error			**Event code**	00090000 hex	
Meaning	An error was detected in the DIP switch setting.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Major fault	**Recovery**	Cycle the power supply.	**Log category**	System
Effects	**User program**	Stops.	**Operation**	Stops.*1		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	There is an error in the DIP switch setting.		Turn OFF all pins on the DIP switch.		Make sure that the DIP switch settings are correct.	
Attached information	Attached information 1: DIP switch readout value (00000000 hex to 0000000F hex)					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Internal Bus Check Error			Event code	000D0000 hex	
Meaning	A fatal error was detected on the internal bus.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1 A connection to the Sysmac Studio may not be possible.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A conductive material has gotten inside.		If there is conductive material nearby, blow out the CPU Unit with air.		Do not do any metal working in the vicinity of the control panel. Also, make sure that the operating environment is free of dirt and dust. Close the control panel.	
	Noise • There is data corruption in bus signals. • There is malfunctioning in bus interface circuits.		If the error occurs even after making the above correction, check the FG, and power supply lines, and other noise entry paths, and implement noise countermeasures as required.		Implement noise countermeasures.	
	The CPU Unit has failed. • The internal bus is disconnected.		If this error persists even after you make the above two corrections, replace the CPU Unit.		None	
Attached information	Attached information 1: System information					
Precautions/ Remarks	When this error occurs, the CPU Unit stops and the error is recorded in the event log. If cycling the power to the Controller clears the error, you will be able to see whether this error occurred by checking the event log. However, a restart is sometimes not possible depending on the error location.					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Non-volatile Memory Life Exceeded			Event code	000E0000 hex	
Meaning	The specified number of deletions for non-volatile memory was exceeded. Or, the number of bad blocks in memory exceeded the specified value.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON, at Controller reset, or periodically
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Non-volatile memory life expired.		Replace the CPU Unit.		Depending on a user program or application, the non-volatile memory life may be shortened. Check the following 1 and 2. 1. Frequency of SD Memory Card backup processing by system-defined variables and special instructions 2. Frequency of instructions to write to non-volatile memory such as MC_SaveCamTable and ChangeIPAdr instructions If the execution of 1 or 2 above fails, re-execute after you remove the cause of the error. If you retry before you remove the cause of error, the number of deletions for non-volatile memory increases and the non-volatile memory life may be shortened.	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Main Memory Check Error			**Event code**	00130000 hex	
Meaning	An error was detected in the memory check of the main memory in the CPU Unit.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	Continuously
Error attributes	**Level**	Major fault	**Recovery**	Cycle the power supply or reset the Controller.	**Log category**	System
Effects	**User program**	Stops.	**Operation**	Stops.*1		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	A conductive material has gotten inside.		If there is conductive material nearby, blow out the CPU Unit with air.		Do not do any metal working in the vicinity of the control panel. Use the control panel only when it is closed.	
	Noise • Data corruption in memory • Microcomputer malfunctioning • Memory write circuit malfunctioning		If the error did not result from the above causes, cycle the power to the Controller and see if that clears the error. If the error occurs frequently, check the FG, power supply lines, and other noise entry paths, and implement noise countermeasures as required.		Implement noise countermeasures.	
	There is a soft error. • Data corruption was caused by cosmic rays or radiation.		If the error did not result from the above causes, and cycling the power to the Controller or resetting the Controller does not clear the error, replace the CPU Unit.		None	
	The CPU Unit has failed. • Memory element failure • Memory peripheral circuit failure				Perform regular inspections.	
Attached information	Attached information 1: System information Attached information 2: System information					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

<table>
<tr><td>Event name</td><td colspan="3">Non-volatile Memory Restored or Formatted</td><td>Event code</td><td colspan="2">10010000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An error was detected in the non-volatile memory check and file system recovery or formatting was executed. Previous files may have been deleted.</td></tr>
<tr><td>Source</td><td colspan="2">PLC Function Module</td><td>Source details</td><td>None</td><td>Detection timing</td><td>At power ON or Controller reset</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Major fault</td><td>Recovery</td><td>Cycle the power supply or reset the Controller.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Stops.</td><td>Operation</td><td colspan="3">Stops.*1</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The Controller power supply was turned OFF while the BUSY indicator was lit.</td><td colspan="2" rowspan="2">Compare the project with the project on the Sysmac Studio. If they match, cycle the power supply to the Controller or reset the Controller to see if that clears the error. If the error is cleared, check that the device operates correctly.
If the comparison shows a mismatch, if the error is not cleared, or if the device does not operate correctly, clear all of memory and then download the project from the Sysmac Studio again. If cycling the power supply to the Controller or resetting the Controller does not clear the error, the memory is corrupted. Replace the CPU Unit. Unexpected operation may occur and can be very dangerous if the power to the Controller is cycled or the Controller is reset before you download the project again.</td><td colspan="2">Do not turn OFF the power supply while the BUSY indicator is lit.</td></tr>
<tr><td colspan="2">The power supply to the Controller was interrupted momentarily while the BUSY indicator was lit.</td><td colspan="2">Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Recovered content
• (00000000 hex: File system recovery successful,
• 00000001 hex: Formatted)</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">Make sure that the projects match and that the device operates correctly, or transfer the project again. If you cycle the power to the Controller or reset the Controller before you do this, unexpected operation may occur and can be very dangerous.</td></tr>
</table>

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Non-volatile Memory Data Corrupted			Event code	10020000 hex	
Meaning	A file that must be in non-volatile memory is missing or corrupted.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Major fault	Recovery	Cycle the power supply or reset the Controller.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The Controller power supply was turned OFF while the BUSY indicator was lit.		Clear all of memory and then download the project from the Sysmac Studio.		Do not turn OFF the power supply while the BUSY indicator is lit.	
	The power supply to the Controller was interrupted momentarily while the BUSY indicator was lit.				Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.	
	The CPU Unit has failed.		If this error remains even after making the above corrections, replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

<table>
<tr><td>Event name</td><td colspan="3">Main Memory Check Error</td><td>Event code</td><td colspan="2">10080000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An error was detected in the memory check of the main memory in the CPU Unit.</td></tr>
<tr><td>Source</td><td colspan="2">PLC Function Module</td><td>Source details</td><td>None</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Major fault</td><td>Recovery</td><td>Cycle the power supply.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Stops.</td><td>Operation</td><td colspan="3">Stops.*1</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="5">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">A conductive material has gotten inside.</td><td colspan="2">If there is conductive material nearby, blow out the CPU Unit with air.</td><td colspan="2">Do not do any metal working in the vicinity of the control panel.
Use the control panel only when it is closed.</td></tr>
<tr><td colspan="2">Noise
• Data corruption in memory
• Microcomputer malfunctioning
• Memory write circuit malfunctioning</td><td colspan="2">If the error did not result from the above causes, cycle the power to the Controller and see if that clears the error.
If the error occurs frequently, check the FG, power supply lines, and other noise entry paths, and implement noise countermeasures as required.</td><td colspan="2">Implement noise countermeasures.</td></tr>
<tr><td colspan="2">There is a soft error.
• Data corruption was caused by cosmic rays or radiation.</td><td colspan="2" rowspan="2">If the error did not result from the above causes, and cycling the power to the Controller or resetting the Controller does not clear the error, replace the CPU Unit.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">The CPU Unit has failed.
• Memory element failure
• Memory peripheral circuit failure</td><td colspan="2">Perform regular inspections.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: System information</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Non-volatile Memory Data Corrupted			Event code	100B0000 hex	
Meaning	A file that must be in non-volatile memory is missing or corrupted.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Major fault	Recovery	Cycle the power supply or reset the Controller.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The Controller power supply was turned OFF while the BUSY indicator was lit.		Clear all of memory and then download the project from the Sysmac Studio.		Do not turn OFF the power supply while the BUSY indicator is lit.	
	The power supply to the Controller was interrupted momentarily while the BUSY indicator was lit.				Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.	
	The CPU Unit has failed.		If this error remains even after making the above corrections, replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Event Level Setting Error			**Event code**	100C0000 hex	
Meaning	The settings in the event level setting file are not correct.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Major fault	**Recovery**	Cycle the power supply or reset the Controller.	**Log category**	System
Effects	**User program**	Stops.	**Operation**	Stops.*1		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The event level settings are not correct because the power supply to the Controller was interrupted or communications with the Sysmac Studio were disconnected during a download of the event level settings.		Perform a Memory All Clear operation and then transfer the event level setting file again.		Do not interrupt the power supply to the Controller or disconnect communications with the Sysmac Studio during a download of the event level settings.	
	The event level settings are not correct because the power supply to the Controller was interrupted during a Clear All Memory operation.				Do not interrupt the power supply to the Controller during a Clear All Memory operation.	
	Non-volatile memory failed.		If the error persists even after you make the above correction, replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Present Values of Retained Variables Restoration Error		Event code	100F0000 hex	
Meaning	The present values of retained variables could not be restored at startup and the values were initialized.				
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Major fault	Recovery	Cycle the power supply or reset the Controller.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variable	Variable		Data type		Name	
	_RetainFail		BOOL		Retention Failure Flag	
Cause and correction	Assumed cause		Correction		Prevention	
	• An error occurred in the software. • Backup memory failure		Perform the following: • Check the values of the retained variables and the retained areas in the memory used for CJ-series Units and change them to the correct values. • If this error persists, replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	The following values are initialized. • Retained variables (variables with Retain attribute or variables with AT specification in the retained area) • Retained area in the memory used for CJ-series Units					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

<table>
<tr><td>Event name</td><td colspan="2">Present Values of Retained Variables Not Saved</td><td>Event code</td><td colspan="2">10100000 hex</td></tr>
<tr><td>Meaning</td><td colspan="5">The process of saving the current value of the retained variable during power interruptions could not be performed because an error occurred in the software. (NX502, NX102, and NX1P2 CPU Unit)(Communication Control Unit)
The process of saving the current value of the retained variable during power interruptions could not be performed because the Controller was forcibly shut down or an error occurred in the software. (NY-series Controller)</td></tr>
<tr><td>Source</td><td colspan="2">PLC Function Module</td><td>Source details</td><td>None</td><td>Detection timing</td><td>At power ON or Controller reset</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Major fault</td><td>Recovery</td><td>Cycle the power supply.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Stops.</td><td>Operation</td><td colspan="3">Stops.*1</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">----</td><td colspan="2">----</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">A forced shutdown is performed. (NY-series Controllers)</td><td colspan="2" rowspan="2">Perform the following:
• Check the values of the retained variables and change them to the correct values. (NY-series Controller)
• If the system uses a Servomotor with an absolute encoder, turn ON the power supply, and then turn ON the Servo and check the actual current position of the axis.

(NX502, NX102 and NX1P2 CPU Unit)
• Check the values of the retained variables and the retained areas in the memory used for CJ-series Units and change them to the correct values.
• After you perform the corrections, set the Retention Inexecution Flag (_RetainUnexec) to FALSE.</td><td colspan="2">Perform a shutdown with other method than the forced shutdown. (NY-series Controllers)</td></tr>
<tr><td colspan="2">An error occurred in the software.</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="5">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="5">The values of the following will be the values from the previous time the power supply wasturned ON.
• Absolute encoder home offset data</td></tr>
</table>

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC System Processing Error			Event code	40020000 hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC System Processing Error			Event code	40030000 hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	Attached information 1: System information					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC System Processing Error			Event code	40040000 hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1 A connection to the Sysmac Studio is not possible.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC System Processing Error			Event code	40050000 hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1 A connection to the Sysmac Studio is not possible.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Real-Time Clock Stopped			Event code	00070000 hex	
Meaning	The oscillation of the real-time clock stopped. The real-time clock is set to an illegal time.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Error reset	Log category	System
Effects	User program	Continues.	Operation	The System Time is not defined. The clock information recorded by CJ-series Units is also not defined.		
System-defined variables	Variable		Data type		Name	
	_CurrentTime		DATE_AND_TIME		System Time	
Cause and correction	Assumed cause		Correction		Prevention	
	The battery voltage is low.		Replace the Battery. Then adjust the real-time clock time.		Regularly replace the Battery.	
	The battery connector has come loose.		Reconnect the connector and make sure it is mated correctly. Then adjust the real-time clock time.		Check for vibration and shock.	
	The Battery is missing.		Install a Battery. Then adjust the real-time clock time.		Install a Battery.	
Attached information	None					
Precautions/ Remarks	This error is checked only when the power is turned ON. You can change the event level to the observation level. If you change the level to the observation level, recovery procedures are not required.					

Event name	Real-Time Clock Failed			Event code	00080000 hex	
Meaning	The real-time clock in the CPU Unit failed.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Continues.	Operation	The System Time is not defined. The clock information recorded by CJ-series Units is also not defined.		
System-defined variables	Variable		Data type		Name	
	_CurrentTime		DATE_AND_TIME		System Time	
Cause and correction	Assumed cause		Correction		Prevention	
	The CPU Unit clock has failed.		Replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	SD Memory Card Invalid Type			Event code	000F0000 hex	
Meaning	The current SD Memory Card is not supported.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON, at Controller reset, or when SD Memory Card is inserted
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	SD PWR indicator is not lit. Power supply to SD Memory Card is stopped.		
System-defined variables	Variable		Data type		Name	
	_Card1Ready		BOOL		SD Memory Card Ready Flag	
Cause and correction	Assumed cause		Correction		Prevention	
	An SD Memory Card that is not supported was inserted into the CPU Unit.		Replace with an HMC-SD291 SD Memory Card, an HMC-SD491 SD Memory Card, or an HMC-SD1A1 SD Memory Card. In the following case, replace with an HMC-SD491 SD Memory Card or an HMC-SD1A1 SD Memory Card. • For NJ501-□□□□ CPU Units, the hardware revision is “A” and the unit version is 1.15 or later.		Use an HMC-SD291 SD Memory Card, an HMC-SD491 SD Memory Card, or an HMC-SD1A1 SD Memory Card. In the following case, use an HMC-SD491 SD Memory Card or an HMC-SD1A1 SD Memory Card. • For NJ501-□□□□ CPU Units, the hardware revision is “A” and the unit version is 1.15 or later.	
Attached information	Attached information 1: “Not UHS-I” is displayed when the SD Memory Card does not support UHS-I.					
Precautions/ Remarks	Refer to *Specifications of Supported SD Memory Cards, Folders, and Files* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for information on supported SD Memory Cards.					

Event name	SD Memory Card Life Exceeded			Event code	00100000 hex	
Meaning	The specified number of deletions for the SD Memory Card was exceeded. Or, the number of bad blocks exceeded the specified value.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON, at Controller reset, or periodically
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_Card1Deteriorated		BOOL		SD Memory Card Life Warning Flag	
Cause and correction	Assumed cause		Correction		Prevention	
	The service life of the SD Memory Card was exceeded.		Back up necessary files in the SD Memory Card. Or replace the SD Memory Card.		Regularly replace the SD Memory Card.	
Attached information	None					
Precautions/ Remarks	• The data on the SD Memory Card may be corrupted. • Normal user program operation may not be possible. • You can change the event level to the minor fault level. If you change the level to the minor fault level, the Recovery column above will be changed to “Error reset.” • You can use the SD memory card life expiration detection function on some specific SD Memory Cards. Refer to *Specifications of Supported SD Memory Cards, Folders, and Files* in the *NX-series Communication Control Unit Built-in Function User's Manual (Cat. No. Z396)* for details.					

Event name	SD Memory Card Invalid Format			Event code	10030000 hex	
Meaning	The file format of the SD Memory Card is not FAT16 or FAT32.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON, at Controller reset, or when SD Memory Card is inserted
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	SD PWR indicator is not lit. You can format the SD Memory Card from the Sysmac Studio.		
System-defined variables	Variable		Data type		Name	
	_Card1Ready		BOOL		SD Memory Card Ready Flag	
Cause and correction	Assumed cause		Correction		Prevention	
	The file format of the SD Memory Card inserted in the CPU Unit is not FAT16 or FAT32.		Make sure that the correct SD Memory Card is inserted in the CPU Unit. If an incorrect SD Memory Card is inserted, replace it with the correct one. If the correct SD Memory Card is inserted, format it correctly before you use it.		Use an OMRON SD Memory Card. Do not format the SD Memory Card on a computer.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">SD Memory Card Restored or Formatted</td><td>Event code</td><td colspan="2">10040000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An error was detected during the file system check and the file system was restored. Files may have been deleted.</td></tr>
<tr><td>Source</td><td colspan="2">PLC Function Module</td><td>Source details</td><td>None</td><td>Detection timing</td><td>At power ON or Controller reset</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">If the file is deleted, normal user program operation may not be possible.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="4">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The Controller power supply was turned OFF while the SD BUSY indicator was lit.</td><td colspan="2" rowspan="3">Check that the correct file is on the SD Memory Card, or that the device operates correctly.
If the correct file is not on the SD Memory Card, or if the device does not operate correctly, download the correct file to the SD Memory Card.
Cycle the power supply to the Controller or reset the Controller and confirm that the system operates correctly.</td><td colspan="2">Do not turn OFF the power supply while the SD BUSY indicator is lit.</td></tr>
<tr><td colspan="2">The power supply to the Controller was interrupted momentarily while the SD BUSY indicator was lit.</td><td colspan="2">Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.</td></tr>
<tr><td colspan="2">The SD Memory Card was removed while the SD PWR indicator was lit.</td><td colspan="2">Do not remove the SD Memory Card while the SD PWR indicator is lit.</td></tr>
<tr><td colspan="2">The SD Memory Card is damaged.</td><td colspan="2">If this error occurs even though the above problem does not exist, replace the SD Memory Card and download the correct files to it.</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">The error is detected at power ON or at a Controller reset only when SD Memory Card diagnosis at startup is enabled.
You can change the event level to the minor fault level. If you change the level to the minor fault level, the Recovery column above will be changed to “Error reset.”</td></tr>
</table>

Event name	SD Memory Card Data Corrupted			Event code	10060000 hex	
Meaning	A file that must be in the SD Memory Card is missing or corrupted.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	SD PWR indicator is not lit. You can format the SD Memory Card from the Sysmac Studio. Normal user program operation may not be possible.		
System-defined variables	Variable		Data type		Name	
	_Card1Ready		BOOL		SD Memory Card Ready Flag	
Cause and correction	Assumed cause		Correction		Prevention	
	The Controller power supply was turned OFF while the SD BUSY indicator was lit.		Format the SD Memory Card and download the correct file.		Do not turn OFF the power supply while the SD BUSY indicator is lit.	
	The power supply to the Controller was interrupted momentarily while the SD BUSY indicator was lit.				Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.	
	The SD Memory Card was removed while the SD PWR indicator was lit.				Do not remove the SD Memory Card while the SD PWR indicator is lit.	
	The SD Memory Card is damaged.		If the error cannot be cleared with the above corrections, replace the SD Memory Card with one that operates normally.		None	
Attached information	None					
Precautions/ Remarks	The error is detected at power ON or at a Controller reset only when SD Memory Card diagnosis at startup is enabled. You can change the event level to the minor fault level. If you change the level to the minor fault level, the Recovery column above will be changed to “Error reset.”					

Event name	SD Memory Card Access Power OFF Error			Event code	10070000 hex	
Meaning	The power supply to the Controller was interrupted during access to the SD Memory Card.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Operation is controlled by the user program when the file is corrupted.		
System-defined variables	Variable		Data type		Name	
	_Card1PowerFail		BOOL		SD Memory Card Power Interruption Flag	
Cause and correction	Assumed cause		Correction		Prevention	
	The Controller power supply was turned OFF while the SD BUSY indicator was lit.		Check that the correct file is on the SD Memory Card, or that the device operates correctly. If the correct file is not on the SD Memory Card, or if the device does not operate correctly, download the correct file to the SD Memory Card. Cycle the power supply to the Controller or reset the Controller and confirm that the system operates correctly. When you have finished the corrections, change the _Card1PowerFail (SD Memory Card Power Interruption Flag) system-defined variable to FALSE.		Do not turn OFF the power supply while the SD BUSY indicator is lit.	
	The power supply to the Controller was interrupted momentarily while the SD BUSY indicator was lit.				Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied in places where the power supply is unstable.	
Attached information	None					
Precautions/ Remarks	When the measure is completed, change the SD Memory Card Power Interruption Flag to FALSE.					

Event name	PLC System Information			Event code	10130000 hex	
Meaning	This event provides internal information from the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Incorrect SD Memory Card Removal			Event code	10310000 hex	
Meaning	SD Memory Card removal processing failed.					
Source	PLC Function Module		Source details	None	Detection timing	At SD Memory Card removal
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The SD Memory Card was removed while the SD PWR indicator was lit.		Check the files on the SD Memory Card to see if they are correct. If the files on the SD Memory Card are not correct, download the correct files to the SD Memory Card.		Press the SD Memory Card power supply switch and confirm that the SD PWR indicator goes out before you remove the SD Memory Card.	
Attached information	None					
Precautions/ Remarks	None					

● Errors Related to Controller Operation

<table>
<tr><td>Event name</td><td colspan="3">User Program/Controller Configurations and Setup Transfer Error</td><td>Event code</td><td colspan="2">10200000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">The user program or Controller Configurations and Setup were not transferred correctly.</td></tr>
<tr><td>Source</td><td colspan="2">PLC Function Module
NX Bus Function Module</td><td>Source details</td><td>None or I/O bus master</td><td>Detection timing</td><td>At power ON or Controller reset</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Major fault</td><td>Recovery</td><td>Cycle the power supply or reset the Controller.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Stops.</td><td>Operation</td><td colspan="3">Stops.*1</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="6">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during a download of the user program or the Controller Configurations and Setup.</td><td colspan="2" rowspan="4">Clear all of memory and then download the project from the Sysmac Studio.
If attached information is registered, cycle the power supply to the Controller and then implement the above correction.
If you cannot perform a Clear All Memory operation from the Sysmac Studio, transfer the project to the Controller with a restore operation from an SD Memory Card.</td><td colspan="2">Do not turn OFF the power supply to the Controller during a download of the user program or the Controller Configurations and Setup.</td></tr>
<tr><td colspan="2">The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during online editing.</td><td colspan="2">Do not interrupt the power supply to the Controller during online editing.</td></tr>
<tr><td colspan="2">The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during a Clear All Memory operation.</td><td colspan="2">Do not interrupt the power supply to the Controller during a Clear All Memory operation.</td></tr>
<tr><td colspan="2">The user program or Controller Configurations and Setup are not correct because the power supply to the Controller was interrupted during a restore operation.</td><td colspan="2">Do not interrupt the power supply to the Controller during a restore operation.</td></tr>
<tr><td colspan="2">Non-volatile memory failed.</td><td colspan="2">If the error persists even after you make the above correction, replace the CPU Unit.</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached Information 1: Cause Details
• None: Power was interrupted during a download, during online editing, or during restoration.
• Downloading/Predownloading: For other causes, the timing of error occurrence (during download or during download preparations) is given.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	Illegal User Program/Controller Configurations and Setup			**Event code**	10250000 hex	
Meaning	The upper limit of the usable memory was exceeded or the user program or Controller Configurations and Setup is corrupted.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	At download, power ON, or Controller reset
Error attributes	**Level**	Major fault	**Recovery**	Cycle the power supply or reset the Controller.	**Log category**	System
Effects	**User program**	Stops.	**Operation**	Stops.*1		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The upper limit of the data size was exceeded.		If an event on restrictions on the number of items used occurred at the same time as this event*2, correct the user program and settings so that the number of items used is not exceeded and then download the data again.		None	
	The main memory capacity was exceeded.		If an event on restrictions on the number of items used did not occur at the same time as this event*2, perform the Clear All Memory operation, cycle the power supply, and then confirm that this event was cleared. If it was cleared, reduce the size of the project, e.g., by sharing programming, and then download the project again.			
	Non-volatile memory is deteriorating or has failed.		If this error persists even after you implement the above two corrections, replace the CPU Unit.			
Attached information	None					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

*2. The *Too Many Reset Motion Control Error Instructions*(571D0000 hex) related to item count restrictions occurs only with CPU Unit versions is Ver.1.02 to Ver.1.09.

Event name	PLC Function Processing Error			Event code	40110000 hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC Function Processing Error			Event code	44420000Hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Major fault	Recovery	Cycle the power supply or reset the Controller.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

*1. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC Function Processing Error			Event code	40120000 hex	
Meaning	A fatal error was detected in the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Partial fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Stops.	Operation	Stops.*1		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

*1. Operation is the same as for a major fault level error. For details, refer to *I/O Operation for Major Fault Level Controller Errors* on page 15-13.

Event name	PLC Function Processing Error			Event code	40130000 hex	
Meaning	A fatal error was detected in part of the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Minor fault	Recovery	Cycle the power supply or reset the Controller.	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	Attached information 1: System information*1 Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

*1. If a *devb-mmcsd* is stored, replace the SD Memory Card and cycle the power supply of the CPU Unit.

Event name	Event Log Save Error			**Event code**	10230000 hex	
Meaning	Saving the event log failed.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	At power ON, or Controller reset
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Starts.	**Operation**	Not affected. However, part or all of the past event log cannot be read.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	A low battery voltage prevented retention of memory during a power interruption. (NJ/NX-series)		Replace the Battery.		Replace the battery periodically.	
	A forced shutdown was performed. (NY-series)		None		Perform a shutdown with other method than the forced shutdown.	
	Data in the event log area are invalid. (NY-series)		If the error persists even after you cycle the power to the Industrial PC, a hardware failure may occur in the event log area. Replace the Industrial PC if you use the event logs in the Industrial PC.		None	
	Data in the event log area are invalid. (NJ/NX-series)		If this error persists even after you cycle the power supply to the CPU Unit, a hardware failure may occur in the event log area. Replace the CPU Unit if you use the event logs in the CPU Unit.		None	
Attached information	Attached Information 1: Error Details • 0: Failure to save all categories of logs, • 1: Failure to save system event log, • 2: Failure to save access event log, • 100: Failure to save user-defined event log					
Precautions/ Remarks	None					

Event name	Backup Failed to Start			Event code	10290000 hex	
Meaning	An error was detected in pre-execution checks for a backup operation.					
Source	PLC Function Module		Source details	None	Detection timing	When backup is specified by the user
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An SD Memory Card is not inserted.		Insert an SD Memory Card.		Insert an SD Memory Card.	
	The SD Memory Card type is not correct.		Replace the SD Memory Card with an SD or SDHC card.		Use an SD or SDHC card.	
	The format of the SD Memory Card is not correct.		Format the SD Memory Card with the Sysmac Studio.		Use a formatted SD Memory Card. Also, do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit.	
	The SD Memory Card is write protected.		Remove write protection from the SD Memory Card.		Make sure that the SD Memory Card is not write protected.	
	The **Prohibiting backing up data to the SD Memory Card** parameter is set to *prohibit* backing up data to an SD Memory Card.		Change the setting of the **Prohibiting backing up data to the SD Memory Card** parameter to enable backing up data to an SD Memory Card.		Set the **Prohibiting backing up data to the SD Memory Card** parameter to enable backing up data to an SD Memory Card.	
	Another backup operation is in progress.		Wait for the other backup operation to end and then perform the backup operation again.		Do not attempt to perform other backup operation during a backup operation.	
	Synchronization, online editing, or the Clear All Memory operation is in progress.		Wait for the synchronization, online editing, or the Clear All Memory operation to end and then perform the backup operation again.		Do not attempt to perform a backup operation during a synchronization, online editing, or the Clear All Memory operation.	
	The backup was canceled by the user.		None		None	
	The online connection with the Sysmac Studio was disconnected.		Check the cable connections. Go offline and then go back online and execute the backup again.		Check the cable to see if it is disconnected or broken. Make sure the cable is connected properly.	
	The SD Memory Card is damaged.		If none of the above causes applies, replace the SD Memory Card.		Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit. Replace the SD Memory Card periodically according to the write life of the SD Memory Card.	
	An unexpected error has occurred.		Contact your OMRON representative or distributor.		None	

Attached information	Attached information 1: Operation type • 0101 hex: Controller to SD Memory Card for switch operation on front of CPU Unit • 0102 hex: Controller to SD Memory Card for system variable operation • 0103 hex: Controller to SD Memory Card for instruction from Sysmac Studio or function module specific trigger) • 0104 hex: Controller to SD Memory Card for instruction operation. • 0201 hex: Controller to computer Attached Information 2: Error Details • 0001 hex: An SD Memory Card is not inserted. • 0002 hex: The SD Memory Card is faulty, the format of the SD Memory Card is not correct, or the SD Memory Card is not the correct type of card. • 0003 hex: The SD Memory Card is write protected. • 0204 hex: SD Memory Card backup is prohibited. • 0205 hex: Another backup operation is in progress. • 0206 hex: Synchronization, online editing, or the Clear All Memory operation is in progress. • 0207 hex: A prohibited character is used in the directory name that is specified in the system-defined variable. • 0401 hex: The backup was canceled by the user. • 0501 hex: The online connection with the Sysmac Studio was disconnected. • 7F01 hex: An unexpected error has occurred.
Precautions/ Remarks	None

Event name	Backup Failed			Event code	102A0000 hex	
Meaning	The backup operation ended in an error.					
Source	PLC Function Module		Source details	None	Detection timing	During backup operation
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The capacity of the SD Memory Card is insufficient.		Replace the SD Memory Card for one with sufficient available space.		Use an SD Memory Card that has sufficient available space.	
	It was not possible to save the data that was specified for backup.		Perform the backup operation again when no data write operation to the CPU Unit is in progress.		Do not write to the CPU Unit when a backup operation is in progress.	
	The SD Memory Card was removed during a backup operation.		Insert an SD Memory Card.		Insert an SD Memory Card.	
	Failed to back up Unit or slave.		Refer to the corrections for the following events: CJ-series Unit Backup Failed (102D0000 hex) or EtherCAT Slave Backup Failed (102F0000 hex).		Refer to the prevention information for the following events: CJ-series Unit Backup Failed (102D0000 hex) or EtherCAT Slave Backup Failed (102F0000 hex).	
	The backup was canceled by the user.		None		None	
	Execution of the Save Cam Table instruction or changing the CPU Unit name is in progress.		Perform the operation after execution of the Save Cam Table instruction or changing the CPU Unit name is completed.		Do not perform a backup during execution of the Save Cam Table instruction or while changing the CPU Unit name.	
	The online connection with the Sysmac Studio was disconnected.		Check the cable connections. Go offline and then go back online and execute the backup again.		Check the cable to see if it is disconnected or broken. Make sure the cable is connected properly.	
	It was not possible to save the data that was specified for backup to the computer.		Increase the available space on the hard disk on the computer.		Make sure there is sufficient space available on the hard disk before you perform a backup.	
	The SD Memory Card is damaged.		If none of the above causes applies, replace the SD Memory Card.		Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit. Replace the SD Memory Card periodically according to the write life of the SD Memory Card.	
	An unexpected error has occurred.		Contact your OMRON representative or distributor.		None	
	Also check the following when you use the Robot Integrated CPU Unit.					
	The SD Memory Card format is invalid		Format the SD Memory Card with the Sysmac Studio.		Use a formatted SD Memory Card.	
	The SD Memory Card is write protected.		Remove write protection from the SD Memory Card.		Make sure that the SD Memory Card is not write protected.	
	The /D folder, which is the data to be backed up, does not exist on the SD Memory Card.		Cycle the power supply of the CPU Unit to return the /D folder to the factory default or download the project from the Sysmac Studio.		Do not delete the /D folder from the SD Memory Card.	

Attached information	Attached information 1: Operation type • 0101 hex: Controller to SD Memory Card for switch operation on front of CPU Unit • 0102 hex: Controller to SD Memory Card for system variable operation • 0103 hex: Controller to SD Memory Card for instruction from Sysmac Studio or function module specific trigger) • 0104 hex: Controller to SD Memory Card for instruction operation. • 0201 hex: Controller to computer Attached Information 2: Error Details • 0001 hex: The SD Memory Card was removed. • 0001 hex: The SD Memory Card is removed or the format is invalid (in the case that the Robot Integrated CPU Unit is used and operation type is 0201 hex). • 0003 hex: The SD Memory Card is write protected (when the Robot Integrated CPU Unit is used). • 0005 hex: There is not sufficient space available on the SD Memory Card. • 0006 hex: Too many files or directories. • 0106 hex: The /D cannot be found in the SD Memory Card (when the Robot Integrated CPU Unit is used). • 0206 hex: Execution of the Save Cam Table instruction or changing the CPU Unit name is in progress. • 00210 hex: A file already exists with the same name as one of the specified directory. • 0302 hex: Saving the backup data failed or the SD Memory Card is faulty. • 0304 hex: The Unit or slave could not be backed up. • 0401 hex: The backup was canceled by the user. • 0501 hex: The online connection with the Sysmac Studio was disconnected. • 0502 hex: It was not possible to save the data that was specified for backup to the computer. • 7F01 hex: An unexpected error has occurred.
Precautions/ Remarks	None

Event name	Restore Operation Failed to Start			Event code	102B0000 hex	
Meaning	An error was detected in pre-execution checks for a restore operation.					
Source	PLC Function Module		Source details	None	Detection timing	When restoring data is specified by the user
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	---	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	Specification with system-defined variables					
	_Card1RestoreSta		_sRESTORE_STA		SD Memory Card Restore Status	
Cause and correction	Assumed cause		Correction		Prevention	
	An SD Memory Card is not inserted.		Insert an SD Memory Card.		Insert an SD Memory Card.	
	The SD Memory Card type is not correct.		Replace the SD Memory Card with an SD or SDHC card.		Use an SD or SDHC card.	
	The format of the SD Memory Card is not correct.		Format the SD Memory Card with the Sysmac Studio and then place the backup file on it.		Use a formatted SD Memory Card and place the backup files on it. Also, do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit.	
	There are no backup files on the SD Memory Card.		Place the backup files in the specified folder on the SD Memory Card.			
	Either the backup files on the SD Memory Card are corrupted or required data is not in the backup files on the SD Memory Card.		Create the backup files again.			
	The unit version of the CPU Unit to which to restore the files is older than the unit version of the backup files on the SD Memory Card.		Replace the CPU Unit with a CPU Unit that has a unit version that is the same as or newer than the unit version of the CPU Unit that was used to create the backup files. Or, specify backup files with the correct unit version for the CPU Unit.		Make sure that the unit version of the CPU Unit and the unit version of the backup files are compatible.	
	The model of the CPU Unit to which to restore the files is not the same as the model of the CPU Unit of the backup files on the SD Memory Card.		Replace the CPU Unit with a CPU Unit that has the same model as the CPU Unit that was used to create the backup files. Or, specify backup files with the correct model for the CPU Unit.		Make sure that the model of the CPU Unit is the same as the model of the CPU Unit that was used to create the backup files.	
	Recovery was executed for the SD Memory Card.		If there are no backup files or no restore command file in the specified folder on the SD Memory Card, place the files in the folder again.		None	
	The CPU Unit is write-protected.		If you use the restore function, select the *Do not use* Option for the **Write protection at startup** setting of the CPU Unit.		If you use the restore function, select the *Do not use* Option for the **Write protection at startup** setting of the CPU Unit.	
	The settings in the restore command file (RestoreCommand.ini) are not correct.		Make sure that the required files are set to *"Yes"* in the restore command file.		Make sure that the required files are set to *"Yes"* in the restore command file.	
	A backup operation is in progress.		Wait for the backup operation to end and then perform the restore operation again.		Do not attempt to perform a restore operation during a backup operation.	

	Synchronization, online editing, or the Clear All Memory operation is in progress.	Wait for the synchronization, online editing, or the Clear All Memory operation to end and then perform the restore operation again.	Do not attempt to perform a restore operation during a synchronization, online editing, or the Clear All Memory operation.
	The online connection with the Sysmac Studio was disconnected.	Check the cable connections. Go offline and then go back online and execute the backup again.	Check the cable to see if it is disconnected or broken. Make sure the cable is connected properly.
	Reading the data for restoration failed because the SD Memory Card is faulty or not formatted correctly.	Perform the same corrective measures as for when the format of the SD Memory Card is not correct or the SD Memory Card is damaged.	Perform the same preventive measures as for the following events: SD Memory Card Invalid Format or Faulty SD Memory Card.
	The SD Memory Card is damaged.	If none of the above causes applies, replace the SD Memory Card.	Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit. Replace the SD Memory Card periodically according to the write life of the SD Memory Card.
	The database connection service version of the CPU Unit to which to restore the files is older than the database connection service version of the backup files on the SD Memory Card.	Replace the CPU Unit with a CPU Unit that has a database connection service version that is the same as or newer than the database connection service version of the CPU Unit that was used to create the backup files. Or, specify backup files with the correct database connection service version for the CPU Unit.	Make sure that the database connection service version of the CPU Unit and the database connection service version of the backup files are compatible.
	The robot version of the CPU Unit to which to restore the files is older than the robot version of the backup files on the SD Memory Card.	Replace the CPU Unit with a CPU Unit that has a robot version that is the same as or newer than the robot version of the CPU Unit that was used to create the backup files. Or, specify backup files with the correct robot version for the CPU Unit.	Make sure that the robot version of the CPU Unit and the robot version of the backup files are compatible.
	The CPU Unit failed to process the power OFF during the last power interruption.	Contact your OMRON representative or distributor.	None
	An unexpected error has occurred.		
	Check the followings for specification with system-defined variables.		
	Restore by system-defined variable is set to Do not use in the Controller Setup.	Set Restore by system-defined variable to Use in the Controller Setup.	Set Restore by system-defined variable to Use in the Controller Setup.
	Password of Restore by system-defined variable in the Controller Setup does not agree with the _Card1RestoreCmd.Password system-defined variable.	Set Password of Restore by system-defined variable in the Controller Setup to the _Card1RestoreCmd.Password system-defined variable.	Set Password of Restore by system-defined variable in the Controller Setup to the _Card1RestoreCmd.Password system-defined variable.
	The DIP switch on the CPU Unit is not set to allow starting the restore of SD Memory Card backups by specification with system-defined variables.	Turn OFF all pins on the DIP switch of the CPU Unit, and then start the restore of SD Memory Card backups by specification with system-defined variables.	Turn OFF all pins on the DIP switch of the CPU Unit, and then start the restore of SD Memory Card backups by specification with system-defined variables.
	There is no such folder as specified by the system-defined variable.	Create a folder specified by the system-defined variable and store the backup files in the folder.	Create a folder specified by the system-defined variable and store the backup files in the folder.

	Required files are not set to transfer in the setting of the system-defined variable.	Make sure that TRUE is set in the system-defined variable to transfer required files.	Make sure that TRUE is set in the system-defined variable to transfer required files.
	Also check the following when you use the Robot Integrated CPU Unit.		
	The SD Memory Card is write protected.	Remove write protection from the SD Memory Card.	Make sure that the SD Memory Card is not write protected.
	The capacity of the SD Memory Card is insufficient.	Replace the SD Memory Card for one with sufficient available space.	Use an SD Memory Card that has sufficient available space.
Attached information	Attached information 1: Operation type • 0101 hex: SD Memory Card to Controller for switch operation on front of CPU Unit • 0102 hex: SD Memory Card to Controller for specification with a system-defined variable • 0201 hex: Computer to Controller Attached Information 2: Error Details • 0001 hex: An SD Memory Card is not inserted. • 0002 hex: The SD Memory Card is faulty, the format of the SD Memory Card is not correct, or the SD Memory Card is not the correct type of card. • 0003 hex: The SD Memory Card is write protected (when the Robot Integrated CPU Unit is used). • 0004 hex: Recovery was executed for the SD Memory Card. • 0005 hex: There is not sufficient space available on the SD Memory Card (when the Robot Integrated CPU Unit is used). • 0101 hex: There is no such folder on the SD Memory Card as specified by the _Card1RestoreCmd.DirName system-defined variable. • 0102 hex: There are no backup files. • 0103 hex: The backup files are corrupted. • 0104 hex: The contents of the restore command file are not correct or required files are not set to transfer in the setting of the system-defined variable. • 0105 hex: The required transfer data is not in the backup file. • 0201 hex: The unit version of the CPU Unit is old. • 0202 hex: The model numbers of the CPU Unit are not the same. • 0203 hex: The CPU Unit is write-protected. • 0205 hex: Another backup operation is in progress. • 0206 hex: Synchronization, online editing, or the Clear All Memory operation is in progress. • 0209 hex: The CPU Unit failed to process the power OFF during the last power interruption. • 0211 hex: The database connection service or robot version of the CPU Unit is old. • 0212 hex: Restore by system-defined variable is set to Do not use in the Controller Setup. • 0213 hex: Password of Restore by system-defined variable in the Controller Setup does not agree with the _Card1RestoreCmd.Password system-defined variable. • 0214 hex: The DIP switch on the CPU Unit is not set to allow starting the restore of SD Memory Card backups by specification with system-defined variables. • 0301 hex: Reading data for restoration failed or the SD Memory Card is faulty. • 0501 hex: The online connection with the Sysmac Studio was disconnected. • 7F01 hex: An unexpected error has occurred.		
Precautions/ Remarks	None		

Event name	Restore Operation Failed			**Event code**	102C0000 hex	
Meaning	The restore operation ended in an error.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	During restore operation
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	---	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	_Card1RestoreSta		_sRESTORE_STA		SD Memory Card Restore Status	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	It was not possible to read the data to restore.		Format the SD Memory Card with the Sysmac Studio and then place the backup files on it.		Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit. Replace the SD Memory Card periodically according to the write life of the SD Memory Card.	
	The SD Memory Card was removed during a restore operation.		Insert an SD Memory Card that contains the backup files, and then execute the restore operation again.		Do not remove the SD Memory Card during the restore operation.	
	Failed to restore Unit or slave.		Refer to the corrections for the following events: CJ-series Unit Restore Operation Failed (102E0000 hex) or EtherCAT Slave Restore Operation Failed (10300000 hex).		Refer to the prevention information for the following events: CJ-series Unit Restore Operation Failed (102E0000 hex) or EtherCAT Slave Restore Operation Failed (10300000 hex).	
	The SD Memory Card is damaged.		If none of the above causes applies, replace the SD Memory Card.		Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit. Replace the SD Memory Card periodically according to the write life of the SD Memory Card.	
	An unexpected error has occurred.		Contact your OMRON representative or distributor.		None	
	Also check the following when you use the Robot Integrated CPU Unit.					
	The SD Memory Card is write protected.		Remove write protection from the SD Memory Card.		Make sure that the SD Memory Card is not write protected.	
	The capacity of the SD Memory Card is insufficient.		Replace the SD Memory Card for one with sufficient available space.		Use an SD Memory Card that has sufficient available space.	
	The number of files or directories in the SD Memory Card exceeded the maximum number supported by the file system of the SD Memory Card.		Delete unnecessary files or directories from the SD Memory Card.		Periodically delete unnecessary files and directories on the SD Memory Card.	

Attached information	Attached information 1: Operation type • 0101 hex: SD Memory Card to Controller for switch operation on front of CPU Unit • 0102 hex: SD Memory Card to Controller for specification with a system-defined variable • 0201 hex: Computer to Controller Attached Information 2: Error Details • 0001 hex: The SD Memory Card was removed. • 0003 hex: The SD Memory Card is write protected (when the Robot Integrated CPU Unit is used). • 0005 hex: There is not sufficient space available on the SD Memory Card (when the Robot Integrated CPU Unit is used). • 0006 hex: Too many files or directories (when the Robot Integrated CPU Unit is used). • 0102 hex: There are no backup files. • 0103 hex: The backup files are corrupted. • 0301 hex: Reading data for restoration failed or the SD Memory Card is faulty. • 0303 hex: The Unit or slave could not be restored. • 7F01 hex: An unexpected error has occurred.
Precautions/ Remarks	None

Event name	Online Edits Transfer Failure			**Event code**	103F0000 hex	
Description	Transferring the online edits failed.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	When online edits are transferred
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The number of variables exceeded the upper limit of variables.		Check the memory usage condition and design a program again so that the number of definitions for retained variables and non-retained variables does not exceed the upper limit of variables.		When you create a program, check the memory usage condition and design the program so that the number of definitions for retained variables and non-retained variables does not exceed the upper limit of variables.	
	The variable setting for Initial Value Specified/No Initial Value Specified was changed.		Transfer the online edits without changing the variable setting for Initial Value Specified/No Initial Value Specified.		Use synchronization function to change the variable setting for Initial Value Specified/No Initial Value Specified.	
Attached information	Attached information 1: Causes of failure • 0001 hex: The number of variables exceeded the upper limit of variables. • 0002 hex: The variable setting for Initial Value Specified/No Initial Value Specified was changed.					
Precautions/ Remarks						

Event name	Safety Data Logging Failed to Start			**Event code**	10630000 hex	
Description	Starting the safety data logging failed.					
Source	PLC Function Module		**Source details**	None	**Detection timing**	When safety data logging is started
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	An SD Memory Card is not inserted.		Insert an SD Memory Card.		Confirm that an SD Memory Card is inserted before you start logging.	
	There are no logging setting files.		Place logging setting files in the specified location "/SFLog/" of the SD Memory Card.		Place logging setting files in the specified location "/SFLog/".	
	The logging settings number of the logging setting file is duplicated.		Delete the unnecessary logging setting file.		Do not set the same logging settings number for more than one logging setting file.	
	The logging settings number of the logging setting file is outside of the specifications.		Create the logging setting file again in the project that was downloaded to the environment where the logging is executed.		Make sure to always transfer the logging settings after you change the project on the Sysmac Studio. Do not edit the logging setting file generated by the Sysmac Studio by any other means.	
	The logging setting files are invalid.		Create logging setting files again in the project transferred to the logging execution environment.		If you make changes to a project in the Sysmac Studio, transfer the logging settings again. Do not edit the logging setting files generated by the Sysmac Studio by other methods.	
	Not all of safety master connections are established.		Establish all safety master connections before attempting to start safety data logging.		Establish all safety master connections before attempting to start safety data logging.	
	Impossible to access a logging target variable that is specified in the logging setting file.		Create the logging setting file again in the project that was downloaded to the environment where the logging is executed.		Make sure to always transfer the logging settings after you change the project on the Sysmac Studio. Do not edit the logging setting file generated by the Sysmac Studio by any other means.	
Attached information	Attached information 1: Causes of failure • 0001 hex: An SD Memory Card is not inserted. • 0002 hex: There are no logging setting files. • 0003 hex: The logging settings number is duplicated. • 0004 hex: The logging settings number is outside of the specifications. • 0005 hex: The logging setting file is invalid. • 0006 hex: Safety master connections are not established. • 0007 hex: Impossible to access a logging target variable.					
Precautions/ Remarks	You cannot start safety data logging before safety validation is performed on the Safety CPU Unit.					

Event name	Safety Data Log File Save Failed			Event code	10640000 hex	
Description	Saving the log file for safety data logging failed.					
Source	PLC Function Module		Source details	None	Detection timing	When safety data logging file is saved
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The SD Memory Card was removed after the start of logging.		Insert an SD Memory Card.		Do not remove the SD Memory Card during logging execution.	
	The SD Memory Card is write-protected.		Remove write protection from the SD Memory Card.		Remove write protection from the SD Memory Card before you start logging.	
	The capacity of the SD Memory Card is insufficient.		Replace the SD Memory Card with one with sufficient available space.		Use an SD Memory Card that has sufficient available space.	
	The maximum number of files for an SD Memory Card was exceeded.		Delete files stored on the SD Memory Card to reduce the number of files.		Delete files periodically to reduce the number of files.	
	The SD Memory Card is damaged.		If none of the above causes applies, replace the SD Memory Card.		Replace the SD Memory Card periodically according to the write life of the SD Memory Card.	
Attached information	Attached information 1: Causes of failure • 0001 hex: An SD Memory Card is not inserted. • 0002 hex: The SD Memory Card is write-protected. • 0003 hex: The capacity of the SD Memory Card is insufficient. • 0004 hex: The maximum number of files was exceeded. • 0005 hex: Other causes Attached information 2: The name of the log file that failed to be saved					
Precautions/ Remarks	None					

Event name	PLC System Information			Event code	40140000 hex	
Meaning	This event provides internal information from the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.		---		---	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	Safe Mode			Event code	40170000 hex	
Meaning	The Controller started in Safe Mode.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON or Controller reset
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Stops.	Operation	---		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The Controller started in Safe Mode.		---		---	
Attached information	None					
Precautions/ Remarks	If the Controller is started when the CPU Unit is in Safe Mode, the CPU Unit will start in PROGRAM mode even if the startup mode is set to RUN mode.					

Event name	NX Message Communications Error			Event code	80230000 hex	
Meaning	An error has occurred in message communications.					
Source	PLC Function Module, EtherCAT Master Function Module, EtherNet/IP Function Module, or NX Bus Function Module		Source details	None	Detection timing	During NX message communications
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	---		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The communications cable is broken.		Check the communications cable and replace it if it is broken.		Check the communications cable to see if it is operating properly.	
	The communications cable connector is disconnected.		Reconnect the connector and make sure it is mated correctly.		Make sure the communications cable is connected properly.	
	The NX message communications load is high.		Reduce the number of times that instructions are used to send NX messages. Or, increase the value of the *TimeOut* input variable to the instruction. If more than one copy of the Sysmac Studio is connected, reduce the frequency of simultaneous operations.		Reduce the number of times that instructions are used to send NX messages. Or, increase the value of the *TimeOut* input variable to the instruction. If more than one copy of the Sysmac Studio is connected, reduce the frequency of simultaneous operations.	
Attached information	Attached information 1: System information Attached information 2: Type of communications • 0: NX bus • 1: EtherCAT • 65,535: Unit internal communications (routing)					
Precautions/ Remarks	None					

Event name	Safety Data Logging Aborted			Event code	90470000 hex	
Description	The execution of safety data logging was aborted.					
Source	PLC Function Module		Source details	None	Detection timing	During the execution of safety data logging
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_PLC_SFLogSta		ARRAY[0..1] OF _sSFLOG_STA		Safety Data Logging Status	
Cause and correction	Assumed cause		Correction		Prevention	
	The execution of safety data logging was aborted by a service switch operation.		---		---	
	Either a communications error on the safety master connections occurred or the Safety CPU Unit entered an operating mode where it could not continue safety process data communications.		Check the safety process data communications related event that occurred most recently, and perform the required actions and corrections. Alternatively, change the Safety CPU Unit operating mode so that it can perform safety process data communications.		Make sure that safety process data communications are not interrupted unintentionally when you start safety data logging.	
	The NX bus was restarted.		---		---	
	The Controller Setup or program was changed.		---		---	
Attached information	Attached information 1: Setting number for the aborted logging Attached information 2: The output log file name Attached information 3: Cause for the interruption • 1: A service switch was pressed. • 2: Safety master connections are not established. • 3: The NX bus was restarted. • 4: The Controller Setup or program was changed.					
Precautions/ Remarks	• The aborted safety data logging does not restart automatically even if the causes of aborting are removed. • The saved log data only includes data that was logged before the occurrence of aborting, regardless of the post-trigger ratio setting.					

Event name	PLC System Information			Event code	40150000 hex	
Meaning	This event provides internal information from the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.		---		---	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	PLC System Information			Event code	44430000 hex	
Meaning	This event provides internal information from the PLC Function Module.					
Source	PLC Function Module		Source details	None	Detection timing	Continuously
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	This event provides internal information from the PLC Function Module. It is recorded to provide additional information for another event.		---		---	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	Clock Changed			Event code	90010000 hex	
Meaning	The clock time was changed.					
Source	PLC Function Module		Source details	None	Detection timing	Commands from user
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_CurrentTime		DATE_AND_TIME		System Time	
Cause and correction	Assumed cause		Correction		Prevention	
	The clock time was changed.		---		---	
Attached information	Attached Information 1: Connection method • 1: Direct Connection via USB • 2: Direct Ethernet connection • 3: Remote USB connection or Ethernet hub connection Attached information 2: When attached information 1 is 2 or 3, the connection source IP address is given. When connection is made through proxy, proxy IP address is given. Attached information 3: Clock time before change					
Precautions/ Remarks	A change of clock time caused by the NTP function or the Set Time instruction (SetTime) of NTP is not recorded in the event log. The time stamp for this event will be for the time after the change.					

Event name	Time Zone Changed			Event code	90020000 hex	
Meaning	The time zone was changed.					
Source	PLC Function Module		Source details	None	Detection timing	When downloading
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_CurrentTime		DATE_AND_TIME		System Time	
Cause and correction	Assumed cause		Correction		Prevention	
	The time zone was changed.		---		---	
Attached information	Attached Information 1: Connection method • 1: Direct Connection via USB • 2: Direct Ethernet connection • 3: Remote USB connection or Ethernet hub connection Attached information 2: When attached information 1 is 2 or 3, the connection source IP address is given. When connection is made through proxy, proxy IP address is given.					
Precautions/ Remarks	None					

Event name	User Program/Controller Configurations and Setup Downloaded			Event code	90050000 hex	
Meaning	The user program and the Controller configurations and setup were downloaded.					
Source	PLC Function Module		Source details	None	Detection timing	During user program/Controller configurations and setup download
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Operation starts according to the user program and the Controller setup data that were downloaded.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The user program and the Controller configurations and setup were downloaded.		---		---	
Attached information	Attached Information 1: Connection method • 1: Direct USB connection • 2: Direct Ethernet connection • 3: Remote USB connection or Ethernet hub connection Attached information 2: When attached information 1 is 2 or 3, the connection source IP address is given. When connection is made through proxy, proxy IP address is given. Attached information 3: Device Output Hold Status • 1: Retained. • 2: Not retained.					
Precautions/ Remarks	None					

Event name	Memory All Cleared			Event code	900B0000 hex	
Meaning	All of memory was cleared.					
Source	PLC Function Module		Source details	None	Detection timing	Commands from user
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	---	Operation	Operation returns to the factory state.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A user with Administrator rights cleared all of the memory.		---		---	
Attached information	Attached Information 1: Connection method • 1: Direct Connection via USB • 2: Direct Ethernet connection • 3: Remote USB connection or Ethernet hub connection Attached information 2: When attached information 1 is 2 or 3, the connection source IP address is given. When connection is made through proxy, proxy IP address is given.					
Precautions/ Remarks	None					

Event name	Event Log Cleared			Event code	900C0000 hex	
Meaning	The event log was cleared.					
Source	PLC Function Module		Source details	None	Detection timing	Commands from user
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The event log was cleared by the user.		---		---	
Attached information	Attached Information 1: Connection method • 1: Direct Connection via USB • 2: Direct Ethernet connection • 3: Remote USB connection or Ethernet hub connection Attached information 2: When attached information 1 is 2 or 3, the connection source IP address is given. When connection is made through proxy, proxy IP address is given. Attached information 3: Cleared events • 0: Logs for all categories were cleared. • 1: The system event log was cleared. • 2: The access event log was cleared. • 100: The user-defined event log was cleared.					
Precautions/ Remarks	None					

Event name	Power Turned ON			Event code	90110000 hex	
Meaning	The power supply was turned ON.					
Source	PLC Function Module		Source details	None	Detection timing	At power ON
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	---	Operation	Operation starts.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The power supply was turned ON.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Power Interrupted			Event code	90120000 hex	
Meaning	The power supply was interrupted.					
Source	PLC Function Module		Source details	None	Detection timing	At power interruption
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Stops.	Operation	All operations stop.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The power supply was interrupted.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Reset Executed			Event code	90150000 hex	
Meaning	A reset was executed.					
Source	PLC Function Module		Source details	None	Detection timing	Commands from user
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	---	Operation	Operation is started after a reset is executed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A reset command was received.		---		---	
Attached information	Attached Information 1: Connection method • 1: Direct Connection via USB • 2: Direct Ethernet connection • 3: Remote USB connection or Ethernet hub connection Attached information 2: When attached information 1 is 2 or 3, the connection source IP address is given. When connection is made through proxy, proxy IP address is given.					
Precautions/ Remarks	None					

Event name	All Controller Errors Cleared			Event code	90180000 hex	
Meaning	All current errors were cleared.					
Source	PLC Function Module		Source details	None	Detection timing	Commands from user
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Clearing all errors for which the causes have been removed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The user cleared all current errors.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Backup Started			Event code	901A0000 hex	
Meaning	A backup operation was started.					
Source	PLC Function Module		Source details	None	Detection timing	At start of backup operation
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A backup operation was started.		---		---	
Attached information	Attached information 1: Operation type • 0101 hex: Controller to SD Memory Card for switch operation on front of CPU Unit • 0102 hex: Controller to SD Memory Card for system-defined variable operation • 0103 hex: Controller to SD Memory Card for instruction from Sysmac Studio or function module specific trigger) • 0104 hex: Controller to SD Memory Card for instruction operation • 0201 hex: Controller to computer					
Precautions/ Remarks	None					

Event name	Backup Completed			Event code	901B0000 hex	
Meaning	The backup operation ended normally.					
Source	PLC Function Module		Source details	None	Detection timing	At end of normal backup operation
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The backup operation ended normally.		---		---	
Attached information	Attached information 1: Operation type • 0101 hex: Controller to SD Memory Card for switch operation on front of CPU Unit • 0102 hex: Controller to SD Memory Card for system variable operation • 0103 hex: Controller to SD Memory Card for instruction from Sysmac Studio or function module specific trigger) • 0104 hex: Controller to SD Memory Card for instruction operation. • 0201 hex: Controller to computer					
Precautions/ Remarks	None					

Event name	Restore Operation Started			Event code	901C0000 hex	
Meaning	A restore operation started.					
Source	PLC Function Module		Source details	None	Detection timing	At start of restore operation
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	---	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A restore operation started.		---		---	
Attached information	Attached information 1: Operation type • 0101 hex: SD Memory Card to Controller for switch operation on front of CPU Unit • 0102 hex: SD Memory Card to Controller for specification with a system-defined variable • 0201 hex: Computer to Controller					
Precautions/ Remarks	None					

Event name	Restore Operation Completed			Event code	901D0000 hex	
Meaning	The restore operation ended normally.					
Source	PLC Function Module		Source details	None	Detection timing	At end of normal restore operation
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	---	Operation	Operation does not start after the completion of a restore operation. To start operation according to the restored user program and settings, turn OFF the power supply to the Controller, turn OFF all pins on the DIP switch on the CPU Unit, and then turn ON the power supply again.		
System-defined variables	Variable		Data type		Name	
	_Card1RestoreSta		_sRESTORE_STA		SD Memory Card Restore Status	
Cause and correction	Assumed cause		Correction		Prevention	
	The restore operation ended normally.		---		---	
Attached information	Attached information 1: Operation type • 0101 hex: SD Memory Card to Controller for switch operation on front of CPU Unit • 0102 hex: SD Memory Card to Controller for specification with a system-defined variable • 0201 hex: Computer to Controller					
Precautions/ Remarks	None					

Event name	Safety Data Logging Started			Event code	90460000 hex	
Description	Safety data logging was started.					
Source	PLC Function Module		Source details	None	Detection timing	When safety data logging is started
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_PLC_SFLogSta		ARRAY[0..1] OF _sSFLOG_STA		Safety Data Logging Status	
Cause and correction	Assumed cause		Correction		Prevention	
	Safety data logging was started because the start conditions were met.		---		---	
Attached information	Attached information 1: Setting number for the started logging					
Precautions/ Remarks	None					

Event name	Safety Data Logging Completed			Event code	90480000 hex	
Description	The execution of safety data logging was completed because the trigger conditions were met.					
Source	PLC Function Module		Source details	None	Detection timing	When safety data logging is completed
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_PLC_SFLogSta		ARRAY[0..1] OF _sSFLOG_STA		Safety Data Logging Status	
Cause and correction	Assumed cause		Correction		Prevention	
	The trigger condition that is specified in the Safety Data Logging Settings is met, and safety data logging ends.		---		---	
Attached information	Attached information 1: Setting number for the completed logging Attached information 2: The output log file name					
Precautions/ Remarks	If more than one safety data logging is executed, do not remove or insert the SD Memory Card until all the safety data logging executions are completed and the data is saved to the SD Memory Card.					

NX Bus Function Module Error Descriptions

● Errors Related to the NX Bus

Event name	NX Bus Controller Error			**Event code**	04100000 hex	
Meaning	An error occurred in the NX bus.					
Source	NX Bus Function Module		**Source details**	Master	**Detection timing**	At CPU Unit power ON, at Controller reset, or during NX bus communications
Error attributes	**Level**	Partial fault	**Recovery**	Cycle the power supply to the CPU Unit or reset the Controller.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	I/O communications will not operate and message communications cannot be performed.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	An I/O communications error occurred between the CPU Unit and the NX Unit.		Cycle the power supply to the CPU Unit. If this error persists, replace the CPU Unit.		None	
Attached information	Attached information 1: System information					
Precautions/ Remarks	None					

Event name	NX Bus Hardware Error			Event code	04110000 hex	
Meaning	A hardware error was detected in the NX Bus Function Module.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Partial fault	Recovery	Cycle the power supply to the CPU Unit or reset the Controller.	Log category	System
Effects	User program	Continues.	Operation	I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A hardware error related to the NX bus was detected.		Cycle the power supply to the CPU Unit. If this error persists, replace the CPU Unit.		None	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	NX Bus Memory Check Error			Event code	10600000 hex	
Meaning	An error was detected in the internal memory check for the NX Bus Function Module.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Partial fault	Recovery	Cycle the power supply to the CPU Unit or reset the Controller.	Log category	System
Effects	User program	Continues.	Operation	I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error was detected in the memory check for the internal protection circuit.		Cycle the power supply to the CPU Unit. If this error persists, replace the CPU Unit.		None	
Attached information	Attached information 1: System information					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Failed to Read NX Unit Operation Settings</td><td>Event code</td><td colspan="2">10610000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">Reading the NX Unit operation settings failed.
Cycle the power supply to the CPU Unit to restore the previous normally-saved settings.</td></tr>
<tr><td>Source</td><td colspan="2">NX Bus Function Module</td><td>Source details</td><td>Master</td><td>Detection timing</td><td>At CPU Unit power ON, at Controller reset, or at NX bus restart</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Partial fault</td><td>Recovery</td><td>Cycle the power supply to the CPU Unit, reset the Controller, or restart the NX bus.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">I/O communications will not operate, but message communications can be performed.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The NX Unit operation settings are not saved normally in the CPU Unit.</td><td colspan="2">Check the NX Unit operation settings and correct the settings.</td><td colspan="2">Do not turn OFF the power supply to the CPU Unit while transfer of the Unit operation settings for the CPU Unit or execution of the NX_SaveParam instruction is in progress.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: System information</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Number of Mountable NX Units Exceeded			Event code	24D00000 hex	
Meaning	The number of mounted NX Units exceeds the specified value for the CPU Unit.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, or at NX bus restart
Error attributes	Level	Partial fault	Recovery	Cycle the power supply to the CPU Unit or reset the Controller.	Log category	System
Effects	User program	Continues.	Operation	• For NX Units within the range of the number of mountable Units, I/O communications will not operate, but message communications can be performed. • For NX Units outside the range of the number of mountable Units, I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	More than the maximum number of NX Units are mounted on the CPU Unit.		Keep the number of NX Units mounted on the CPU Unit at the specified number or less.		Mount the specified number of NX Units or less.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Total I/O Data Size in NX Units Excessive		Event code	24D20000 hex	
Meaning	The total size of I/O data in the mounted NX Units exceeds the maximum specified value for the CPU Unit.				
Source	NX Bus Function Module	Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, or at NX bus restart
Error attributes	Level: Partial fault	Recovery	Cycle the power supply to the CPU Unit or reset the Controller.	Log category	System
Effects	User program: Continues.	Operation	I/O communications will not operate, but message communications can be performed.		

System-defined variables	Variable	Data type	Name
	None	---	---

Cause and correction	Assumed cause	Correction	Prevention
	The total size of I/O data in the mounted NX Units exceeds the maximum specified value for the CPU Unit.	Reduce the number of NX Units mounted on the CPU Unit to keep the total size of I/O data at the maximum specified value or less.	Reduce the number of NX Units mounted on the CPU Unit to keep the total size of I/O data at the maximum specified value or less.

Attached information	None
Precautions/ Remarks	None

Event name	NX Unit Version Not Matched			Event code	35900000 hex	
Meaning	There is a mounted NX Unit with a unit version earlier than that in the Unit configuration information registered in the CPU Unit.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, or at NX bus restart
Error attributes	Level	Partial fault	Recovery	Cycle the power supply to the CPU Unit, reset the Controller, or restart the NX bus.	Log category	System
Effects	User program	Continues.	Operation	• For NX Units with this error, I/O communications will not operate and message communications cannot be performed. • For NX Units without this error, I/O communications will not operate, but message communications can be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The unit version of an NX Unit mounted in the actual configuration is earlier than that in the Unit configuration information registered in the CPU Unit.		To match the Unit configuration information with the actual configuration, download the Unit configuration information that contains the unit version of the NX Unit mounted in the actual configuration to the CPU Unit. To match the actual configuration with the Unit configuration information, replace the NX Unit in the actual configuration with an NX Unit with a unit version later than that in the Unit configuration information.		Download Unit configuration information for which you confirmed that the comparison result showed *Not compatible* in the Compare and Merge Window of the Sysmac Studio to the CPU Unit.	
Attached information	Attached information 1: Unit number of the NX Unit where the error occurred Attached information 2: Unit version in the Unit configuration information of the NX Unit where the error occurred					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Unregistered NX Unit Mounted</td><td>Event code</td><td colspan="2">35910000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">There is a mounted NX Unit that does not exist in the Unit configuration information registered in the CPU Unit. If there are more than one NX Unit relevant to this event, only the NX Unit that is nearest to the CPU Unit is registered with the event.</td></tr>
<tr><td>Source</td><td colspan="2">NX Bus Function Module</td><td>Source details</td><td>Master</td><td>Detection timing</td><td>At CPU Unit power ON, at Controller reset, or at NX bus restart</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Partial fault</td><td>Recovery</td><td>Cycle the power supply to the CPU Unit, reset the Controller, or restart the NX bus.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">• For NX Units with this error, I/O communications will not operate and message communications cannot be performed.
• For NX Units without this error, I/O communications will not operate, but message communications can be performed.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">There is a mounted Unit that does not exist in the Unit configuration information registered in the CPU Unit.</td><td colspan="2">To match the Unit configuration information with the actual configuration, download to the CPU Unit the Unit configuration information to which you added the relevant NX Unit. To match the actual configuration with the Unit configuration information, remove the relevant NX Unit.</td><td colspan="2" rowspan="2">Match the project downloaded to the CPU Unit with the system configuration.</td></tr>
<tr><td colspan="2">There is a mounted Unit in which the NX Unit Mounting Setting is set to Disabled.</td><td colspan="2">To match the Unit configuration information with the actual configuration, download to the CPU Unit the Unit configuration information in which the NX Unit Mounting Setting for the relevant NX Unit is set to Enabled. To match the actual configuration with the Unit configuration information, remove the relevant NX Unit.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Mounting position of the NX Unit where the error occurred</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	NX Unit Serial Number Mismatch			Event code	35930000 hex	
Meaning	There is a mounted NX Unit with a serial number different from that in the Unit configuration information registered in the CPU Unit.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, or at NX bus restart
Error attributes	Level	Partial fault	Recovery	Cycle the power supply to the CPU Unit, reset the Controller, or restart the NX bus.	Log category	System
Effects	User program	Continues.	Operation	• For NX Units with this error, I/O communications will not operate and message communications cannot be performed. • For NX Units without this error, I/O communications will not operate, but message communications can be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	One or more NX Units with the serial number set in the Unit configuration information registered in the CPU Unit are not mounted.		To match the actual configuration with the Unit configuration information, match the serial number of the relevant NX Unit . To match the Unit configuration information with the actual configuration, download the Unit configuration information with the serial number of the relevant NX Unit to the CPU Unit.		Read the serial numbers of the actually mounted Units into a project in the Sysmac Studio before you set the Serial Number Verification setting to verify the serial numbers.	
Attached information	Attached information 1: Unit number of the NX Unit where the error occurred Attached information 2: Serial number in the Unit configuration information of the NX Unit where the error occurred					
Precautions/ Remarks	None					

Event name	NX Bus Function Processing Error			Event code	44440000 hex	
Meaning	A fatal error was detected in the NX Bus Function Module.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Partial fault	Recovery	Cycle the power supply to the CPU Unit.	Log category	System
Effects	User program	Continues.	Operation	I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An error occurred in the software.		Contact your OMRON representative.		None	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	NX Bus I/O Communications Stopped Due to Another Event			Event code	85540000 hex	
Meaning	The I/O communications on the NX bus were stopped because an error that prevents I/O communications on the NX bus occurred.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Partial fault	Recovery	Error reset	Log category	System
Effects	User program	Continues.	Operation	I/O communications will not operate, but message communications can be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The I/O communications were stopped because a minor fault error (another event) that triggers fail-soft operation occurred when the Fail-soft Operation Setting is *Stop*.		Eliminate errors for other events that causes this event.		To continue the I/O communications when an error that triggers fail-soft operation is encountered, change the Fail-soft Operation Setting to *Fail-soft*.	
	The I/O communications were stopped because the *Registered NX Unit Not Mounted* event occurred and the actual configuration prevents I/O communications from starting.					
Attached information	Attached information 1: Event code that caused this event Attached information 2: System information					
Precautions/ Remarks	None					

Event name	Registered NX Unit Not Mounted			Event code	35920000 hex	
Meaning	One or more NX Units set in the Unit configuration information registered in the CPU Unit are not mounted. If there are more than one NX Unit relevant to this event, only the NX Unit that is nearest to the CPU Unit is registered with the event.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, or at NX bus restart
Error attributes	Level	Minor fault	Recovery	Cycle the power supply to the CPU Unit, reset the Controller, or restart the NX bus.	Log category	System
Effects	User program	Continues.	Operation	For NX Units with this error, I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	One or more NX Units set in the Unit configuration information registered in the CPU Unit are not mounted.		To match the actual configuration with the Unit configuration information, mount the relevant NX Unit. To match the Unit configuration information with the actual configuration, download to the CPU Unit the Unit configuration information from which you deleted the relevant NX Unit.		Match the project downloaded to the CPU Unit with the system configuration.	
	The power supply to the Additional NX Unit Power Supply Unit is not turned ON.		Turn ON the power supply to the Additional NX Unit Power Supply Unit.		Use the same Unit power supply to supply the Unit power to the CPU Rack.	
Attached information	Attached information 1: Unit number of the NX Unit where the error occurred					
Precautions/ Remarks	None					

Event name	NX Bus Communications Error			Event code	85500000 hex	
Meaning	A communications error that prevents normal NX bus communications was detected. If there are more than one NX Unit relevant to this event, only the NX Unit that is nearest to the CPU Unit is registered with the event.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Minor fault	Recovery	Cycle the power supply to the CPU Unit, reset the Controller, or restart the NX bus.	Log category	System
Effects	User program	Continues.	Operation	For NX Units located outside the NX Unit where an error occurred, I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The NX bus connector contact is faulty due to vibration or shock.		Mount the NX Units and End Cover securely and secure them with End Plates.		Perform installation according to the user's manual	
	Excessive noise is applied to the NX bus connector.		Implement noise countermeasures according to the user's manual.			
	An NX Unit was removed.		Mount the removed NX Unit again.			
	An error occurred in an NX Unit.		Cycle the power supply to the relevant NX Unit. If this error persists, replace the NX Unit.		None	
Attached information	Attached information 1: Unit number of the NX Unit where the error occurred					
Precautions/ Remarks	None					

Event name	NX Unit Communications Timeout			Event code	85510000 hex	
Meaning	An error occurred in I/O data communications with the NX Units.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Minor fault	Recovery	Error reset	Log category	System
Effects	User program	Continues.	Operation	For NX Units with this error, I/O communications will not operate, but message communications can be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An NX Bus Communications Error has occurred.		Correct the NX Bus Communications Error.		Take preventive measures against the NX Bus Communications Error.	
	An error occurred in an NX Unit.		Cycle the power supply to the relevant NX Unit. If this error persists, replace the NX Unit.		None	
Attached information	Attached information 1: Unit number of the NX Unit where the error occurred Attached information 2: System information					
Precautions/ Remarks	None					

Event name	NX Unit Initialization Error			Event code	85520000 hex	
Meaning	Initializing an NX Unit failed.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, at NX bus restart, or at error reset
Error attributes	Level	Minor fault	Recovery	Error reset	Log category	System
Effects	User program	Continues.	Operation	For NX Units with this error, I/O communications will not operate, but message communications can be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Initialization with the Unit configuration information registered in the CPU Unit failed.		Connect the Sysmac Studio and reconfigure the Unit configuration information in the CPU Unit.		Download the Unit configuration information to the CPU Unit and the NX Unit.	
	An NX Bus Communications Error has occurred.		Correct the NX Bus Communications Error.		Take preventive measures against the NX Bus Communications Error.	
	The Channel Enable/Disable Setting for all channels of the Analog Unit are set to *Disable*.		Set the Channel Enable/Disable Setting to *Enable* for at least one channel.		For an Analog Unit, set the Channel Enable/Disable Setting to *Enable* for at least one channel.	
	Initialization of an NX Unit failed.		Cycle the power supply to the relevant NX Unit. If this error persists, replace the NX Unit.		For an Analog Unit, set the Channel Enable/Disable Setting to *Enable* for at least one channel.	
Attached information	Attached information 1: Unit number of the NX Unit where the error occurred Attached information 2: System information					
Precautions/ Remarks	None					

Event name	NX Unit Startup Error			Event code	85530000 hex	
Meaning	Starting an NX Unit failed.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON, at Controller reset, at NX bus restart, or at error reset
Error attributes	Level	Minor fault	Recovery	Cycle the power supply to the CPU Unit or reset the Controller.	Log category	System
Effects	User program	Continues.	Operation	For NX Units with this error, I/O communications will not operate and message communications cannot be performed.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A startup error occurred in an NX Unit.		Cycle the power supply to the relevant NX Unit. If this error persists, replace the NX Unit.		None	
Attached information	Attached information 1: Mounting position of the NX Unit where the error occurred Attached information 2: System information					
Precautions/ Remarks	None					

Event name	NX Unit Backup Failed			Event code	103C0000 hex	
Meaning	The backup operation for an NX Unit ended in an error.					
Source	NX Bus Function Module		Source details	Master	Detection timing	When backup is executed
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	There is also another error related to the NX Bus Function Module.		Check errors related to the NX Bus Function Module and perform the required corrections.		Back up the data when there are no NX bus errors.	
	An NX Bus Communications Error has occurred.		Implement countermeasures against the NX Bus Communications Error.			
	Backup data cannot be received from an NX Unit.		Reset the error for the relevant NX Unit.			
Attached information	Attached Information 1: Error Location • 0: NX bus master • 1 or higher: Unit number of the NX Unit Attached Information 2: Cause of the error • 1: There is an error related to the NX Bus Function Module. • 2: Communications with an NX Unit failed. Attached information 3: System information					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">NX Unit Restore Operation Failed</td><td>Event code</td><td colspan="2">103D0000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">The restore operation for an NX Unit ended in an error.</td></tr>
<tr><td>Source</td><td colspan="2">NX Bus Function Module</td><td>Source details</td><td>Master</td><td>Detection timing</td><td>During restore operation</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">Not affected.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="5">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">There is also another error related to the NX Bus Function Module.</td><td colspan="2">Check errors related to the NX Bus Function Module and perform the required corrections.</td><td colspan="2" rowspan="4">Restore the data when there are no NX bus errors.</td></tr>
<tr><td colspan="2">An NX Bus Communications Error has occurred.</td><td colspan="2">Implement countermeasures against the NX Bus Communications Error.</td></tr>
<tr><td colspan="2">The backup data cannot be sent to an NX Unit.</td><td colspan="2">Reset the error for the relevant NX Unit.</td></tr>
<tr><td colspan="2">The Unit configuration in the backup file does not agree with the actual Unit configuration.</td><td colspan="2">Use an NX Unit revision that is the same or higher than the revision used when the data was backed up. If you replace a slave with the Serial Number Check Method set to Setting = Actual device, do not use the restore function. Instead, change the network configuration from the Sysmac Studio, download the network configuration, and then transfer the slave parameters.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached Information 1: Error Location
• 0: NX bus master
• 1 or higher: Unit number of the NX Unit
Attached Information 2: Cause of the error
• 1: There is an error related to the NX Bus Function Module.
• 2: Communications with an NX Unit failed.
• 3: The Unit configuration in the backup data does not agree with the actual Unit configuration.
Attached information 3: System information</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	NX Unit Event Log Save Error			Event code		10620000 hex
Meaning	Saving or reading the NX Unit event log failed. Continuing to operate with this error may result in no event log saved at CPU Unit power OFF although it has no effect on the control function.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At CPU Unit power ON or at Controller reset
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Part or all of the past event log cannot be read.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Data in the NX Unit event log area are invalid.		If this error persists even after you cycle the power supply to the CPU Unit, a hardware failure may occur in the NX Unit event log area. Replace the CPU Unit if you use the event logs in the CPU Unit.		None	
Attached information	Attached information 1: System information					
Precautions/ Remarks	None					

Event name	NX Bus System Information			Event code		44450000 hex
Meaning	This event provides internal information from the NX Bus Function Module.					
Source	NX Bus Function Module		Source details	Master	Detection timing	Continuously
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	This event provides internal information from the NX Bus Function Module.		---		---	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	NX Bus Restart Executed			Event code	95800000 hex	
Meaning	An NX bus restart was executed.					
Source	NX Bus Function Module		Source details	Master	Detection timing	At NX bus restart or at NX Unit restart
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_NXB_UnitIOActiveTbl		ARRAY [0..32] OF BOOL		NX Unit I/O Data Active Status	
	_NXB_UnitMsgActiveTbl		ARRAY [0..32] OF BOOL		NX Unit Message Enabled Status	
Cause and correction	Assumed cause		Correction		Prevention	
	An NX bus restart command was received.		---		---	
Attached information	Attached information 1: Type of restart • 0: The NX bus was restarted • 1: An NX Unit was restarted Attached information 2: Unit number of the Unit that executed a restart • 0: NX bus master • 1 or higher: NX Unit					
Precautions/ Remarks	None					

Event name	NX Unit Memory All Cleared			Event code	95810000 hex	
Description	The NX Unit operation settings were initialized.					
Source	NX Bus Function Module		Source details	Master	Detection timing	When NX Unit memory is all cleared
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	_NXB_UnitIOActiveTbl		ARRAY [0..32] OF BOOL		NX Unit I/O Data Active Status	
	_NXB_UnitMsgActiveTbl		ARRAY [0..32] OF BOOL		NX Unit Message Communications Enabled Status	
Cause and correction	Assumed cause		Correction		Prevention	
	A Clear All Memory operation for an NX Unit was received.		Make the Unit operation settings as necessary for the NX Unit for which you executed Clear All Memory operation. If the attached information 2 is not 0, check any minor fault or higher-level error that occurrs in the NX Bus Function Module and the NX Unit, and make the required corrections.		---	
Attached information	Attached information 1: Unit number of the NX Unit for which you executed Clear All Memory Attached information 2: Execution results of Clear All Memory operation • 0: All cleared • 1: Hardware error • 2: Initialization failure • 3: Initialization not possible					
Precautions/ Remarks	None					

EtherNet/IP Function Module Error Descriptions

● Built-in EtherNet/IP Port on CPU Unit

Event name	EtherNet/IP Processing Error			**Event code**	14220000 hex	
Meaning	A fatal error was detected in the EtherNet/IP Function Module.					
Source	EtherNet/IP Function Module		**Source details**	Communications port	**Detection timing**	Continuously
Error attributes	**Level**	Partial fault	**Recovery**	Cycle the power supply.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	EtherNet/IP communications will not operate.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	OFF		Lights.		---	
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Hardware has failed.		Replace the CPU Unit.		None	
Attached information	Attached information 1: System information Attached information 2: System information Attached information 3: System information Attached information 4: System information					
Precautions/ Remarks	None					

Event name	Communications Controller Error			**Event code**	04210000 hex	
Meaning	A hardware error was detected in the communications controller of the built-in EtherNet/IP port.					
Source	EtherNet/IP Function Module		**Source details**	Communications port 1 or 2	**Detection timing**	Continuously
Error attributes	**Level**	Minor fault	**Recovery**	Cycle the power supply.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	EtherNet/IP communications are not possible for the relevant communications port.		
System-defined variables	**Variable**		**Data type**		**Name**	
	_EIP1_LanHwErr		BOOL		Port1 Communications Controller Error	
	_EIP2_LanHwErr		BOOL		Port2 Communications Controller Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Hardware error in the communications controller		Replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	After the _EIP1_LanHwErr or _EIP2_LanHwErr system-defined variable changes to TRUE, it will not change to FALSE unless the power supply to the Controller is cycled.					

Event name	Identity Error			Event code	14210000 hex	
Meaning	The CIP identity information in non-volatile memory was not read correctly.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	CIP/CIP1/CIP2	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port.		
System-defined variable	Variable		Data type		Name	
	_EIP_IdentityErr		BOOL		Identity Error	
	_EIP1_IdentityErr		BOOL		CIP Communications1 Identity Error	
	_EIP2_IdentityErr		BOOL		CIP Communications2 Identity Error	
Cause and correction	Assumed cause		Correction		Prevention	
	Non-volatile memory failure		Replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	MAC Address Error			Event code	14230000 hex	
Meaning	The MAC address in non-volatile memory was not read correctly.					
Source	EtherNet/IP Function Module		Source details	Communications port 1 or 2	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port.		
System-defined variables	Variable		Data type		Name	
	_EIP1_MacAdrErr		BOOL		Port 1 MAC Address Error	
	_EIP2_MacAdrErr		BOOL		Port2 MAC Address Error	
Cause and correction	Assumed cause		Correction		Prevention	
	Non-volatile memory failure		Replace the CPU Unit.		None	
Attached information	None					
Precautions/ Remarks	After the _EIP1_MacAdrErr or _EIP2_MacAdrErr system-defined variable changes to TRUE, it will not change to FALSE unless the power supply to the Controller is cycled.					

Event name	IP Address Switch Settings Error			Event code		28040000 hex
Meaning	An error was detected in the IP address switch settings.					
Source	EtherNet/IP Function Module		Source details	Communications port 1 or 2	Detection timing	At power ON, Controller reset, or at user operation
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the settings), cycle the power supply, or reset Controller.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port.		

System-defined variables	Variable	Data type	Name
	_EIP1_IPAdrCfgErr	BOOL	Port1 IP Address Setting Error
	_EIP2_IPAdrCfgErr	BOOL	Port2 IP Address Setting Error

Cause and correction	Assumed cause	Correction	Prevention
	The built-in EtherNet/IP port settings (TCP/IP settings)are set to obtain from BOOTP server, but the IP address switch is not set correctly.	If the IP address is obtained from the BOOTP server, the IP address switch is set to FF. Or, built-in EtherNet/IP port settings (TCP/IP settings) are set to obtain from BOOTP server and IP address switch is set to 00.	If the IP address is obtained from the BOOTP server, the IP address switch is set to FF. Or, built-in EtherNet/IP port settings (TCP/IP settings) are set to obtain from BOOTP server and IP address switch is set to 00.
	Communications port 1 and communications port 2 of the built-in EtherNet/IP ports belong to the same network.	Change the setting of the subnet mask in the built-in EtherNet/IP port settings (TCP/IP settings) or the setting of the IP address switch so that communications port 1 and communications port 2 of the built-in EtherNet/IP ports do not belong to the same network.	Set the subnet mask in the built-in EtherNet/IP port settings (TCP/IP settings) or the IP address switch so that communications port 1 and communications port 2 of the built-in EtherNet/IP ports do not belong to the same network.
	All bits for the host address of the built-in EtherNet/IP port are 0 or 1.	Change the setting of the subnet mask in the built-in EtherNet/IP port settings (TCP/IP settings) or the setting of the IP address switch so that all bits for the host address of the built-in EtherNet/IP port are not 0 or 1.	Set the subnet mask in the built-in EtherNet/IP port settings (TCP/IP settings) or the IP address switch so that all bits for the host address of the built-in EtherNet/IP port are not 0 or 1.

Attached information	Attached information 1: Type of errors 01Hex: When the settings are inconsistent Attached information 2: Error Details 00 hex: The built-in EtherNet/IP port settings (TCP/IP settings)are set to obtain from BOOTP server, but the IP address switch is not set correctly. 01 hex: Communications port 1 and communications port 2 of the built-in EtherNet/IP ports belong to the same network. 02 hex: All bits for the host address of the built-in EtherNet/IP port are 0 or 1.
Precautions/ Remarks	If the IP address switch is set to 01 to FE, the set value of the IP address switch becomes the last 8 bits of the IP address and the IP address is determined. Then, the network address and host address are determined according to the setting of the subnet mask.

Event name	Tag Data Link Setting Error			Event code	34200000 hex	
Meaning	An error was detected in the communications settings for tag data links.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	CIP/CIP1/CIP2	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the tag data link settings), cycle the power supply, or reset Controller.	Log category	System
Effects	User program	Continues.	Operation	Tag data link communications will not operate.		

System-defined variable	Variable	Data type	Name
	_EIP_TDLinkCfgErr	BOOL	Tag Data Link Setting Error
	_EIP1_TDLinkCfgErr	BOOL	CIP Communications1 Tag Data Link Setting Error
	_EIP2_TDLinkCfgErr	BOOL	CIP Communications2 Tag Data Link Setting Error

Cause and correction	Assumed cause	Correction	Prevention
	Power was interrupted when a download was in progress for the data link settings.	Implement one of the following measures. • Clear All Memory • Download the tag data link settings again. • Clear the tag data link settings.	Do not turn OFF the power supply to the Controller while a download is in progress for the tag data link settings.
	Memory error	If the above measures do not work, replace the CPU Unit.	None

Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings)
Precautions/ Remarks	None

<table>
<tr><td>Event name</td><td colspan="3">IP Rout Table Setting Error</td><td>Event code</td><td colspan="2">34230000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An IP routing setting error was detected.</td></tr>
<tr><td>Source</td><td colspan="2">EtherNet/IP Function Module</td><td>Source details</td><td>Communications port</td><td>Detection timing</td><td>At power ON or Controller reset</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Automatic recovery (after downloading the settings), cycle the power supply, or reset Controller.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">Communications that use the relevant IP routing settings are not possible.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">_EIP_IPRTblErr</td><td colspan="2">BOOL</td><td colspan="2">IP Route Table Error</td></tr>
<tr><td rowspan="4">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">Setting error</td><td colspan="2">Identify the error from the attached information, correct the setting, and then download the settings again.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings.</td><td colspan="2">Perform the Clear All Memory operation or download the settings again.</td><td colspan="2">Do not turn OFF the power supply to the Controller while a download is in progress for the built-in EtherNet/IP port settings.</td></tr>
<tr><td colspan="2">Memory error</td><td colspan="2">If operation is not recovered by the above, replace the CPU Unit.</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings)
Attached information 2: Error Details
(00 hex: Non-volatile memory access error
When the settings are inconsistent
(11 hex: Illegal IP router table settings, 12 hex: Illegal Hosts setting, 13 hex: Invalid default gateway, 14 hex: Illegal IPForward settings, 15 hex: Illegal NAT settings, 16 hex: Illegal PacketFilter settings)</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">The cause of error can be identified with the attached information.</td></tr>
</table>

Event name	FTP Server Setting Error			Event code	34240000 hex	
Meaning	An error was detected in the FTP server settings.					
Source	EtherNet/IP Function Module		Source details	FTP	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the FTP settings), cycle the power supply, or reset Controller	Log category	System
Effects	User program	Continues.	Operation	FTP will not operate.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Setting error		Identify the error from the attached information, correct the setting, and then download the settings again.		None	
	Power was interrupted when a download was in progress for the FTP server settings.		Perform the Clear All Memory operation or download the settings again.		Do not turn OFF the power supply to the Controller while a download is in progress for the FTP server settings.	
	Memory error		If operation is not recovered by the above, replace the CPU Unit.		None	
Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings)					
Precautions/ Remarks	The cause of error can be identified with the attached information.					

Event name	NTP Client Setting Error			**Event code**	34250000 hex	
Meaning	An error was detected in the NTP client settings.					
Source	EtherNet/IP Function Module		**Source details**	NTP	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the NTP settings), cycle the power supply, or reset Controller	**Log category**	System
Effects	**User program**	Continues.	**Operation**	NTP operation stops.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Setting error		Identify the error from the attached information, correct the setting, and then download the settings again.		None	
	Power was interrupted when a download was in progress for the NTP client settings.		Perform the Clear All Memory operation or download the settings again.		Do not turn OFF the power supply to the Controller while a download is in progress for the NTP client settings.	
	Memory error		If operation is not recovered by the above, replace the CPU Unit.		None	
Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings)					
Precautions/ Remarks	The cause of error can be identified with the attached information.					

Event name	SNMP Setting Error			Event code	34260000 hex	
Meaning	An error was detected in the SNMP agent/trap settings.					
Source	EtherNet/IP Function Module		Source details	SNMP	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the SNMP settings), cycle the power supply, or reset Controller	Log category	System
Effects	User program	Continues.	Operation	SNMP operation stops.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Setting error		Identify the error from the attached information, correct the setting, and then download the settings again.		None	
	Power was interrupted when a download was in progress for the SNMP agent/trap settings.		Perform the Clear All Memory operation or download the settings again.		Do not turn OFF the power supply to the Controller while a download is in progress for the SNMP agent/trap settings.	
	Memory error		If operation is not recovered by the above, replace the CPU Unit.		None	
Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings) Attached Information 2: Error Location When the settings are inconsistent (01 hex: SNMP agent settings, 02 hex: SNMP trap settings)					
Precautions/ Remarks	The cause of error can be identified with the attached information.					

Event name	Tag Name Resolution Error			**Event code**	34270000 hex	
Meaning	Resolution of a tag used in a tag data link failed.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		**Source details**	CIP/CIP1/CIP2	**Detection timing**	At power ON, at Controller reset, when variables are changed from the Sysmac Studio, or when the data link table is changed from the Network Configurator
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the tag settings)	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Data links will not operate for unresolved tags. Data links for other tags will operate.		

System-defined variable	**Variable**	**Data type**	**Name**
	_EIP_TagAdrErr	BOOL	Tag Name Resolution Error
	_EIP1_TagAdrErr	BOOL	CIP Communications1 Tag Name Resolution Error
	_EIP2_TagAdrErr	BOOL	CIP Communications2 Tag Name Resolution Error
Cause and correction	**Assumed cause**	**Correction**	**Prevention**
	The size of the network variable is different from the tag settings.	Correct the sizes in the tag settings to match the network variables.	Set the sizes in the tag settings to match the network variables.
	The I/O direction set for a tag data link and the I/O direction of the Controller variable do not match.	Correct the tag settings or the settings of the Controller variables so that the I/O direction for the tag data links match the I/O direction of the Controller variables.	Set the tag settings or the settings of the Controller variables so that the I/O directions for the tag data links match the I/O directions of the Controller variables.
	There are no network variables for the Controller tag settings.	Correct the tag settings so that existing network variables are set for the tags.	Set the tag settings so that existing network variables are set for the tags.
	A variable in the Controller that is set for a tag data link has the Network Publish attribute set to **Input** but also has the Constant attribute.	Remove the Constant attribute from the Controller variable that has the Network Publish attribute set to **Input**.	Do not set the Constant attribute for a Controller variable that has the Network Publish attribute set to **Input**.
Attached information	None		
Precautions/ Remarks	None		

Event name	Basic Ethernet Setting Error			Event code	34280000 hex	
Meaning	An error was detected in the Ethernet settings.					
Source	EtherNet/IP Function Module		Source details	Communications port 1 or 2	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Automatic recovery, cycle the power supply, or reset the Controller.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port.		

System-defined variables	Variable	Data type	Name
	_EIP1_EtnCfgErr	BOOL	Port1 Basic Ethernet Setting Error
	_EIP2_EtnCfgErr	BOOL	Port2 Basic Ethernet Setting Error

Cause and correction	Assumed cause	Correction	Prevention
	Setting error	Identify the error from the attached information, correct the setting, and then download the settings again.	None
	Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings.	Perform the Clear All Memory operation or download the settings.	Do not turn OFF the power supply to the Controller while a download is in progress for the built-in EtherNet/IP port settings.
	Memory error	If operation is not recovered by the above, replace the CPU Unit.	None

Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings) Attached information 2: Error details (00 hex: Non-volatile memory access error, 11 hex: Incorrect baud rate setting, 12 hex: Unsupported baud rate)
Precautions/ Remarks	The cause of error can be identified with the attached information.

Event name	IP Address Setting Error			Event code	34290000 hex	
Meaning	An error was detected in the IP address settings.					
Source	EtherNet/IP Function Module		Source details	Communications port 1 or 2	Detection timing	At power ON, at Controller reset, or at user operation
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the settings), cycle the power supply, or reset Controller.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port.		

System-defined variable	Variable	Data type	Name
	_EIP1_IPAdrCfgErr	BOOL	Port1 IP Address Setting Error
	_EIP2_IPAdrCfgErr	BOOL	Port2 IP Address Setting Error

Cause and correction	Assumed cause	Correction	Prevention
	Setting error	Identify the error from the attached information, correct the setting, and then download the settings again.	None
	Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings.	Perform the Clear All Memory operation or download the settings again.	Do not turn OFF the power supply to the Controller while a download is in progress for the built-in EtherNet/IP port settings.
	The IP address acquired from the BOOTP or DHCP server is illegal.	Correct the IP address that was provided to this port by the BOOTP or DHCP server so that it is within the range specified for an NX-series Controller.	Set the IP address that was provided to this port by the BOOTP or DHCP server so that it is within the range specified for an NX-series Controller.
	Memory error	If operation is not recovered by the above replace the CPU Unit.	None

Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings) Attached information 2: Error Details (00 hex: Non-volatile memory access error When the settings are inconsistent (11 hex: Illegal IP address, 12 hex: Illegal subnet mask)
Precautions/ Remarks	The cause of error can be identified with the attached information.

Event name	DNS Setting Error			Event code	342A0000 hex	
Meaning	An error was detected in the DNS settings or Hosts settings.					
Source	EtherNet/IP Function Module		Source details	Communications port	Detection timing	At power ON or Controller reset
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the settings), cycle the power supply, or reset Controller.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications will not operate.		
System-defined variables	Variable		Data type		Name	
	_EIP_DNSCfgErr		BOOL		DNS Setting Error	
Cause and correction	Assumed cause		Correction		Prevention	
	Setting error		Identify the error from the attached information, correct the setting, and then download the settings again.		None	
	Power was interrupted when a download was in progress for the built-in EtherNet/IP port settings.		Perform the Clear All Memory operation or download the settings again.		Do not turn OFF the power supply to the Controller while a download is in progress for the built-in EtherNet/IP port settings.	
	Memory error		If operation is not recovered by the above replace the CPU Unit.		None	
Attached information	Attached information 1: Type of errors (01 hex: Non-volatile memory access error, 02 hex: Inconsistency in settings) Attached information 2: Error Details (00 hex: Non-volatile memory access error When the settings are inconsistent 14 hex: Preferred DNS setting error, 15 hex: Alternate DNS setting error, 16 hex: Illegal domain name, 17Hex: Illegal Hosts setting					
Precautions/ Remarks	The cause of error can be identified with the attached information.					

Event name	Controller Insufficient Memory Warning		Event code	50010000 hex	
Meaning	The amount of data for the EtherCAT slave configuration, network-published information, or other data exceeds the value that is specified for the CPU Unit. You may not be able to perform online editing or other operations.				
Source	EtherCAT Master Function Module or EtherNet/IP Function Module	Source details	Master or CIP	Detection timing	At power ON, download, or online editing
Error attributes	Level: Minor fault	Recovery	Automatic recovery	Log category	System
Effects	User program: Continues.	Operation	Not affected.		
System-defined variables	Variable	Data type	Name		
	None	---	---		
Cause and correction	Assumed cause	Correction	Prevention		
	The amount of data for the EtherCAT slave configuration, network-published information, or other data exceeds the value that is specified for the CPU Unit.	Reduce the number of PDOs that are used by the EtherCAT slaves. Reduce the number of data types that are used for network variables or reduce the length of the text strings that are used for names.	None		
Attached information	None				
Precautions/ Remarks	You may not be able to perform online editing or other operations.				

Event name	DNS Server Connection Error		Event code	84030000 hex	
Meaning	Connection with the DNS server failed.				
Source	EtherNet/IP Function Module	Source details	Communications port	Detection timing	At DNS operation
Error attributes	Level: Minor fault	Recovery	Automatic recovery (after downloading the DNS settings)	Log category	System
Effects	User program: Continues.	Operation	Communications using DNS stop.		
System-defined variables	Variable	Data type	Name		
	_EIP_DNSSrvErr	BOOL	DNS Server Connection Error		
Cause and correction	Assumed cause	Correction	Prevention		
	Setting error	If there is a mistake with the specifications of the connected server, correct the server specifications and download them again.	Make sure that the connected server is specified correctly.		
	The server is down.	Check if the server at the remote connection is operating normally and set it to operate normally if it is not.	Check to make sure that the server at the remote connection is operating normally.		
	An error occurred in the communications path.	Check the communications path to the server and take corrective measures if there are any problems.	None		
Attached information	None				
Precautions/ Remarks	None				

Event name	NTP Server Connection Error			**Event code**	84040000 hex	
Meaning	Connection with the NTP server failed.					
Source	EtherNet/IP Function Module		**Source details**	NTP	**Detection timing**	At NTP operation
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the NTP settings)	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Time cannot be acquired from NTP.		
System-defined variables	**Variable**		**Data type**		**Name**	
	_EIP_NTPSrvErr		BOOL		NTP Server Connection Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Setting error		If there is a mistake with the specifications of the connected server, correct the server specifications and download them again.		Make sure that the connected server is specified correctly.	
	The server is down.		Check if the server at the remote connection is operating normally and set it to operate normally if it is not.		Check to make sure that the server at the remote connection is operating normally.	
	An error occurred in the communications path.		Check the communications path to the server and take corrective measures if there are any problems.		None	
Attached information	None					
Precautions/ Remarks	For CPU Units with unit version 1.37 or later (NX701-□□□□) or unit version 1.70 or later (other than NX701-□□□□), you can change the event level to observation. If you change to the observation level, the *EtherNet/IP NET ERR* column above will be changed to --- *(no change)*. If you change to the observation level, you can check whether the NTP Server Connection Error is persisting using the *_EIP_NTPSrvErr* system-defined variable.					

Event name	Tag Data Link Connection Failed			**Event code**	84070000 hex	
Meaning	Establishing a tag data link connection failed.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		**Source details**	CIP/CIP1/CIP2	**Detection timing**	When establishing tag data link connection
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Data links will not operate for connections that could not be established. Data links for other connections will operate.		

System-defined variable	**Variable**	**Data type**	**Name**
	_EIP_TDLinkOpnErr	BOOL	Tag Data Link Connection Failed
	_EIP1_TDLinkOpnErr	BOOL	CIP Communications1 Tag Data Link Connection Failed
	_EIP2_TDLinkOpnErr	BOOL	CIP Communications2 Tag Data Link Connection Failed

Cause and correction	**Assumed cause**	**Correction**	**Prevention**
	The tag data link connection information is not the same for the originator and target.	Correct the tag data link connection information, and then download the device parameters or connection settings from the Network Configurator or Sysmac Studio.	Before you use the tag data links, make sure that the tag data link connection information in the originator and target are suitable.
	Insufficient connections	Reduce the number of class-3 messages.	Reduce the number of data links and class-3 messages that are used.
	CIP message communications at the target node are stopped. (for NJ/NX-series CPU Units)	Make the device start normal CIP message communications.	Make the device start normal CIP message communications before you use a tag data link.
	Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings (for NX-series EtherNet/IP Units).	Do not configure the NX-series EtherNet/IP Unit, which is included in the CIP Safety connection settings, to use tag data link communications (for NX-series EtherNet/IP Units).	Do not configure the NX-series EtherNet/IP Unit, which is included in the CIP Safety connection settings, to use tag data link communications (for NX-series EtherNet/IP Units).
	The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings (for NX-series EtherNet/IP Units).	Do not add the NX-series EtherNet/IP Unit, for which tag data link communications are set to use, to the CIP Safety connection settings (for NX-series EtherNet/IP Units).	Do not add the NX-series EtherNet/IP Unit, for which tag data link communications are set to use, to the CIP Safety connection settings (for NX-series EtherNet/IP Units).

Attached information	Attached information 1: Target node IP address (example: C0A8FA01 hex = address 192.168.250.1) Attached information 2: Connection instance No. 0 to 255 Attached information 3: Connection status (example: 010000117 hex for General Status 01 and Additional Status 0117)
Precautions/ Remarks	• You can investigate a detailed cause from the connection status. • This event occurs only once even if this error occurred simultaneously in several connections for the same target node.

Event name	Tag Data Link Timeout			Event code	84080000 hex	
Meaning	A timeout occurred in a tag data link.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	CIP/CIP1/CIP2	Detection timing	Continuously after starting tag data link communications
Error attributes	Level	Minor fault	Recovery	Automatic recovery	Log category	System
Effects	User program	Continues.	Operation	The relevant data link connection will stop. Reconnection processing is periodically repeated for the tag data link error target.		

System-defined variable	Variable	Data type	Name
	_EIP_TDLinkErr	BOOL	Tag Data Link Communications Error
	_EIP1_TDLinkErr	BOOL	CIP Communications1 Tag Data Link Communications Error
	_EIP2_TDLinkErr	BOOL	CIP Communications2 Tag Data Link Communications Error

Cause and correction	Assumed cause	Correction	Prevention
	The power supply to the target node is OFF.	Check the status of the target node and start it normally.	Use the tag data link after you confirm that the target node is normal.
	Communications with the target node stop.		
	The Ethernet cable connector for EtherNet/IP is disconnected.	Reconnect the connector and make sure it is connected correctly.	Connect the connector securely.
	The Ethernet cable for EtherNet/IP is broken.	Replace the Ethernet cable.	None
	The link to the built-in EtherNet/IP port is OFF.	Refer to the Link OFF Detected error (84060000 hex) for the assumed causes and other information on link OFF.	Refer to the Link OFF Detected error (84060000 hex) for the assumed causes and other information on link OFF.
	CIP message communications at the target node are stopped. (for NJ/NX-series CPU Units)	Make the device start normal CIP message communications.	Make the device start normal CIP message communications before you use a tag data link.
	When the Packet Filter function is enabled in the Built-in EtherNet/IP Port Settings, packets from the target are not allowed. (for NJ/NX-series CPU Units)	Allow packets from the target in the Packet Filter settings of the Built-in EtherNet/IP Port Settings.	Make sure that packets from the target are allowed in the Packet Filter settings of the Built-in EtherNet/IP Port Settings before you use a tag data link.
	CIP communications are not allowed by the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path. (for NJ/NX-series CPU Units)	Allow CIP communications in the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path.	Make sure that CIP communications are allowed in the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path to use tag data links.
	The packet loss occurred on the path due to the network communications load.	Increase the timeout value or RPI. Or, review the network environment and network devices.	Design the network so that there is not too much load on the network.
	Noise	Implement noise countermeasures if there is excessive noise.	Implement noise countermeasures if there is excessive noise.

Attached information	Attached information 1: Connection instance No. 0 to 255 Attached information 2: Target node IP address (example: C0A8FA01 hex = address 192.168.250.1)

Precautions/ Remarks	• The following cases are not included in this error. Connections as a target • This event occurs only once even if this error occurred simultaneously in several connections for the same target node.

Event name	Tag Data Link Connection Timeout			**Event code**	84090000 hex	
Meaning	A timeout occurred while trying to establish a tag data link connection.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		**Source details**	CIP/CIP1/CIP2	**Detection timing**	When establishing tag data link connection
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Data links will not operate for connections that timed out. Reconnection processing is periodically repeated for the connection that timed out.		

System-defined variable	**Variable**	**Data type**	**Name**
	_EIP_TDLinkOpnErr	BOOL	Tag Data Link Connection Failed
	_EIP1_TDLinkOpnErr	BOOL	CIP Communications1 Tag Data Link Connection Failed
	_EIP2_TDLinkOpnErr	BOOL	CIP Communications2 Tag Data Link Connection Failed

Cause and correction	**Assumed cause**	**Correction**	**Prevention**
	The power supply to the target node is OFF.	Check the status of the target node and start it normally.	Use the tag data link after you confirm that the target node is normal.
	Communications at the target node are stopped.		
	CIP message communications are stopped at the target node or built-in EtherNet/IP Port. (for NJ/NX-series CPU Units)	Make the device start normal CIP message communications.	Make the device start normal CIP message communications before you use a tag data link.
	The Ethernet cable connector for EtherNet/IP is disconnected.	Reconnect the connector and make sure it is connected correctly.	Connect the connector securely.
	The Ethernet cable for EtherNet/IP is broken.	Replace the Ethernet cable.	None
	CIP communications are not allowed by the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path. (for NJ/NX-series CPU Units)	Allow CIP communications in the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path.	Make sure that CIP communications are allowed in the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path to use tag data links.
	An error occurred in the communications path.	Check the communications path and take corrective measures if there are any problems.	None

Attached information	Attached information 1: Target node IP address (example: C0A8FA01 hex = address 192.168.250.1)
Precautions/ Remarks	• You can change the event level to the observation level. If you change the level to the observation level, the EtherNet/IP NET ERR column above will be changed to "---" (no change) and recovery will not be necessary. • The following cases are not included in this error. Connections as a target Connection timeouts due to a Link OFF detection for an Ethernet switch • This event occurs only once even if this error occurred simultaneously in several connections for the same target node.

Event name	IP Address Duplication Error			Event code	840A0000 hex	
Meaning	The same IP address is used more than once.					
Source	EtherNet/IP Function Module		Source details	Communications port 1 or 2	Detection timing	After link is established
Error attributes	Level	Minor fault	Recovery	Automatic recovery (after downloading the IP address settings), cycle the power supply, or reset Controller.	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port. Packets addressed to the local IP address of the relevant communications port are discarded.		
System-defined variable	Variable		Data type		Name	
	_EIP1_IPAdrDupErr		BOOL		Port1 IP Address Duplication Error	
	_EIP2_IPAdrDupErr		BOOL		Port2 IP Address Duplication Error	
Cause and correction	Assumed cause		Correction		Prevention	
	The IP address of the built-in EtherNet/IP port is also used as the IP address of another node.		Perform either of the following corrections. • Check the IP addresses of other nodes and correct the IP address settings so that the same address is not used by more than one node. • Remove the other node that has the duplicate IP address from the network and then cycle the power supply to the Controller or reset the Controller.		Perform allocations so that IP addresses of nodes on the network are used for only one node.	
Attached information	Attached information 1: Duplicated IP address (example: C0A8FA01 hex = address 192.168.250.1)					
Precautions/ Remarks	A duplicated address error occurs if an ARP is sent with the set IP address and there is an ARP response.					

Event name	BOOTP Server Connection Error			Event code	840B0000 hex	
Meaning	Connection with the BOOTP server failed.					
Source	EtherNet/IP Function Module		Source details	Communications port 1 or 2	Detection timing	At BOOTP operation
Error attributes	Level	Minor fault	Recovery	Automatic recovery	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications are not possible for the relevant communications port. Requests to the BOOTP server will continue until there is a response from the BOOTP server. Data refreshing with the PLC Function Module will continue. An IP address was not set for the EtherNet/IP port when it was supposed to be set from the BOOTP server.		

System-defined variables	Variable	Data type	Name
	_EIP1_BootpErr	BOOL	Port1 BOOTP Server Error
	_EIP2_BootpErr	BOOL	Port2 BOOTP Server Error

Cause and correction	Assumed cause	Correction	Prevention
	Server setting error	Correct the server settings at the remote connection.	Check to make sure that the server settings at the remote connection are correct.
	The server is down.	Check if the server at the remote connection is operating normally and set it to operate normally if it is not.	Check to make sure that the server at the remote connection is operating normally.
	An error occurred in the communications path.	Check the communications path to the server and take corrective measures if there are any problems.	None

Attached information	None
Precautions/ Remarks	None

<table>
<tr><td>Event name</td><td colspan="3">Allowed Communications Bandwidth per Unit Exceeded</td><td>Event code</td><td colspan="2">840C0000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">The total bandwidth for the connections that are set or established exceeded the allowed communications bandwidth of tag data links and CIP Safety communications*1 per Unit for all of the built-in EtherNet/IP ports.</td></tr>
<tr><td>Source</td><td colspan="2">In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module</td><td>Source details</td><td>CIP1/CIP2</td><td>Detection timing</td><td>When establishing tag data link connection or CIP Safety connection</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Automatic recovery (after downloading the settings), cycle the power supply, or reset Controller.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">Tag data links and CIP Safety communications*1 will not operate in the bandwidth that exceeds the allowed communications bandwidth per Unit.</td></tr>
<tr><td rowspan="4">System-defined variable</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">_EIP_TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">Tag Data Link Connection Failed</td></tr>
<tr><td colspan="2">_EIP1_TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications1 Tag Data Link Connection Failed</td></tr>
<tr><td colspan="2">_EIP2_TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications2 Tag Data Link Connection Failed</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">An attempt was made to establish a connection that would cause the used bandwidth (PPS) total of the packet transfer rates of the tag data links and CIP Safety communications*1 that use all of the built-in EtherNet/IP ports to exceed the allowed communications bandwidth per Unit.</td><td colspan="2">Change the settings at the originator node for the tag data links and CIP Safety communications*1 so that the total PPS for all of the built-in EtherNet/IP ports does not exceed the allowed communications bandwidth per Unit, and then cycle the power supply to the Controller or reset the Controller.</td><td colspan="2">Set the tag data links and CIP Safety communications*1 so that the total PPS for all of the built-in EtherNet/IP ports does not exceed the allowed communications bandwidth per Unit.</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">You can confirm the bandwidth (PPS) of the tag data link for EtherNet/IP ports in the Ethernet Information Tab Page on the Network Configurator.
Refer to Ethernet Information Tab Page section in Checking Status with the Network Configurator in the for how to confirm the bandwidth (PPS) on the Network Configurator.</td></tr>
</table>

*1. This applies for a CPU Unit that supports CIP Safety communications.

Event name	IP Address Switch Change during Operation Error			Event code		840D0000 hex
Meaning	The IP address switch setting was changed during the operation.					
Source	EtherNet/IP Function Module		Source details	Communications port, communications port 1 or 2	Detection timing	When IP address switch setting is changed during operation
Error attributes	Level	Minor fault	Recovery	Cycle the power supply.	Log category	System
Effects	User program	Continues.	Operation	CIP Safety I/O communications will stop. Other tag data link operations and CIP message communications will continue.		

System-defined variables	Variable	Data type	Name
	_EIP_ChgIpSwErr	BOOL	IP Address Switch Change during Operation Error
	_EIP1_ChgIpSwEr	BOOL	Port 1 IP Address Switch Change during Operation Error
	_EIP2_ChgIpSwErr	BOOL	Port 2 IP Address Switch Change during Operation Error

Cause and correction	Assumed cause	Correction	Prevention
	The IP address switch setting was changed during the operation.	Restore the previous setting and restart the Units.	Change the address switch setting when the power supply to the Controller is turned OFF.

Attached information	None
Precautions/ Remarks	None

Event name	Number of Tag Sets for Tag Data Links Exceeded		Event code	840E0000 hex	
Meaning	The total number of tag sets for tag data links for all ports of the built-in Ethernet/IP port exceeds the upper limit.				
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module	Source details	CIP1/CIP2	Detection timing	At power ON, Controller reset, download from the Sysmac Studio, or download from the Network Configurator
Error attributes	Level: Minor fault	Recovery	Automatic recovery	Log category	System
Effects	User program: Continues.	Operation	Tag data link communications for the relevant port were stopped.		

System-defined variable	Variable	Data type	Name
	_EIP_TDLinkCfgErr	BOOL	Tag Data Link Setting Error
	_EIP1_TDLinkCfgErr	BOOL	CIP Communications1 Tag Data Link Setting Error
	_EIP2_TDLinkCfgErr	BOOL	CIP Communications2 Tag Data Link Setting Error

Cause and correction	Assumed cause	Correction	Prevention
	The total number for all ports of tag sets for tag data links that are set for each built-in Ethernet/IP port exceeds the total number of which the product can be allowed.	Change the number of tag sets so that the total number for all ports of tag sets for tag data links that are set for each built-in Ethernet/IP port does not exceed the total number of which the product can be allowed.	When the number of tag sets for tag data links that are set for each built-in Ethernet/IP port is changed, check that the total number of tag sets for all ports does not exceed the total number of which the product can be allowed in advance.

Attached information	Attached information 1: The number of tag sets that are set for the port. Attached information 2: Total number of tag sets that are set for the product. Attached information 3: Total number of tag sets that the product can be allowed.
Precautions/ Remarks	None

Event name	Access Detected Outside Range of Variable		Event code	54E00000Hex		
Meaning	Accessing a value that is out of range was detected for a tag variable that is used in a tag data link.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	Communications port	Detection timing	When variable is written
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An out-of-range value was written by an EtherNet/IP tag data link for a variable with a specified range. A value that does not specify an enumerator was written by an EtherNet/IP tag data link for an enumeration variable.		Correct the value that is written to the variable with a specified range so that the value is in the range. Correct the value that is written to the enumeration variable so that the value specifies an enumerator.		Write values that are in range for variables with specified ranges. Write values that specify enumerators to enumeration variables.	
Attached information	None					
Precautions/ Remarks	• Write operations for out-of-range values or values that do not specify enumerators do not end normally. • Write operations for in-range values or values that specify enumerators end normally.					

Event name	Packet Discarded Due to Full Receive Buffer		Event code	84050000 hex		
Meaning	A packet was discarded.					
Source	EtherNet/IP Function Module		Source details	Communications port, communications port 1, or communications port 2	Detection timing	After link is established
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	A network convergence occurred.		The load on the network is too high. Check whether there are nodes that send unnecessary broadcast frames on the network and remove them. After that, check that the received number of frames has reduced in the network statistical information.		Make sure that unnecessary broadcast frames are not sent on the network. Do not connect the Ethernet cable in a loop.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Link OFF Detected			Event code	84060000 hex	
Meaning	An Ethernet link OFF was detected.					
Source	EtherNet/IP Function Module		Source details	Communications port, communications port 1 or 2	Detection timing	Continuously
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	EtherNet/IP communications will not operate.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	An Ethernet cable is broken, disconnected, or loose.		Firmly connect the Ethernet cable. Replace the cable if it is broken.		Firmly connect the Ethernet cable. Also, make sure that the cable to be used is not disconnected.	
	The Ethernet switch's power supply is turned OFF.		Turn ON the power supply to the Ethernet switch. Replace the Ethernet switch if it fails.		Do not turn OFF the Ethernet switch.	
	Communications speed mismatched.		Modify the setting so that the communication speed is the same as that of the remote node.		Set the same communication speed as that on the remote node.	
	Noise		Implement noise countermeasures if there is excessive noise.		Implement noise countermeasures.	
	One of the following operations was performed. • The Identity object was reset. • Settings for EtherNet/IP were downloaded from the Network Configurator or Sysmac Studio, or the Clear All Memory operation was performed. • EtherNet/IP was restarted.		None. This error occurs when the operations on the left are performed.		None. This error occurs when the operations on the left are performed.	
	If an Ethernet link off is detected on port 2, **Use Port 2** check box is not selected.		When using port2, select the **Use Port 2** Check Box and configure the settings.		Make sure that the **Use Port 2** setting is correct.	
Attached information	None					
Precautions/ Remarks	The level can be changed to minor fault. When it is changed to minor fault, the recovery method used is "automatic recovery".					

Event name	Tag Data Link Download Started			Event code	94010000 hex	
Meaning	Changing the tag data link settings started.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	CIP/CIP1/CIP2	Detection timing	At user operation
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Changing the tag data link settings started.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode)					
Precautions/ Remarks	None					

Event name	Tag Data Link Download Finished			Event code	94020000 hex	
Meaning	Changing the tag data link settings finished.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	CIP/CIP1/CIP2	Detection timing	At user operation
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Changing the tag data link settings finished.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode)					
Precautions/ Remarks	None					

Event name	Tag Data Link Stopped			**Event code**	94030000 hex	
Meaning	Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		**Source details**	CIP *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ CIP1 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ CIP2 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/*1 to 4: Mounting position of the X Bus Unit* and *CIP1 /CIP2* are given in combination.*Built-in EtherNet/IP Port on CPU Unit* on page 15-136 CIP/CIP1/CIP2	**Detection timing**	At user operation
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	_EIP_TDLinkStopCmd		BOOL		Tag Data Link Communications Stop Switch	
	_EIP1_TDLinkStopCmd		BOOL		CIP Communications1 Tag Data Link Communications Stop Switch	
	_EIP2_TDLinkStopCmd		BOOL		CIP Communications2 Tag Data Link Communications Stop Switch	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode) Attached information 2: Operation method (01 hex: Operation by Network Configurator or Sysmac Studio, 02 hex: Manipulation by a system defined variable, 03 hex: Manipulation by special instructions) Attached information 3: • When attached information 2 is 03 hex IP address of the target node • When attached information 2 is a value other than 03 hex 0					
Precautions/ Remarks	None					

Event name	Tag Data Link Started			**Event code**	94040000 hex	
Meaning	Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		**Source details**	CIP *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ CIP1 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ CIP2 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/*1 to 4: Mounting position of the X Bus Unit* and *CIP1 /CIP2* are given in combination.*Built-in EtherNet/IP Port on CPU Unit* on page 15-136 CIP/CIP1/CIP2	**Detection timing**	At user operation
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	_EIP_TDLinkStartCmd *Built-in EtherNet/IP Port on CPU Unit* on page 15-136		BOOL		Tag Data Link Communications Start Switch	
	_EIP1_TDLinkStartCmd *Built-in EtherNet/IP Port on CPU Unit* on page 15-136		BOOL		CIP Communications1 Tag Data Link Communications Start Switch	
	_EIP2_TDLinkStartCmd *Built-in EtherNet/IP Port on CPU Unit* on page 15-136		BOOL		CIP Communications2 Tag Data Link Communications Start Switch	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode) Attached information 2: Operation method (01 hex: Operation by Network Configurator or Sysmac Studio, 02 hex: Manipulation by a system defined variable, 03 hex: Manipulation by special instructions) Attached information 3: • When attached information 2 is 03 hex IP address of the target node • When attached information 2 is a value other than 03 hex 0					
Precautions/ Remarks	None					

Event name	Link Detected			Event code	94050000 hex	
Meaning	Establishment of an Ethernet link was detected.					
Source	EtherNet/IP Function Module		Source details	Communications port / Communications port 1 / Communications port 2 / Internal port 1	Detection timing	When links are established
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Establishment of an Ethernet link was detected.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Restarting Ethernet Port			Event code	94060000 hex	
Meaning	The built-in EtherNet/IP port was restarted.					
Source	EtherNet/IP Function Module		Source details	Communications port *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ Communications port 1 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ Communications port 2 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ Internal port 1	Detection timing	At user operation
Error attributes	Level	Information	Recovery	---	Log category	Access
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The built-in EtherNet/IP port was restarted.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Tag Data Link All Run			Event code		94070000 hex
Meaning	Tag data link connections to all nodes have been normally established.					
Source	In the CPU Unit, EtherNet/IP Function Module. For the X Bus Unit, X Bus Ethernet/IP Function Module		Source details	CIP/CIP1/CIP2	Detection timing	When establishing tag data link connection
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variable	Variable		Data type		Name	
	_EIP_TDLinkAllRunSta		BOOL		All Tag Data Link Communications Status	
	_EIP1_TDLinkAllRunSta		BOOL		CIP Communications1 All Tag Data Link Communications Status	
	_EIP2_TDLinkAllRunSta		BOOL		CIP Communications2 All Tag Data Link Communications Status	
Cause and correction	Assumed cause		Correction		Prevention	
	Tag data link connections to all target nodes have been established.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	IP Address Fixed			Event code		94080000 hex
Meaning	The correct IP address has been determined and Ethernet communications can start.					
Source	EtherNet/IP Function Module		Source details	Communications port *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ Communications port 1 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ Communications port 2 *Built-in EtherNet/IP Port on CPU Unit* on page 15-136/ Internal port 1	Detection timing	At power ON or Controller reset
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The correct IP address has been determined and Ethernet communications can start.		---		---	
Attached information	Attached Information 1: IP address (example: C0A8FA01 hex = address 192.168.250.1)					
Precautions/ Remarks	None					

Event name	BOOTP Client Started			Event code	94090000 hex	
Meaning	The BOOTP client started requesting an IP address.					
Source	EtherNet/IP Function Module		Source details	Communications port, communications port 1, or communications port 2	Detection timing	At power ON or Controller reset
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The BOOTP client started requesting an IP address.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	FTP Server Started			Event code	940A0000Hex	
Meaning	The FTP agent started normally.					
Source	EtherNet/IP Function Module		Source details	FTP	Detection timing	At power ON or Controller reset
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The FTP agent started normally.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	NTP Client Started			Event code	940B0000Hex	
Meaning	The NTP client started normally and a request for the NTP server to obtain the time started.					
Source	EtherNet/IP Function Module		Source details	NTP	Detection timing	At power ON or Controller reset
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	Not affected.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	The NTP client started normally and a request for the NTP server to obtain the time started.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	SNMP Started			**Event code**	940C0000Hex	
Meaning	The SNMP agent started normally.					
Source	EtherNet/IP Function Module		**Source details**	SNMP	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The SNMP agent started normally.		---		---	
Attached information	None					
Precautions/ Remarks	None					

● Other Troubles and Corrections

Problem	Correction
At startup, some of the receive data is FALSE when it should be TRUE.	• If the user program uses receive data, make sure that the All Tag Data Link Communications Status in communications status 1 or the Controller Operating Mode for the target node is TRUE before you use the receive data. To use operation information from the Controller, use Controller status in the tag sets on both the sending and receiving nodes.
Tag data link communications are not stable.	• Use a 100 Mbps Ethernet switch if 10 Mbps is set or if you are using a 10 Mbps or 100 Mbps repeater hub. The performance of the tag data links assumes that an Ethernet switch is used to achieve a 12000 pps bandwidth for full-duplex, 100 Mbps auto-negotiation communications. • Check for noise on the communications path, non-standard cables, damaged cables/connectors, loose connectors, unexpectedly high communications traffic, and incorrect loops in connections between Ethernet switches. • Contact the Ethernet switch manufacturer if there are problems with the transfer capacity of the Ethernet switches in the communications path. If Ethernet switches are cascaded, the load may be concentrated on the middle Ethernet switches. Change the network configuration so that the load is not concentrated. • Refer to the user's manual for the originator device to remove the cause of the error.

15-3-3 Safety CPU Unit Error

Error Table

The errors (events) that can occur in the Safety CPU Unit are listed in the following tables.

● System Error

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
05200000 hex	System Error	A hardware error was detected during self-diagnosis of the hardware.	• Hardware has failed. • A memory error occurred due to a transient cause, such as a software error or excessive noise.			○			page 15-178

● Communications Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
35200001 hex	FSoE Master Connection Not Established Error	FSoE communications were not established with the FSoE slave.	• The FSoE communications settings are not correct, the FSoE slave is not in the correct status, etc. • The FSoE slave for FSoE communications is not connected. • The FSoE slave set in the NX Unit Mounting Setting for FSoE communications is disabled. • The version of the FSoE slave to be communicated is older than the configured version.			○			page 15-179

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80200000 hex	NX Unit I/O Communications Error	An I/O communications error occurred between the NX bus master and the NX Unit.	NX Bus of the CPU Unit • An error occurred in the CPU Unit, which prevents the NX bus communications from being carried out normally. • The NX Unit is not mounted properly. • The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect. • The power cable for the Unit power supply is broken. • The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient. • There is a hardware error in the NX Unit. Communications Coupler Unit • An error occurred in the Communications Coupler Unit, which prevents the NX bus communications from being carried out normally. • The NX Unit is not mounted properly. • The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect. • The power cable for the Unit power supply is broken. • The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient. • There is a hardware error in the NX Unit.			○			page 15-180

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80300001 hex	FSoE Master Connection Timeout	A communication timeout occurred in FSoE communications with the FSoE slave.	• A setting is not correct. The setting of the safety task period is too short. • There is excessive noise. • The Safety CPU Unit or FSoE slave entered a state where it could not continue FSoE communications. • The process data communications were not performed correctly because an error or status change occurred in the NX bus master to which the Unit is connected.			○			page 15-182
80310000 hex	CIP Safety Originator Connection Not Established Error	CIP safety originator connection was not established.	• The target node is different. • The target node is not configured. • The target node status is invalid. • The **Do not use** Option is selected for CIP message server setting in the EtherNet/IP Port Settings. • The settings of the NX-series CPU Unit and NX-series EtherNet/IP Unit related to CIP Safety communications do not match the settings of the Safety CPU Unit. • Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings. • The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings. • The **Do not use** Option is selected for CIP Safety communications in the Built-in EtherNet/IP Port Settings.			○			page 15-183

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80320000 hex	CIP Safety Originator Connection Timeout	A timeout occurred in CIP safety originator connection.	• The communications cable is disconnected or broken. • The target node entered a state where it could not accept the connection. • The timeout value in the communications setup is too small. • CIP message communications at the target node are stopped. • When the Packet Filter function is enabled in the EtherNet/IP Port Settings, CIP Safety packets from the target node are not allowed. • CIP Safety packets are not allowed by the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path. • There is excessive noise.			○			page 15-185
80330000 hex	CIP Safety Target Does Not Exist	The target node does not exist.	• The communications cable is disconnected or broken. • The target node entered a state where it could not accept the connection. • The timeout value in the communications setup is too small. • CIP message communications at the target node are stopped. • CIP Safety packets from the originator node are not allowed by the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path. • There is excessive noise.			○			page 15-186

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80340000 hex	CIP Safety Target Connection Timeout	A timeout occurred in the CIP Safety Target connection.	• The communications cable is disconnected or broken. • The originator device entered a state where it could not accept the connection. • The timeout value for the communications settings is too small. • CIP Safety packets from the originator node are not allowed by the Packet Filter (Simple) or Packet Filter functions in the EtherNet/IP Port Settings or on the devices on the communication path. • The CIP message server setting for the originator node is set to Do not use. • When the Packet Filter function of the originator node is enabled, CIP Safety packets from the target node are not allowed. • There is excessive noise. • The **Do not use** Option is selected for CIP Safety communications in the Built-in EtherNet/IP Port Settings.			○			page 15-187
84F00000 hex	NX Bus I/O Communications Stopped	An error occurred in I/O communications between the NX bus master and an NX Unit.	• There is a hardware error in the NX bus master or an NX Unit.			○			page 15-188

● Operation Continuation Error Related to Program Execution Function

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
74A00000 hex	SF_Antivalent Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-189

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
74A10000 hex	SF_EDM Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-189
74A20000 hex	SF_EmergencyStop Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-190
74A30000 hex	SF_EnableSwitch Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-190
74A40000 hex	SF_Equivalent Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-191
74A50000 hex	SF_ESPE Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-191
74A60000 hex	SF_GuardLocking Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-192
74A70000 hex	SF_GuardMonitoring Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-192
74A80000 hex	SF_ModeSelector Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-193

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
74A90000 hex	SF_Muting-Par Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-193
74AA0000 hex	SF_Muting-Par_2Sensor Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-194
74AB0000 hex	SF_Muting-Seq Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-194
74AC0000 hex	SF_OutControl Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-195
74AD0000 hex	SF_SafetyRequest Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-195
74AE0000 hex	SF_TestableSafety-Sensor Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-196
74AF0000 hex	SF_Two-HandControlTypeII Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-196
74B00000 hex	SF_Two-HandControlTypeIII Error	An error was detected in execution of a safety function block.	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.			○			page 15-197

● Operation Stop Error Related to Program Execution

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
55000000 hex	Division by Zero	Division by zero was detected.	The divisor is zero.			○			page 15-198
55010000 hex	Cast Error	A casting error was detected.	A value was input that exceeded the range of the receiving variable.			○			page 15-199
55020000 hex	MUX Error	An MUX instruction error was detected.	The value of the selection input (K) to the MUX instruction is not correct.			○			page 15-200

● Setting Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
10500000 hex	NX Bus Communications Settings Read Error	There is an error in the NX bus communications settings that are saved in non-volatile memory.	• A hardware failure occurred in the non-volatile memory. • Power was turned OFF while saving data to the non-volatile memory.			○			page 15-201
10510000 hex	Safety Application Data Read Error	There is an error in the safety application data that is saved in non-volatile memory.	• A hardware failure occurred in the non-volatile memory. • Power was turned OFF while saving data to the non-volatile memory.			○			page 15-201
10520000 hex	NX Bus Communications Settings and Safety Application Data Mismatch	There is an error in the safety application data that is saved in non-volatile memory.	• The NX bus communications settings that were transferred to the Safety CPU Unit do not match the safety application data.			○			page 15-202
10530000 hex	Non-volatile Memory Access Error	Reading/writing non-volatile memory failed.	Non-volatile memory failure.			○			page 15-203
24AA0000 hex	Incorrect DIP Switch Setting	The DIP switch setting is not correct.	• The DIP switch setting was changed to an incorrect value.				○		page 15-203

● Restore Function Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
35250000 hex	Safety Unit Restore Operation Failed to Start (SD Memory Card Access Failed)	Access to the SD Memory Card failed when you start the restore operation for a Safety Unit.	• An SD Memory Card is not inserted. • The SD Memory Card type is not correct. • The format of the SD Memory Card is not correct. • The SD Memory Card is damaged.				○		page 15-207
35260000 hex	Safety Unit Restore Operation Failed to Start (Safety Unit Restore File Read Failure)	Reading the Safety Unit Restore File failed.	• The Safety Unit Restore File is not stored in the specified folder. • The Safety Unit Restore File is corrupted.				○		page 15-208
35270000 hex	Safety Unit Restore Operation Failed to Start (Model Mismatch)	A model mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.	• The restore operation for a Safety Unit was performed on an incorrect Unit. • An incorrect Safety Unit Restore File was used.				○		page 15-209
35280000 hex	Safety Unit Restore Operation Failed to Start (Version Mismatch)	A version mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.	• The restore operation for a Safety Unit was performed on an incompatible unit. • An incorrect Safety Unit Restore File was used.				○		page 15-210
35290000 hex	Safety Unit Restore Operation Failed to Start (Node Name Mismatch)	A node name mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.	• The restore operation for a Safety Unit was performed on an incorrect Unit. • An incorrect Safety Unit Restore File was used. • The node name specified when the Safety Unit Restore File was generated is incorrect.				○		page 15-211
352A0000 hex	Safety Unit Restore Operation Failed to Start (Safety Password Mismatch)	A safety password mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.	• The restore operation for a Safety Unit was performed on an incorrect Unit. • An incorrect Safety Unit Restore File was used. • The safety password specified when the Safety Unit Restore File was generated is incorrect.				○		page 15-212

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
352B0000 hex	Safety Unit Restore Operation Failed	The restore operation for a Safety Unit ended in an error.	• The SD Memory Card was removed during a restore operation for a Safety Unit. • Data was read from or written to the SD Memory Card via the Support Software or an FTP client during a restore operation for a Safety Unit.				○		page 15-213

● Other Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80220000 hex	NX Message Communications Error	An error was detected in message communications for an NX Unit and the message frame was discarded.	• The message communications load is high. • The communications cable is disconnected or broken. This cause does not apply if attached information 2 is 0 (NX bus). • Message communications were cut off as the result of executing a synchronization or restoration operation on the Sysmac Studio or as the result of disconnecting an EtherCAT slave.				○		page 15-204
951E0000 hex	Sysmac Studio Communications Connection Timeout	A communications timeout occurred between the Sysmac Studio and the Safety CPU Unit.	• The communications cable was disconnected.					○	page 15-205
951F0000 hex	Clear All Memory Rejected	Clearing all of memory failed.	• The Clear All Memory operation for a Controller or a Slave Terminal was performed.					○	page 15-205

● User Access Log

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
90400000 hex	Event Log Cleared	The event log was cleared.	• The event log was cleared by the user.					○	page 15-206
90430000 hex	Memory All Cleared	The Unit settings were cleared.	• The Clear All Memory operation was performed.					○	page 15-206

Error Descriptions

Details on the errors (events) that can occur in the Safety CPU Unit are given in the following tables.

● System Error

<table>
<tr><td>Event name</td><td colspan="3">System Error</td><td>Event code</td><td colspan="2">05200000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">A hardware error was detected during self-diagnosis of the hardware.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Cycle the power supply to the Unit.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The Unit stops operating and the I/O data changes to the safe states.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">Hardware has failed.
A memory error occurred due to a transient cause, such as a software error or excessive noise.</td><td colspan="2">Cycle the power supply. If the error occurs again, replace the Unit.</td><td colspan="2">If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: System information, status code
Attached information 2: System information, status code
Attached information 3: System information, status code
Attached information 4: System information, status code</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

● Communications Errors

Event name	FSoE Master Connection Not Established Error			**Event code**	35200001 hex	
Meaning	FSoE communications were not established with the FSoE slave.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	In DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery when cause of error is removed	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The Unit continues to operate, but the safe states are used for the I/O data of the safety connection where the error was detected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The FSoE communications settings are not correct, the FSoE slave is not in the correct status, etc.		Refer to the error for the FSoE slave and correct the problem.		Refer to the errors for the FSoE slaves and implement countermeasures.	
	The FSoE slave for FSoE communications is not connected.		Make sure the FSoE slave is connected correctly.		Make sure that all of the FSoE slaves to communicate with are connected before you change the Safety CPU Unit to DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode.	
	The FSoE slave set in the NX Unit Mounting Setting for FSoE communications is disabled.		Set the disabled FSoE slaves in the NX Unit Mounting Setting so that they do not participate in FSoE communications and then transfer the data to the Safety CPU Unit.		Set the disabled FSoE slaves in the NX Unit Mounting Setting so that they do not participate in FSoE communications.	
	The version of the FSoE slave to be communicated is older than the configured version.		Change the version of the FSoE slave in the project to the version of the FSoE to be communicated, and then transfer the setting to the Safety CPU Unit again. Or, replace to a Unit that has a newer version than the Unit that is set with the FSoE salve to be communicated.		Keep the version of the FSoE slave in the project consistent with the version of the FSoE slave to be communicated.	
Attached information	None					
Precautions/ Remarks	The relevant Units will maintain the safe states for I/O data with FSoE connections after an error is detected. However, when the cause of the error is removed, FSoE communications will recover automatically.					

<table>
<tr><td>Event name</td><td colspan="3">NX Unit I/O Communications Error</td><td>Event code</td><td colspan="2">80200000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An I/O communications error occurred between the NX bus master and the NX Unit.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Support Software is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td rowspan="2">Error attributes</td><td>Level</td><td colspan="2">Minor fault</td><td>Log category</td><td colspan="2">System</td></tr>
<tr><td>Recovery</td><td colspan="5">[NX Bus of the CPU Unit]
[Fail-soft Operation Setting is Stop]
Errors are reset in the NX Bus Function Module.
[Fail-soft Operation Setting is Fail-soft Operation]
Errors are reset in the NX Unit.
[Communications Coupler Unit]
[Fail-soft Operation Setting is Stop]
If errors are detected in the controller, errors are reset in the controller.
If errors are not detected in the controller, errors are reset in the Communications Coupler Unit and the NX Unit.
[Fail-soft Operation Setting is Fail-soft Operation]
Errors are reset in the Communications Coupler Unit and the NX Unit.</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The NX Unit will continue to operate.
Input data: Updating input values stops.
Output data: The output values depend on the Load Rejection Output Setting.</td></tr>
<tr><td>System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="9">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="6">[NX Bus of the CPU Unit]</td></tr>
<tr><td colspan="2">An error occurred in the CPU Unit, which prevents the NX bus communications from being carried out normally.</td><td colspan="2">Check the error in the CPU Unit and try the solutions specified in Correction.</td><td colspan="2">Try the solutions specified in Prevention for the error in the CPU Unit.</td></tr>
<tr><td colspan="2">The NX Unit is not mounted properly.</td><td colspan="2">Mount the NX Units and End Cover securely and secure them with End Plates.</td><td colspan="2">Mount the NX Units and End Cover securely and secure them with End Plates.</td></tr>
<tr><td colspan="2">The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect.</td><td colspan="2">Correctly wire the Unit power supply to the NX Units.</td><td colspan="2">Correctly wire the Unit power supply to the NX Units.</td></tr>
<tr><td colspan="2">The power cable for the Unit power supply is broken.</td><td colspan="2">If the power cable connecting the Unit power supply and the NX Units is broken, replace the power cable.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient.</td><td colspan="2">Configure the power supply system correctly in accordance with the power supply specifications.</td><td colspan="2">Configure the power supply system correctly in accordance with the power supply specifications.</td></tr>
<tr><td colspan="2">There is a hardware error in the NX Unit.</td><td colspan="2">If the error occurs again even after you make the above correction, replace the NX Unit.</td><td colspan="2">None</td></tr>
</table>

Cause and correction	[Communications Coupler Unit]		
	An error occurred in the Communications Coupler Unit, which prevents the NX bus communications from being carried out normally.	Check the error in the Communications Coupler Unit and try the solutions specified in Correction.	Try the solutions specified in Prevention for the error in the Communications Coupler Unit.
	The NX Unit is not mounted properly.	Mount the NX Units and End Cover securely and secure them with End Plates.	Mount the NX Units and End Cover securely and secure them with End Plates.
	The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect.	Correctly wire the Unit power supply to the NX Units.	Correctly wire the Unit power supply to the NX Units.
	The power cable for the Unit power supply is broken.	If the power cable connecting the Unit power supply and the NX Units is broken, replace the power cable.	None
	The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient.	Configure the power supply system correctly in accordance with the power supply specifications.	Configure the power supply system correctly in accordance with the power supply specifications.
	There is a hardware error in the NX Unit.	If the error occurs again even after you make the above correction, replace the NX Unit.	None
Attached information	None		
Precautions/ Remarks	None		

Event name	FSoE Master Connection Timeout			**Event code**	80300001 hex	
Meaning	A communication timeout occurred in FSoE communications with the FSoE slave.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	In DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery when cause of error is removed	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The Unit continues to operate, but the safe states are used for the I/O data of the safety connection where the error was detected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	A setting is not correct. The setting of the safety task period is too short.		Increase the safety task period and then transfer the settings to the Safety CPU Unit.		Set the system configuration and setup according to the corrections that are given on the left.	
	There is excessive noise.		Implement noise countermeasures.		Implement noise countermeasures if excessive noise caused the error.	
	The Safety CPU Unit or FSoE slave entered a state where it could not continue FSoE communications.		Check the status of the Safety CPU Unit or FSoE slave.		Refer to troubleshooting information for the Safety CPU Unit or FSoE slave.	
	The process data communications were not performed correctly because an error or status change occurred in the NX bus master to which the Unit is connected.		Check the status of the NX bus master to which the Unit is connected.		Set the system configuration and setup according to the corrections that are given on the left.	
Attached information	None					
Precautions/ Remarks	The relevant Units will maintain the safe states for I/O data with FSoE connections after an error is detected. However, when the cause of the error is removed, FSoE communications will recover automatically.					

Event name	CIP Safety Originator Connection Not Established Error			Event code	80310000 hex	
Meaning	CIP safety originator connection was not established.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode
Error attributes	Level	Minor fault	Recovery	Automatic recovery when cause of error is removed	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate, but the safe states are used for the I/O data of the safety connection where the error was detected.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The target node is different.		Check if the target node is correct.		Set the system configuration and setup according to the corrections that are given on the left.	
	The target node is not configured.		Check if the target node is configured.			
	The target node is not in the correct status.		Check if the target node is in a state where it can accept the connection.			
	The **Do not use** Option is selected for CIP message server setting in the EtherNet/IP Port Settings.		Check if the **Use** Option is selected for the CIP message server setting in the EtherNet/IP Port Settings.			
	The settings of the NX-series CPU Unit and NX-series EtherNet/IP Unit related to CIP Safety communications do not match the settings of the Safety CPU Unit.		Enable transfer of the settings for X Bus Units (settings of CIP Safety connections) in the Synchronization Window on the Sysmac Studio, and check whether they are downloaded.			
	Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings.		Do not make the setting to use tag data link communications to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings.			
	The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings.		Do not add the NX-series EtherNet/IP Unit with tag data link communications to the CIP Safety connection settings.			
	The **Do not use** Option is selected for CIP Safety communications in the Built-in EtherNet/IP Port Settings.		Check if the **Use** Option is selected for the CIP safety communication setting in the Built-in EtherNet/IP Port Settings.			

Attached information	Attached information 1:	IP address of the target node (example: C0A8FA01 hex = address 192.168.250.1)
	Attached information 2:	General Status defined in CIP specifications
	Attached information 3:	Extended Status defined in CIP specifications
Precautions/ Remarks	None	

Event name	CIP Safety Originator Connection Timeout			Event code	80320000 hex	
Meaning	A timeout occurred in CIP safety originator connection.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode
Error attributes	Level	Minor fault	Recovery	Automatic recovery when cause of error is removed	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate, but the safe states are used for the I/O data of the safety connection where the error was detected.		

System-defined variables	Variable	Data type	Name
	None	None	None

Cause and correction	Assumed cause	Correction	Prevention
	The communications cable is disconnected or broken.	Connect the communications cable securely.	Set the system configuration and setup according to the corrections that are given on the left.
	The target node entered a status where it could not accept the connection.	Check if the target node is in a state where it can accept the connection.	
	The timeout value for the communications settings is too small.	Increase the timeout value in the communications setup and transfer the settings.	
	CIP message communications at the target node are stopped.	Check if CIP message communications are started at the target node.	
	When the Packet Filter function is enabled in the EtherNet/IP Port Settings, CIP Safety packets from the target node are not allowed.	Allow CIP Safety packets from the target node in the Packet Filter settings of the EtherNet/IP Port Settings.	
	CIP Safety packets are not allowed by the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path.	Allow CIP Safety packets in the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path.	
	There is excessive noise.	Implement noise countermeasures.	

Attached information	Attached information 1:	IP address of the target node (example: C0A8FA01 hex = address 192.168.250.1)
Precautions/ Remarks	None	

Event name	CIP Safety Target Does Not Exist		Event code	80330000 hex	
Meaning	The target node does not exist.				
Source	Depends on where the Sysmac Studio is connected and the system configuration.	Source details	NX Unit	Detection timing	In DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode
Error attributes	Level: Minor fault	Recovery	Automatic recovery when cause of error is removed	Log category	System
Effects	User program: Continues.	Operation	The Unit continues to operate, but the safe states are used for the I/O data of the safety connection where the error was detected.		

System-defined variables	Variable	Data type	Name
	None	None	None

Cause and correction	Assumed cause	Correction	Prevention
	The communications cable is disconnected or broken.	Connect the communications cable securely.	Set the system configuration and setup according to the corrections that are given on the left.
	The target node entered a state where it could not accept the connection.	Check if the target node is in a state where it can accept the connection.	
	The timeout value for the communications settings is too small.	Increase the timeout value in the communications setup and transfer the settings.	
	CIP message communications at the target node are stopped.	Check if CIP message communications are started at the target node.	
	CIP Safety packets from the originator node are not allowed by the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path.	Allow CIP Safety packets from the originator node in the Packet Filter (Simple) or Packet Filter functions on the target node or the devices on the communication path.	
	There is excessive noise.	Implement noise countermeasures.	

Attached information		
	Attached information 1:	IP address of the target node (example: C0A8FA01 hex = address 192.168.250.1)
	Attached information 2:	General Status defined in CIP specifications
	Attached information 3:	Extended Status defined in CIP specifications

Precautions/ Remarks	None

Event name	CIP Safety Target Connection Timeout			Event code	80340000 hex	
Meaning	A timeout occurred in the CIP Safety Target connection.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (STOPPED), DEBUG mode (RUN), or RUN mode
Error attributes	Level	Minor fault	Recovery	Automatic recovery when cause of error is removed	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate, but the safe states are used for the I/O data of the safety connection where the error was detected.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The communications cable is disconnected or broken.		Connect the communications cable securely.		Set the system configuration and setup according to the corrections that are given on the left.	
	The originator device entered a status where it could not accept the connection.		Check if the originator device is in a state where it can accept the connection.			
	The timeout value for the communications settings is too small.		Increase the timeout value in the communications setup and transfer the settings.			
	CIP Safety packets from the originator node are not allowed by the Packet Filter (Simple) or Packet Filter functions in the EtherNet/IP Port Settings or on the devices on the communication path.		Allow CIP Safety packets from the originator node in the Packet Filter (Simple) or Packet Filter functions in the EtherNet/IP Port Settings or on the devices on the communication path.			
	The CIP message server setting for the originator node is set to **Do not use**.		Set the CIP message server setting of the originator node to **Use**.			
	When the Packet Filter function of the originator node is enabled, CIP Safety packets from the target node are not allowed.		Allow CIP Safety packets from the target node in the Packet Filter function of the originator node.			
	There is excessive noise.		Implement noise countermeasures.			
	The **Do not use** Option is selected for CIP Safety communications in the Built-in EtherNet/IP Port Settings.		Check if the **Use** Option is selected for the CIP safety communication setting in the Built-in EtherNet/IP Port Settings.			
Attached information	Attached information 1:	Assembly Instance No. 0300 hex: Input Assembly 1 0301 hex: Input Assembly 2 0302 hex: Input Assembly 3 03A0 hex: Output Assembly 1				
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="2">NX Bus I/O Communications Stopped</td><td>Event code</td><td colspan="2">84F00000 hex</td></tr>
<tr><td>Meaning</td><td colspan="5">An error occurred in I/O communications between the NX bus master and an NX Unit.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Cycle the power supply to the NX bus master and NX Units.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The NX Units will continue to operate.
• Input data:
An error occurs in safety process data communications because refreshing is stopped. The values of the status and exposed variables in the standard process data are not refreshed.
• Output data:
An error occurs in safety process data communications because 0’s are output.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td>Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td>None</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td>Prevention</td></tr>
<tr><td colspan="2">There is a hardware error in the NX bus master or an NX Unit.</td><td colspan="2">If the error occurs again even after you cycle the power supply to the NX Units, replace the NX bus master or the NX Unit.</td><td>None</td></tr>
<tr><td>Attached information</td><td colspan="5">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="5">None</td></tr>
</table>

● Operation Continuation Error Related to Program Execution Function

Event name	SF_Antivalent Error			Event code	74A00000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: DiagCode					
Precautions/ Remarks	None					

Event name	SF_EDM Error			Event code	74A10000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: DiagCode					
Precautions/ Remarks	None					

Event name	SF_EmergencyStop Error		Event code	74A20000 hex	
Meaning	An error was detected in execution of a safety function block.				
Source	Depends on where the Sysmac Studio is connected and the system configuration.	Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.	
System-defined variables	Variable		Data type	Name	
	None		None	None	
Cause and correction	Assumed cause		Correction	Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.	Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code				
Precautions/ Remarks	None				

Event name	SF_EnableSwitch Error		Event code	74A30000 hex	
Meaning	An error was detected in execution of a safety function block.				
Source	Depends on where the Sysmac Studio is connected and the system configuration.	Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.	
System-defined variables	Variable		Data type	Name	
	None		None	None	
Cause and correction	Assumed cause		Correction	Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.	Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code				
Precautions/ Remarks	None				

Event name	SF_Equivalent Error			Event code	74A40000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_ESPE Error			Event code	74A50000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_GuardLocking Error			Event code	74A60000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_GuardMonitoring Error			Event code	74A70000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_ModeSelector Error			Event code	74A80000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_MutingPar Error			Event code	74A90000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_MutingPar_2Sensor Error			Event code	74AA0000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_MutingSeq Error			Event code	74AB0000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_OutControl Error			Event code	74AC0000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_SafetyRequest Error			Event code	74AD0000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_TestableSafetySensor Error			Event code		74AE0000 hex
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_TwoHandControlTypeII Error			Event code		74AF0000 hex
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

Event name	SF_TwoHandControlTypeIII Error			Event code	74B00000 hex	
Meaning	An error was detected in execution of a safety function block.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	In DEBUG mode (RUN) or RUN mode
Error attributes	Level	Minor fault	Recovery	Implement the correction.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	Refer to information on the diagnostic code that is given for attached information 1 in the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931)*.		Implement the correction for the relevant cause of the diagnostic code that is given for attached information 1.		Program operation considering the corrections that are given on the left.	
Attached information	Attached information 1: Diagnostic code					
Precautions/ Remarks	None					

● Operation Stop Error Related to Program Execution

Event name	Division by Zero			**Event code**	55000000 hex	
Meaning	Division by zero was detected.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	In DEBUG mode (RUN) or RUN mode
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The CPU Unit executes NX bus communications but execution of the user program stops. (All I/O data will remain at 0.)		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The divisor is zero.		Correct the program so that the divisor is not 0. Perform the following corrections according to the operating mode of the Safety CPU Unit. • RUN mode: Change to PROGRAM mode and transfer the corrected user program. • DEBUG mode (RUN): Change to PROGRAM mode and transfer the corrected user program.		Program operation considering the corrections that are given on the left.	
Attached information	None					
Precautions/ Remarks	The CPU Unit executes NX bus communications but execution of the user program stops. (All I/O data will remain at 0.)					

<table>
<tr><td>Event name</td><td colspan="3">Cast Error</td><td>Event code</td><td colspan="2">55010000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">A casting error was detected.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>In DEBUG mode (RUN) or RUN mode</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Automatic recovery</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The CPU Unit executes NX bus communications but execution of the user program stops. (All I/O data will remain at 0.)</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">A value was input that exceeded the range of the receiving variable.</td><td colspan="2">Do not allow the value to exceed the range of the receiving variable.
Perform the following corrections according to the operating mode of the Safety CPU Unit.
• RUN mode: Change to PROGRAM mode and transfer the corrected user program.
• DEBUG mode (RUN): Change to PROGRAM mode and transfer the corrected user program.</td><td colspan="2">Program operation considering the corrections that are given on the left.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Error details

0x01000ADF: The conversion between the signed and unsigned data types was failed.
0x01000AE0: The positive upper limit of the data type after conversion was exceeded.
0x01000AE1: The negative upper limit of the data type after conversion was exceeded.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">The CPU Unit executes NX bus communications but execution of the user program stops. (All I/O data will remain at 0.)</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="2">MUX Error</td><td>Event code</td><td colspan="2">55020000 hex</td></tr>
<tr><td>Meaning</td><td colspan="5">An MUX instruction error was detected.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>In DEBUG mode (RUN) or RUN mode</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Automatic recovery</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The CPU Unit executes NX bus communications but execution of the user program stops. (All I/O data will remain at 0.)</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The value of the selection input (K) to the MUX instruction is not correct.</td><td colspan="2">Correct the program so that the value of the selection input (K) to the MUX instruction is in range. Perform the following corrections according to the operating mode of the Safety CPU Unit.
• RUN mode: Change to PROGRAM mode and transfer the corrected user program.
• DEBUG mode: Change to PROGRAM mode and transfer the corrected user program.</td><td colspan="2">Program operation considering the corrections that are given on the left.</td></tr>
<tr><td>Attached information</td><td>Attached information 1:</td><td colspan="5">0x01000ADD: The value of the selection input (K) is negative.
0x01000ADE: The value of the selection input (K) exceeded the upper limit of the selection range.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">The CPU Unit executes NX bus communications but execution of the user program stops. (All I/O data will remain at 0.)</td></tr>
</table>

● Setting Errors

Event name	NX Bus Communications Settings Read Error			Event code	10500000 hex	
Meaning	There is an error in the NX bus communications settings that are saved in non-volatile memory.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	At power ON or restart
Error attributes	Level	Minor fault	Recovery	When settings are transferred	Log category	System
Effects	User program	Continues.	Operation	I/O refreshing stops for the Safety CPU Unit.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	A hardware failure occurred in the non-volatile memory.		Transfer the configuration information to the Safety CPU Unit again. Replace the CPU Unit if the error occurs again.		None	
	Power was turned OFF while saving data to the non-volatile memory.				Do not turn OFF the power supply while transferring parameters from the Sysmac Studio.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Safety Application Data Read Error			Event code	10510000 hex	
Meaning	There is an error in the safety application data that is saved in non-volatile memory.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	At power ON or restart
Error attributes	Level	Minor fault	Recovery	When settings are transferred	Log category	System
Effects	User program	Continues.	Operation	The safety program is not executed in the Safety CPU Unit and it operates in PROGRAM mode.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	A hardware failure occurred in the non-volatile memory.		Transfer the safety application data to the Safety CPU Unit again.		None	
	Power was turned OFF while saving data to the non-volatile memory.				Do not turn OFF the power supply while transferring parameters from the Sysmac Studio.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">NX Bus Communications Settings and Safety Application Data Mismatch</td><td>Event code</td><td colspan="2">10520000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">There is an error in the safety application data that is saved in non-volatile memory.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>When applicable</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>When settings are transferred</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The Safety CPU Unit executes NX bus communications with the relevant Units but refreshing for the safety program stops. (All I/O data will remain at 0.)</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The NX bus communications settings that were transferred to the Safety CPU Unit do not match the safety application data.</td><td colspan="2">Transfer the Slave Terminal configuration information and the safety application data to the Safety CPU Unit again.</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

If you cannot resolve the *NX Bus Communications Settings and Safety Application Data Mismatch* after you implement the normal correction, refer to *A-18 Safety: Update Configurations and Setup Transfer Data* on page A-111.

Event name	Non-volatile Memory Access Error			Event code	10530000 hex	
Meaning	Reading/writing non-volatile memory failed.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	When power is turned ON to the NX Unit, when the operating mode is changed, or when Clear All Memory is executed for NX Unit
Error attributes	Level	Minor fault	Recovery	Clear All Memory operation for the Unit	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	Non-volatile memory failure.		Perform the Clear All Memory operation or download the settings again. Replace the CPU Unit if the error occurs again.		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	Incorrect DIP Switch Setting			Event code	24AA0000 hex	
Meaning	The DIP switch setting is not correct.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	At startup
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	---		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The DIP switch setting was changed to an incorrect value.		Check the DIP switch setting and change the value to a correct value.		If you change the DIP switch setting, make sure that the DIP switch setting that you changed is correct.	
Attached information	Attached information 1:	DIP switch set value				
Precautions/ Remarks	None					

● Other Errors

<table>
<tr><td>Event name</td><td colspan="2">NX Message Communications Error</td><td>Event code</td><td colspan="2">80220000 hex</td></tr>
<tr><td>Meaning</td><td colspan="5">An error was detected in message communications for an NX Unit and the message frame was discarded.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During NX message communications</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">Not affected.</td></tr>
<tr><td>System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td>Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td></td><td colspan="2">The message communications load is high.</td><td colspan="2">Reduce the number of times that instructions are used to send NX messages.
Refer to the appendix of the NJ/NX-series Instructions Reference Manual (Cat. No. W502) for information on the instructions that send messages.</td><td colspan="2">Reduce the number of times that instructions are used to send NX messages.</td></tr>
<tr><td></td><td colspan="2">The communications cable is disconnected or broken. This cause does not apply if attached information 2 is 0 (NX bus).</td><td colspan="2">Connect the communications cable securely</td><td colspan="2">Connect the communications cable securely.</td></tr>
<tr><td></td><td colspan="2">Message communications were cut off as the result of executing a synchronization or restoration operation on the Sysmac Studio or as the result of disconnecting an EtherCAT slave.</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td>Attached information</td><td>Attached information 1:</td><td colspan="5">System information</td></tr>
<tr><td></td><td>Attached information 2:</td><td colspan="5">Type of communications where error occurred
0: NX bus
1: EtherCAT
2: Serial communications (USB)
65535: Internal Unit communications (routing)</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Sysmac Studio Communications Connection Timeout		Event code	951E0000 hex		
Meaning	A communications timeout occurred between the Sysmac Studio and the Safety CPU Unit.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	When applicable
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	If the CPU Unit was in DEBUG mode, it automatically enters PROGRAM mode.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The communications cable was disconnected.		Do not do anything to disconnect communications with the Sysmac Studio while the Safety CPU Unit is operating in DEBUG mode.		Perform debugging considering the corrections that are given on the left.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Clear All Memory Rejected		Event code	951F0000 hex		
Meaning	Clearing all of memory failed.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	When commanded from user
Error attributes	Level	Information	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	---		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The Clear All Memory operation for a Controller or a Slave Terminal was performed.		Specify the Units individually and perform the Clear All Memory operation.		Specify the Units individually and perform the Clear All Memory operation.	
Attached information	Attached information 1: The Clear All Memory operation for the Controller or the Slave Terminal was performed.					
Precautions/ Remarks	The Clear All Memory operation for the Safety CPU Unit cannot be performed for the Controller or the Slave Terminal.					

● User Access Log

Event name	Event Log Cleared			**Event code**	90400000 hex	
Meaning	The event log was cleared.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When commanded from user
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The event log was cleared by the user.		---		---	
Attached information	Attached information 1:	Events that were cleared. 1: The system event log was cleared. 2: The access event log was cleared.				
Precautions/ Remarks	None					

Event name	Memory All Cleared			**Event code**	90430000 hex	
Meaning	The Unit settings were cleared.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When commanded from user
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	The Unit settings are cleared.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The Clear All Memory operation was performed.		---		---	
Attached information	Attached information 1:	Unit number of the NX Unit where the Clear All Memory operation was performed				
	Attached information 2:	Execution results 0: Successful 1: Hardware error 2: Initialization failed 3: Initialization not possible				
Precautions/ Remarks	Refer to the attached information for the results of the Clear All Memory operation.					

● Errors Related to Restore Function

Event name	Safety Unit Restore Operation Failed to Start (SD Memory Card Access Failed)			**Event code**	35250000 hex	
Meaning	Access to the SD Memory Card failed when you start the restore operation for a Safety Unit.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When Safety Unit restoring data is specified by the user
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	---		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	An SD Memory Card is not inserted.		Insert an SD Memory Card.		Insert an SD Memory Card.	
	The SD Memory Card type is not correct.		Replace the SD Memory Card with an SD or SDHC card.		Use an SD or SDHC card.	
	The format of the SD Memory Card is not correct.		Format the SD Memory Card with the Sysmac Studio.		Use a formatted SD Memory Card.	
	The SD Memory Card is damaged.		If none of these causes apply, replace the SD Memory Card.		Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit. Replace the SD Memory Card periodically according to the write life of the SD Memory Card.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Safety Unit Restore Operation Failed to Start (Safety Unit Restore File Read Failure)</td><td>Event code</td><td colspan="2">35260000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">Reading the Safety Unit Restore File failed.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>When Safety Unit restoring data is specified by the user</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">---</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The Safety Unit Restore File is not stored in the specified folder.</td><td colspan="2">Store the Safety Unit Restore File in the specified folder again.</td><td colspan="2" rowspan="2">Use a formatted SD Memory Card and store the Safety Unit Restore File in the specified folder. Do not edit the Safety Unit Restore File.
Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit.</td></tr>
<tr><td colspan="2">The Safety Unit Restore File is corrupted.</td><td colspan="2">Create the Safety Unit Restore File again.</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="2">Safety Unit Restore Operation Failed to Start (Model Mismatch)</td><td>Event code</td><td colspan="2">35270000 hex</td></tr>
<tr><td>Meaning</td><td colspan="5">A model mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>When Safety Unit restoring data is specified by the user</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">---</td></tr>
<tr><td>System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td>Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td></td><td colspan="2">The restore operation for a Safety Unit was performed on an incorrect Unit.</td><td colspan="2">After making sure that the destination is set to an intended unit, cycle the power supply and then perform the restore operation for a Safety Unit again.</td><td colspan="2">After making sure that the destination is set to an intended unit, start the restore operation for a Safety Unit.</td></tr>
<tr><td></td><td colspan="2">An incorrect Safety Unit Restore File was used.</td><td colspan="2">On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card.
After making sure that the safety signature is the intended signature, cycle the power supply and then perform the restore operation for a Safety Unit again.</td><td colspan="2">On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card. After making sure that the safety signature is the intended signature, start the restore operation for a Safety Unit.</td></tr>
<tr><td>Attached information</td><td colspan="5">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="5">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="3">Safety Unit Restore Operation Failed to Start (Version Mismatch)</td><td>Event code</td><td colspan="2">35280000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">A version mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>When Safety Unit restoring data is specified by the user</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">---</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The restore operation for a Safety Unit was performed on an incompatible unit.</td><td colspan="2">After making sure that the destination is set to a compatible unit, cycle the power supply and then perform the restore operation for a Safety Unit again.</td><td colspan="2">After making sure that the destination is set to a compatible unit, start the restore operation for a Safety Unit.</td></tr>
<tr><td colspan="2">An incorrect Safety Unit Restore File was used.</td><td colspan="2">On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card.
After making sure that the safety signature is the intended signature, cycle the power supply and then perform the restore operation for a Safety Unit again.</td><td colspan="2">On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card. After making sure that the safety signature is the intended signature, start the restore operation for a Safety Unit.</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Safety Unit Restore Operation Failed to Start (Node Name Mismatch)			**Event code**	35290000 hex	
Meaning	A node name mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When Safety Unit restoring data is specified by the user
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	---		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The restore operation for a Safety Unit was performed on an incorrect Unit.		After making sure that the destination is set to an intended unit, cycle the power supply and then perform the restore operation for a Safety Unit again.		After making sure that the destination is set to an intended unit, start the restore operation for a Safety Unit.	
	An incorrect Safety Unit Restore File was used.		On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card. After making sure that the safety signature is the intended signature, cycle the power supply and then perform the restore operation for a Safety Unit again.		On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card. After making sure that the safety signature is the intended signature, start the restore operation for a Safety Unit.	
	The node name specified when the Safety Unit Restore File was generated is incorrect.		Specify a correct node name for the Safety Unit Restore File.		When you enter a node name, visually check that the specified node name is correct.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Safety Unit Restore Operation Failed to Start (Safety Password Mismatch)		**Event code**	352A0000 hex		
Meaning	A safety password mismatch was detected during pre-execution checks for a restore operation for a Safety Unit.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When Safety Unit restoring data is specified by the user
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	---		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The restore operation for a Safety Unit was performed on an incorrect Unit.		After making sure that the destination is set to an intended unit, cycle the power supply and then perform the restore operation for a Safety Unit again.		After making sure that the destination is set to an intended unit, start the restore operation for a Safety Unit.	
	An incorrect Safety Unit Restore File was used.		On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card. After making sure that the safety signature is the intended signature, cycle the power supply and then perform the restore operation for a Safety Unit again.		On the front indicators of the Safety CPU Unit, check the safety signature for the Safety Unit Restore File that is stored in the SD Memory Card. After making sure that the safety signature is the intended signature, start the restore operation for a Safety Unit.	
	The safety password specified when the Safety Unit Restore File was generated is incorrect.		Specify a correct safety password for the Safety Unit Restore File.		Specify a correct password when you enter the safety password.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Safety Unit Restore Operation Failed			Event code	352B0000 hex	
Meaning	The restore operation for a Safety Unit ended in an error.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	When Safety Unit restoring data is specified by the user
Error attributes	Level	Observation	Recovery	---	Log category	System
Effects	User program	Continues.	Operation	---		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The SD Memory Card was removed during a restore operation for a Safety Unit.		Insert the SD Memory Card that contains the Safety Unit Restore File, cycle the power supply and then perform the restore operation for a Safety Unit again.		Do not remove the SD Memory Card during the restore operation for a Safety Unit.	
	Data was read from or written to the SD Memory Card via the Support Software or an FTP client during a restore operation for a Safety Unit.		Store the correct Safety Unit Restore File to the SD Memory Card, cycle the power supply and then perform the restore operation for a Safety Unit again.		Do not read data from or write data to the SD Memory Card via the Support Software or an FTP client during the restore operation for a Safety Unit.	
Attached information	None					
Precautions/ Remarks	None					

15-3-4 Safety I/O Unit Error

Error Table

The errors (events) that can occur in the Safety I/O Units are listed in the following tables.

● System Error

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
05200000 hex	System Error	A hardware error was detected during self-diagnosis of the hardware.	• Hardware has failed. • A memory error occurred due to a transient cause, such as a software error or excessive noise.			○			page 15-219

● Communications Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
35210000 hex	Safety Process Data Communications Not Established - Incorrect Unit Parameter Error	Safety process data communications was not established with the Safety CPU Unit.	• The model or safety I/O terminal settings are not correct.			○			page 15-220
35230000 hex	Safety Process Data Communications Not Established, Incorrect FSoE Slave Address Error	Safety process data communications was not established with the Safety CPU Unit because of an incorrect FSoE slave address.	• The setting of the FSoE slave address in the safety process data communications settings is different from the setting in the Unit.			○			page 15-221
35240000 hex	Safety Process Data Communications Not Established, Incorrect Frame Error	Safety process data communications were not established with the Safety CPU Unit because an incorrect frame was received.	• An incorrect frame was received in safety process data communications. • There is excessive noise.			○			page 15-222

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80200000 hex	NX Unit I/O Communications Error	An I/O communications error occurred in an NX Unit.	NX Bus of the CPU Unit • An error occurred in the CPU unit, which prevents the NX bus communications from being carried out normally. • The NX Unit is not mounted properly. • The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect. • The power cable for the Unit power supply is broken. • The unit power voltage is out of the supported range, or the unit power capacity is not sufficient. • There is a hardware error in the NX Unit. Communications Coupler Unit • An error occurred in the communications coupler unit, which prevents the NX bus communications from being carried out normally. • The NX Unit is not mounted properly. • The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect. • The power cable for the Unit power supply is broken. • The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient. • There is a hardware error in the NX Unit.			○			page 15-223

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80300000 hex	Safety Process Data Communications Timeout	A communications timeout occurred in safety process data communications with the Safety Control Unit.	• A setting is not correct. The setting of the safety task period is too short. • There is excessive noise. • The Safety CPU Unit or safety slave entered a status where it could not continue safety process data communications. • The process data communications were not performed correctly because an error or status change occurred in the NX bus master to which the Unit is connected.			○			page 15-225
84F10000 hex	NX Bus I/O Communications Stopped	An error occurred in I/O communications between the NX bus master and an NX Unit.	There is a hardware error in the NX bus master or an NX Unit.			○			page 15-226

● Safety I/O Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
05210000 hex	Internal Circuit Error at Safety Input	A fault was detected in the internal circuit for the safety input terminal.	• The internal circuit for the safety input terminal is faulty. • A memory error or signal error occurred due to a transient cause, such as an excessive noise.			○			page 15-227
05220000 hex	Internal Circuit Error at Test Output	A fault was detected in the internal circuit for the test output terminal.	• The internal circuit for the test output terminal is faulty. • A memory error or signal error occurred due to a transient cause, such as an excessive noise.			○			page 15-228
05230000 hex	Internal Circuit Error at Safety Output	A fault was detected in the internal circuit for the safety output terminal.	• The internal circuit for the safety output terminal is faulty. • A memory error or signal error occurred due to a transient cause, such as an excessive noise.			○			page 15-229
65200000 hex	I/O Power Supply Voltage Error	An incorrect I/O power supply voltage was detected.	• The input power or output power is not supplied correctly.			○			page 15-230
65210000 hex	Output Power Interrupt Circuit Error	An error was detected by the output power interruption test.	• The wiring is not correct or there is a fault in the hardware.			○			page 15-231

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
65220000 hex	External Test Signal Failure at Safety Input	An error was detected in test pulse evaluation of the safety input terminals.	• The positive power supply wire is in contact with the input signal line. • The input signal lines are shorted. • The external device is faulty. • An error occurred in the test output terminal used with the safety input terminal.			○			page 15-232
65230000 hex	Discrepancy Error at Safety Input	An error was detected in discrepancy evaluation of safety input terminals.	• There is a ground fault or disconnection in the input signal line. • The connected device is faulty. • The setting of the discrepancy time is not correct. • Chattering occurred in the input signal from the external input device, such as a safety door. • An error occurred in the test output terminal used with the safety input terminal.			○			page 15-233
65240000 hex	Overload Detected at Test Output	An overcurrent was detected at the test output terminal.	• There is a ground fault on the output signal line. • The external device is faulty.			○			page 15-234
65250000 hex	Stuck-at-high Detected at Test Output	It was detected that the test output terminal is stuck ON.	• The positive power supply line is in contact with the output signal line. • The internal circuit is faulty. • A memory error or signal error occurred due to a transient cause, such as a software error or excessive noise.			○			page 15-235
65270000 hex	Short Circuit Detected at Safety Output	A ground fault was detected on the safety output terminal.	• There is a ground fault on the output signal line.			○			page 15-236
65280000 hex	Stuck-at-high Detected at Safety Output	It was detected that the safety output terminal is stuck ON.	• The positive power supply line is in contact with the output signal line. • The output power supply is outside the specifications. • The internal circuit is faulty. • A memory error or signal error occurred due to a transient cause, such as a software error or excessive noise.			○			page 15-237

● Other Errors

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
80220000 hex	NX Message Communications Error	An error was detected in message communications for an NX Unit and the message frame was discarded.	• The message communications load is high. • The communications cable is disconnected or broken. • Message communications were cut off as the result of executing a synchronization or restoration operation on the Sysmac Studio or as the result of disconnecting an EtherCAT slave.				○		page 15-238

● User Access Log

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
90400000 hex	Event Log Cleared	The event log was cleared.	The event log was cleared by the user.					○	page 15-239
90430000 hex	Memory All Cleared	The Unit settings were cleared.	The Clear All Memory operation was performed.					○	page 15-239

Error Descriptions

Details on the errors (events) that can occur in the Safety I/O Units are given in the following tables.

● System Error

Event name	System Error			**Event code**	05200000 hex	
Meaning	A hardware error was detected during self-diagnosis of the hardware.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	Continuously
Error attributes	**Level**	Minor fault	**Recovery**	Cycle the power supply to the Unit.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The Unit stops operating and the I/O data changes to the safe states.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Hardware has failed.		Cycle the power supply. If the error occurs again, replace the Unit.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
	A memory error occurred due to a transient cause, such as a software error or excessive noise.					
Attached information	Attached information 1: System information, status code Attached information 2: System information, status code Attached information 3: System information, status code Attached information 4: System information, status code					
Precautions/ Remarks	None					

● Communications Errors

Event name	Safety Process Data Communications Not Established - Incorrect Unit Parameter Error			**Event code**	35210000 hex	
Meaning	Safety process data communications was not established with the Safety CPU Unit.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When safety process data communications are established
Error attributes	**Level**	Minor fault	**Recovery**	For request to establish communications from Safety CPU Unit after removing cause of error	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The Unit stops operating and the I/O data changes to the safe states.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The model or safety I/O terminal settings are not correct.		Check the safety I/O terminal settings, correct any errors, and then transfer the settings to the Safety CPU Unit.		Set the parameters considering the corrections that are given on the left.	
			Check the model of the Safety I/O Unit to see if it is correct.			
Attached information	None					
Precautions/ Remarks	None					

Event name	Safety Process Data Communications Not Established, Incorrect FSoE Slave Address Error			**Event code**	35230000 hex	
Meaning	Safety process data communications was not established with the Safety CPU Unit because of an incorrect FSoE slave address.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When safety process data communications are established
Error attributes	**Level**	Minor fault	**Recovery**	For request to establish communications from Safety CPU Unit after removing cause of error	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The Unit stops operating and the I/O data changes to the safe states.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The setting of the FSoE slave address in the safety process data communications settings is different from the setting in the Unit.		Perform the Clear All Memory operation for the Unit.		If you use a Safety I/O Unit for which safety process data communications were previously established in another system, perform the Clear All Memory operation before you use the Unit.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Safety Process Data Communications Not Established, Incorrect Frame Error</td><td>Event code</td><td colspan="2">35240000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">Safety process data communications was not established with the Safety CPU Unit because an incorrect frame was received.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>When safety process data communications are established</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>For request to establish communications from Safety CPU Unit after removing cause of error</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The Unit stops operating and the I/O data changes to the safe states.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">An incorrect frame was received in safety process data communications.</td><td colspan="2">Make sure that the system configurations and model numbers agree for the Safety CPU Unit and Safety I/O Units.</td><td colspan="2">Set the system configuration and setup according to the corrections that are given on the left.</td></tr>
<tr><td colspan="2">There is excessive noise.</td><td colspan="2">Implement noise countermeasures.</td><td colspan="2">Implement noise countermeasures if excessive noise caused the error.</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	NX Unit I/O Communications Error			**Event code**	80200000 hex	
Meaning	An I/O communications error occurred between the NX bus master and the NX Unit.					
Source	Depends on where the Support Software is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	Continuously
Error attributes	**Level**	Minor fault		**Log category**	System	
	Recovery	[NX Bus of the CPU Unit] When Fail-soft Operation Is Set to *Stop* Errors are reset in the NX Bus Function Module. When Fail-soft Operation Is Set to *Fail-soft* Reset the error in the NX Unit. [Communications Coupler Unit] When Fail-soft Operation Is Set to *Stop* If errors are detected in the controller, errors are reset in the controller. If errors are not detected in the controller, errors are reset in the Communications Coupler Unit and the NX Unit. When Fail-soft Operation Is Set to *Fail-soft* Errors are reset in the Communications Coupler Unit and the NX Unit.				
Effects	**User program**	Continues.	**Operation**	The NX Unit will continue to operate. Input data: Updating input values stops. Output data: The output values depend on the Load Rejection Output Setting.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	[NX Bus of the CPU Unit]					
	An error occurred in the CPU Unit, which prevents the NX bus communications from being carried out normally.		Check the error in the CPU Unit and try the solutions specified in Correction.		Try the solutions specified in Prevention for the error in the CPU Unit.	
	The NX Unit is not mounted properly.		Mount the NX Units and End Cover securely and secure them with End Plates.		Mount the NX Units and End Cover securely and secure them with End Plates.	
	The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect.		Correctly wire the Unit power supply to the NX Units.		Correctly wire the Unit power supply to the NX Units.	
	The power cable for the Unit power supply is broken.		If the power cable connecting the Unit power supply and the NX Units is broken, replace the power cable.		None	
	The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient.		Configure the power supply system correctly in accordance with the power supply specifications.		Configure the power supply system correctly in accordance with the power supply specifications.	
	There is a hardware error in the NX Unit.		If the error occurs again even after you make the above correction, replace the NX Unit.		None	

Cause and correction	[Communications Coupler Unit]		
	An error occurred in the Communications Coupler Unit, which prevents the NX bus communications from being carried out normally.	Check the error in the Communications Coupler Unit and try the solutions specified in Correction.	Try the solutions specified in Prevention for the error in the Communications Coupler Unit.
	The NX Unit is not mounted properly.	Mount the NX Units and End Cover securely and secure them with End Plates.	Mount the NX Units and End Cover securely and secure them with End Plates.
	The power cable for the Unit power supply is disconnected. Or, the wiring from the Unit power supply to the NX Units is incorrect.	Correctly wire the Unit power supply to the NX Units.	Correctly wire the Unit power supply to the NX Units.
	The power cable for the Unit power supply is broken.	If the power cable connecting the Unit power supply and the NX Units is broken, replace the power cable.	None
	The Unit power voltage is out of the supported range, or the Unit power capacity is not sufficient.	Configure the power supply system correctly in accordance with the power supply specifications.	Configure the power supply system correctly in accordance with the power supply specifications.
	There is a hardware error in the NX Unit.	If the error occurs again even after you make the above correction, replace the NX Unit.	None
Attached information	None		
Precautions/ Remarks	None		

Event name	Safety Process Data Communications Timeout			**Event code**	80300000 hex	
Meaning	A communications timeout occurred in safety process data communications with the Safety Control Unit.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When establishing or during safety process data communications
Error attributes	**Level**	Minor fault	**Recovery**	For request to establish communications from Safety CPU Unit after removing cause of error	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The Unit continues to operate. The safe states are used for the I/O data of the safety connection where the error was detected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	A setting is not correct. The setting of the safety task period is too short.		Increase the safety task period and then transfer the settings to the Safety CPU Unit.		Set the system configuration and setup according to the corrections that are given on the left.	
	There is excessive noise.		Implement noise countermeasures.		Implement noise countermeasures if excessive noise caused the error.	
	The Safety CPU Unit or safety slave entered a status where it could not continue safety process data communications.		Check the status of the Safety CPU Unit or safety slave.		Refer to troubleshooting information for the Safety CPU Unit or safety slave.	
	An error or status change occurred in the NX Bus Master to which the Unit is connected, preventing correct process data communications.		Check the status of the NX Bus Master to which the Unit is connected.		Set the system configuration and setup according to the corrections that are given on the left.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">NX Bus I/O Communications Stopped</td><td>Event code</td><td colspan="2">84F10000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An error occurred in I/O communications between the NX Bus Master and an NX Unit.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Cycle the power supply to the NX bus master and NX Units.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The NX Units will continue to operate.
• Input data:
An error occurs in safety process data communications because refreshing is stopped. The values of the status in standard process data are not refreshed.
• Output data:
An error occurs in safety process data communications because 0’s are output.</td></tr>
<tr><td>System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td>Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td></td><td colspan="2">There is a hardware error in the NX bus master or an NX Unit.</td><td colspan="2">If the error occurs again even after you cycle the power supply to the NX Units, replace the NX Bus Master or the NX Unit.</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

● Safety I/O Errors

Event name	Internal Circuit Error at Safety Input			**Event code**	05210000 hex	
Meaning	A fault was detected in the internal circuit for the safety input terminal.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	During refreshing
Error attributes	**Level**	Minor fault	**Recovery**	Cycle the power supply to the Unit.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The safety input terminal retains the safe state until the power supply is cycled.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The internal circuit for the safety input terminal is faulty.		Cycle the power supply. If the error occurs again, replace the Unit.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
	A memory error or signal error occurred due to a transient cause, such as an excessive noise.					
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Internal Circuit Error at Test Output</td><td>Event code</td><td colspan="2">05220000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">A fault was detected in the internal circuit for the test output terminal.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During refreshing</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Cycle the power supply to the Unit.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The test output terminal retains the safe state until the power supply is cycled. Also, an External Test Signal Failure at Safety Input event (65220000 hex) will occur for the safety input terminal that is the test source of the test output terminal.</td></tr>
<tr><td>System-defined Variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The internal circuit for the test output terminal is faulty.</td><td colspan="2" rowspan="2">Cycle the power supply. If the error occurs again, replace the Unit.</td><td colspan="2" rowspan="2">If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.</td></tr>
<tr><td colspan="2">A memory error or signal error occurred due to a transient cause, such as an excessive noise.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Terminal number</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="3">Internal Circuit Error at Safety Output</td><td>Event code</td><td colspan="2">05230000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">A fault was detected in the internal circuit for the safety output terminal.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During refreshing</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>Cycle the power supply to the Unit.</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The safety output terminal retains the safe state until the power supply is cycled.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The internal circuit for the safety output terminal is faulty.</td><td colspan="2" rowspan="2">Cycle the power supply. If the error occurs again, replace the Unit.</td><td colspan="2" rowspan="2">If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.</td></tr>
<tr><td colspan="2">A memory error or signal error occurred due to a transient cause, such as an excessive noise.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Terminal number</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="3">I/O Power Supply Voltage Error</td><td>Event code</td><td colspan="2">65200000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An incorrect I/O power supply voltage was detected.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During refreshing</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>When cause of error is removed</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The Unit continues to operate, but the I/O data retains the safe states.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="2">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The input power or output power is not supplied correctly.</td><td colspan="2">Check the following and supply the rated power.
• Is the power supply voltage within the specifications?
• Is the wiring correct and not disconnected?
• Is 24 V applied to the safety output terminal and is the safety output terminal not touching the positive power supply wire?
If the voltage that is measured is correct, the Unit may be faulty. In that case, replace the CPU Unit.</td><td colspan="2">Design the system considering the corrections that are given on the left.</td></tr>
<tr><td>Attached information</td><td colspan="6">None</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Output Power Interrupt Circuit Error		Event code	65210000 hex	
Meaning	An error was detected by the output power interruption test.				
Source	Depends on where the Sysmac Studio is connected and the system configuration.	Source details	NX Unit	Detection timing	During refreshing
Error attributes	Level	Minor fault	Recovery	When cause of error is removed and then one of the following is performed • The I/O power supply is turned OFF. • Safety process data communications are stopped.	Log category	System
Effects	User program	Continues.	Operation	The Unit continues to operate, but the I/O data retains the safe states.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	The wiring is not correct or there is a fault in the hardware.		Check the following and supply the rated power. • Is the power supply voltage within the specifications? • Is the wiring correct and not disconnected? • Is 24 V applied to the safety output terminal and is the safety output terminal not touching the positive power supply wire? If the voltage that is measured is correct, the Unit may be faulty. In that case, replace the CPU Unit.		Design the system considering the corrections that are given on the left.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">External Test Signal Failure at Safety Input</td><td>Event code</td><td colspan="2">65220000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An error was detected in test pulse evaluation of the safety input terminals.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During refreshing</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>When safety input terminal goes inactive after cause of error is removed</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The safety input terminal retains the safe state until the error is cleared.</td></tr>
<tr><td>System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="5">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">The positive power supply wire is in contact with the input signal line.</td><td colspan="2" rowspan="2">Check the external wiring.</td><td colspan="2" rowspan="3">Set the parameters and wire the system considering the corrections that are given on the left.</td></tr>
<tr><td colspan="2">The input signal lines are shorted.</td></tr>
<tr><td colspan="2">The external device is faulty.</td><td colspan="2">Replace the external device.</td></tr>
<tr><td colspan="2">An error occurred in the test output terminal used with the safety input terminal.</td><td colspan="2">Check the error in the test output terminal and try the solutions specified in Correction.</td><td colspan="2">Try the solutions specified in Prevention for the error in the test output terminal.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Terminal number</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Discrepancy Error at Safety Input			Event code	65230000 hex	
Meaning	An error was detected in discrepancy evaluation of safety input terminals.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	During refreshing
Error attributes	Level	Minor fault	Recovery	When safety input terminal goes inactive after cause of error is removed	Log category	System
Effects	User program	Continues.	Operation	The safety input terminal retains the safe state until the error is cleared.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	There is a ground fault or disconnection in the input signal line.		Check the external wiring.		Set the parameters and wire the system considering the corrections that are given on the left.	
	The connected device is faulty.		Replace the external device.			
	The setting of the discrepancy time is not correct.		Correct the setting of the discrepancy time. If that does not correct the problem, use an input filter to set an ON delay or an OFF delay.			
	Chattering occurred in the input signal from the external input device, such as a safety door.					
	An error occurred in the test output terminal used with the safety input terminal.		Check the error in the test output terminal and try the solutions specified in Correction.		Try the solutions specified in Prevention for the error in the test output terminal.	
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Overload Detected at Test Output</td><td>Event code</td><td colspan="2">65240000 hex</td></tr>
<tr><td>Meaning</td><td colspan="6">An overcurrent was detected at the test output terminal.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During refreshing</td></tr>
<tr><td rowspan="2">Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery</td><td>When safety input terminal goes inactive after cause of error is removed</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">The safety input terminal that is the test source of the test output terminal retains the safe state until the error is removed.</td></tr>
<tr><td rowspan="2">System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td rowspan="3">Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td colspan="2">There is a ground fault on the output signal line.</td><td colspan="2">Check the external wiring.</td><td colspan="2" rowspan="2">Set the parameters and wire the system considering the corrections that are given on the left.</td></tr>
<tr><td colspan="2">The external device is faulty.</td><td colspan="2">Replace the external device.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Terminal number</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Stuck-at-high Detected at Test Output		Event Code	65250000 hex	
Meaning	It was detected that the test output terminal is stuck ON.				
Source	Depends on where the Sysmac Studio is connected and the system configuration.	Source details	NX Unit	Detection timing	During refreshing
Error attributes	Level: Minor fault	Recovery	When safety input terminal goes inactive after cause of error is removed	Log category	System
Effects	User program: Continues.	Operation	The safety input terminal that is the test source of the test output terminal retains the safe state until the error is removed.		

System-defined variables	Variable	Data type	Name
	None	None	None

Cause and correction	Assumed cause	Correction	Prevention
	The positive power supply line is in contact with the output signal line.	Check the external wiring.	Set the parameters and wire the system considering the corrections that are given on the left.
	The internal circuit is faulty.	Cycle the power supply. If the error occurs again, replace the Unit.	If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.
	A memory error or signal error occurred due to a transient cause, such as a software error or excessive noise.		

Attached information	Attached information 1: Terminal number
Precautions/ Remarks	None

Event name	Short Circuit Detected at Safety Output			Event code	65270000 hex	
Meaning	A ground fault was detected on the safety output terminal.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		Source details	NX Unit	Detection timing	During refreshing
Error attributes	Level	Minor fault	Recovery	When safety output terminal goes inactive after cause of error is removed	Log category	System
Effects	User program	Continues.	Operation	The safety output terminal retains the safe state until the error is cleared.		
System-defined variables	Variable		Data type		Name	
	None		None		None	
Cause and correction	Assumed cause		Correction		Prevention	
	There is a ground fault on the output signal line.		Check the external wiring.		Set the parameters and wire the system considering the corrections that are given on the left.	
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

Event name	Stuck-at-high Detected at Safety Output		Event Code	65280000 hex	
Meaning	It was detected that the safety output terminal is stuck ON.				
Source	Depends on where the Sysmac Studio is connected and the system configuration.	Source details	NX Unit	Detection timing	During refreshing
Error attributes	Level: Minor fault	Recovery	When safety output terminal goes inactive after cause of error is removed	Log category	System
Effects	User program: Continues.	Operation	The safety output terminal retains the safe state until the error is cleared.		

System-defined variables	Variable	Data type	Name
	None	None	None

Cause and correction	Assumed cause	Correction	Prevention
	The positive power supply line is in contact with the output signal line.	Check the external wiring.	Set the parameters and wire the system considering the corrections that are given on the left.
	The output power supply is outside the specifications.	Check the output power supply.	
	The internal circuit is faulty.	Cycle the power supply. If the error occurs again, replace the Unit.	If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.
	A memory error or signal error occurred due to a transient cause, such as a software error or excessive noise.		

Attached information	Attached information 1: Terminal number
Precautions/ Remarks	None

● Other Errors

<table>
<tr><td>Event name</td><td colspan="2">NX Message Communications Error</td><td>Event code</td><td colspan="2">80220000 hex</td></tr>
<tr><td>Meaning</td><td colspan="5">An error was detected in message communications for an NX Unit and the message frame was discarded.</td></tr>
<tr><td>Source</td><td colspan="2">Depends on where the Sysmac Studio is connected and the system configuration.</td><td>Source details</td><td>NX Unit</td><td>Detection timing</td><td>During NX message communications</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Observation</td><td>Recovery</td><td>---</td><td>Log category</td><td>System</td></tr>
<tr><td>Effects</td><td>User program</td><td>Continues.</td><td>Operation</td><td colspan="3">Not affected.</td></tr>
<tr><td>System-defined variables</td><td colspan="2">Variable</td><td colspan="2">Data type</td><td colspan="2">Name</td></tr>
<tr><td></td><td colspan="2">None</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td>Cause and correction</td><td colspan="2">Assumed cause</td><td colspan="2">Correction</td><td colspan="2">Prevention</td></tr>
<tr><td></td><td colspan="2">The message communications load is high.</td><td colspan="2">Reduce the number of times that instructions are used to send NX messages.

Refer to the appendix of the NJ/NX-series Instructions Reference Manual (Cat. No. W502) for information on the instructions that send messages.</td><td colspan="2">Reduce the number of times that instructions are used to send NX messages.</td></tr>
<tr><td></td><td colspan="2">The communications cable is disconnected or broken. This cause does not apply if attached information 2 is 0 (NX bus).</td><td colspan="2">Connect the communications cable securely.</td><td colspan="2">Connect the communications cable securely.</td></tr>
<tr><td></td><td colspan="2">Message communications were cut off as the result of executing a synchronization or restoration operation on the Sysmac Studio or as the result of disconnecting an EtherCAT slave.</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: System information
Attached information 2: Type of communications where error occurred
0: NX bus
1: EtherCAT
2: Serial communications (USB)
65535: Internal Unit communications (routing)</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

● User Access Log

Event name	Event Log Cleared			**Event code**	90400000 hex	
Meaning	The event log was cleared.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When commanded from user
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The event log was cleared by the user.		---		---	
Attached information	Attached information 1:	Cleared events 1: The system event log was cleared. 2: The access event log was cleared.				
Precautions/ Remarks	None					

Event name	Memory All Cleared			**Event code**	90430000 hex	
Meaning	The Unit settings were cleared.					
Source	Depends on where the Sysmac Studio is connected and the system configuration.		**Source details**	NX Unit	**Detection timing**	When commanded from user
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	The Unit settings are cleared.		
System-defined variables	**Variable**		**Data type**		**Name**	
	None		None		None	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The Clear All Memory operation was performed.		---		---	
Attached information	Attached information 1:	Unit number of the NX Unit where the Clear All Memory operation was performed				
	Attached information 2:	Execution results 0: Successful 1: Hardware error 2: Initialization failed 3: Initialization not possible				
Precautions/ Remarks	Refer to the attached information for the results of the Clear All Memory operation.					

15-3-5 Other Troubles and Corrections

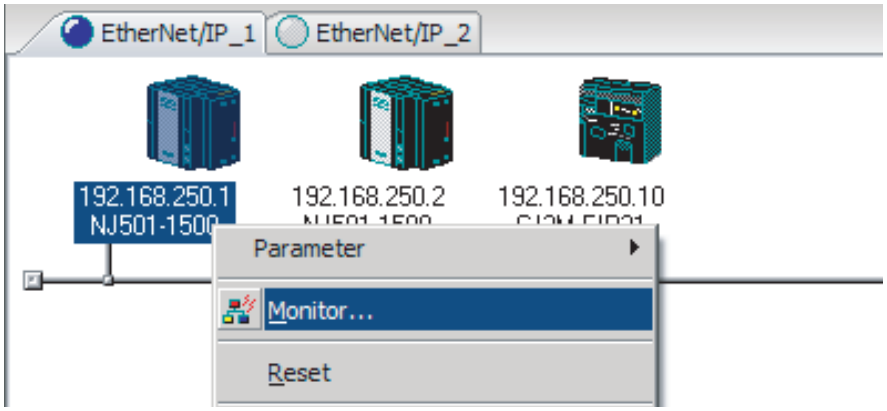
Security Errors

No.	Problem	Correction
1	Forgot the Administrator password.	You cannot access the Administrator's password. Always record the Administrator password so that you do not forget it.
2	Cannot release the operation lock with the Sysmac Studio.	Log in with verification authority that is equal to or higher than the verification rights when you connected online.
3	Operation was locked when verifying operation authority on the Sysmac Studio.	If the password for verification of operation authority is entered incorrectly five times in row, operation is locked for 10 minutes. Wait until the operation lock is released.
4	Cannot release the operation lock with the Sysmac Studio after the operator left the Sysmac Studio unattended.	You can release the operation lock with an operation authority that is equal to or higher than the operator. The required operation authority will be that of an operator (the operation authority that was verified when going online with the Sysmac Studio).
5	Writing to the Communication Control Unit is not possible for some operations. • Names Communication Control Unit name • Operation Commands Clear All Memory, and event log clearing • Synchronizing and Downloading CPU/Expansion Rack Configuration and Setup, Controller Setup, restoring	The Communication Control Unit is write protected. Release the write protection.
6	Forgot the safety password.	You cannot access the safety password. Always record the safety password so that you do not forget it.

15-4 Checking Status with the Network Configurator

15-4-1 The Network Configurator's Device Monitor Function

Connect the Network Configurator online, select the device to be checked, right-click to display the pop-up menu, and select **Monitor**.



The **Monitor Device** Dialog Box will be displayed.

Additional Information

If a communications error occurs during monitoring, the dialog box will continue to show the last information that was collected.
To start monitoring again, close the **Monitor Device** Dialog Box, and then open the **Monitor Device** Dialog Box again.

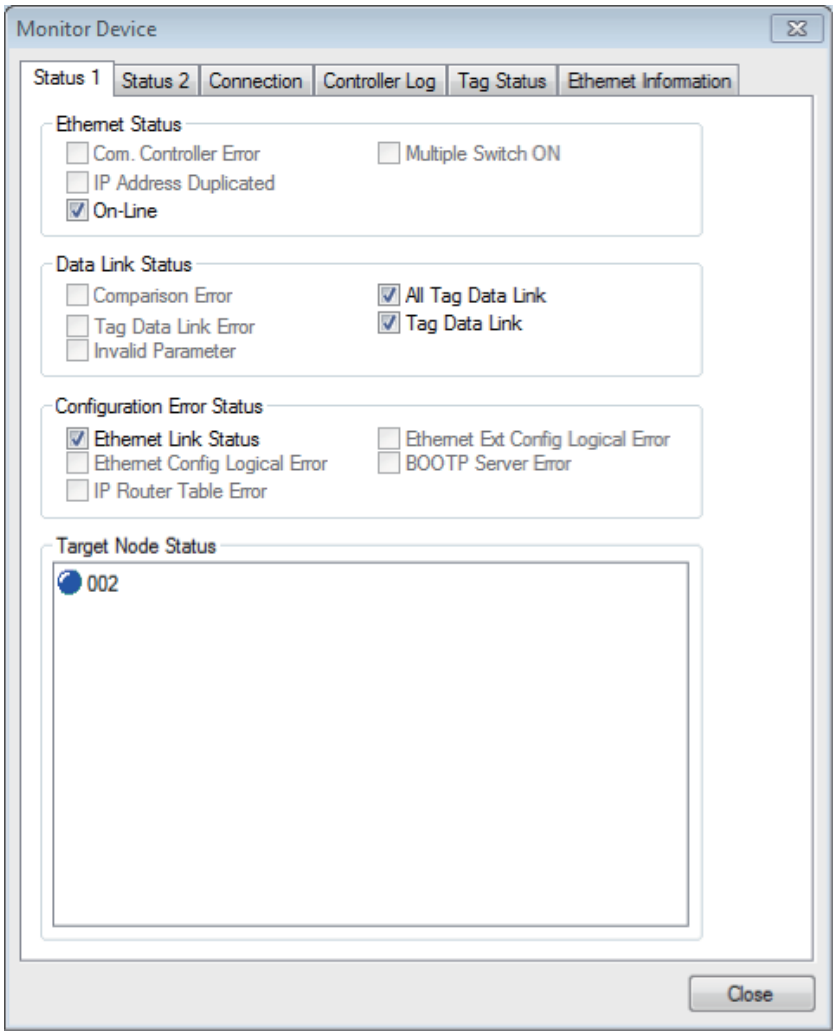
● Status 1 Tab Page

The following check boxes are displayed for the status. If a check box is checked with ☑, the status is TRUE.

Classification	Item	TRUE status description
Ethernet Status	Com. Controller Error	An error occurred in the Communications Controller.
	IP Address Duplicated	The same IP address is assigned to more than one node.
	On-Line	The Unit is online. (The EtherNet/IP Unit can perform communications processing.)
	Multiple Switch ON	More than one data link start/stop switch changed to TRUE at the same time.
Data Link Status	Comparison Error	The remote node information in the tag data link parameters was different from the actual node information. Main causes: • The specified target does not exist. • The variable name does not match. • The connection size is different. • Connection resources are not sufficient.

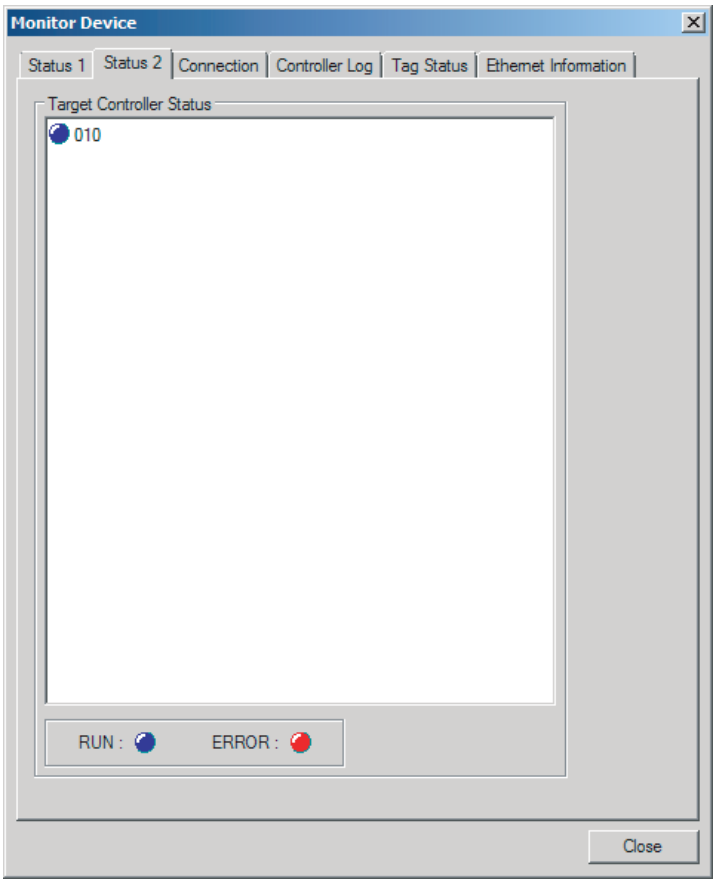
Classification	Item	TRUE status description
Data Link Status	Tag Data Link Error	There were two or more errors in a connection as an originator.
	Invalid Parameter	An error was found in the parameters for tag data links that are saved in non-volatile memory.
	All Tag Data Link	Tag data links are communicating in all connections as the originator.
	Tag Data Link	Tag data links are communicating in one or more connections as the originator.
Configuration Error Status	Ethernet Link Status	A link is established with the Ethernet switch.
	Ethernet Basic Settings Logic Error	The following settings are incorrect: • TCP/IP settings (IP address, subnet mask, or link settings)
	IP Router Table Error	There is a mistake in the IP router table information.
	Ethernet Ext Config Logical Error	Always FALSE.
	BOOTP Server Error	One of the following errors occurred when using the BOOTP server: • The IP address received from the BOOTP server is incorrect. • A communications timeout occurred with the server.

In the **Target Node Status**, information about the target node that acts as the originator is displayed.
If all tag data link connections to the node are established and normal, this information is displayed in blue. However, if any connection is broken it is displayed in red.


Monitor Device
Status 1
Status 2
Connection
Controller Log
Tag Status
Ethernet Information
Ethernet Status
Com. Controller Error
Multiple Switch ON
IP Address Duplicated
On-Line
Data Link Status
Comparison Error
All Tag Data Link
Tag Data Link Error
Tag Data Link
Invalid Parameter
Configuration Error Status
Ethernet Link Status
Ethernet Ext Config Logical Error
Ethernet Config Logical Error
BOOTP Server Error
IP Router Table Error
Target Node Status
002
Close

Status 2 Tab Page

This tab page displays information on nodes with tag data link originator settings. This information is in blue if the connection is normal, or red if an error occurred.

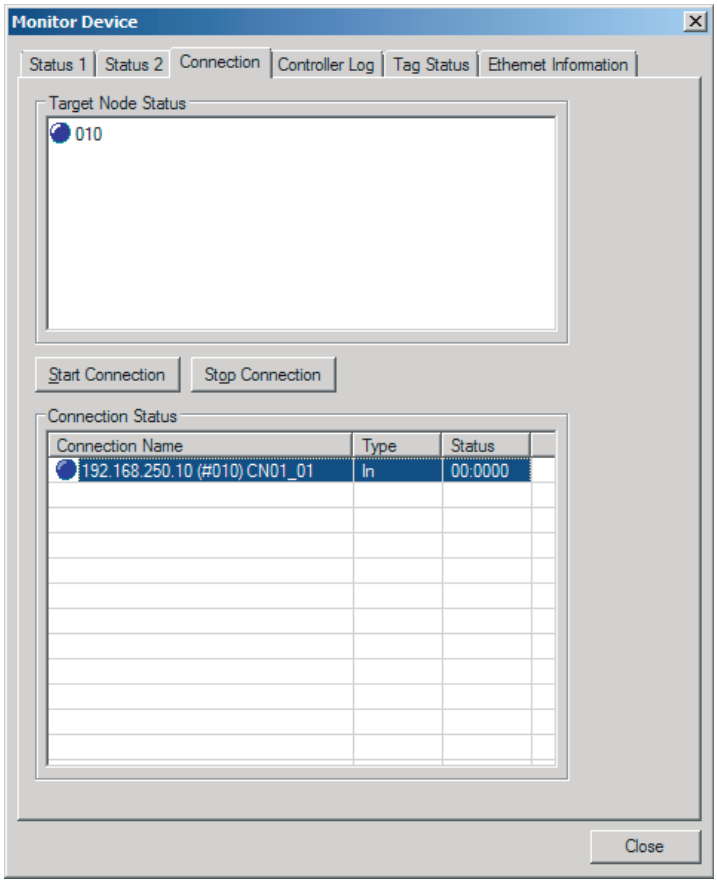


Additional Information

The target Controller status can be used when the Controller status is set to **Included** for all the target sets for both originator and target connections.
If it is set to **Not included**, it is grayed out on the display.

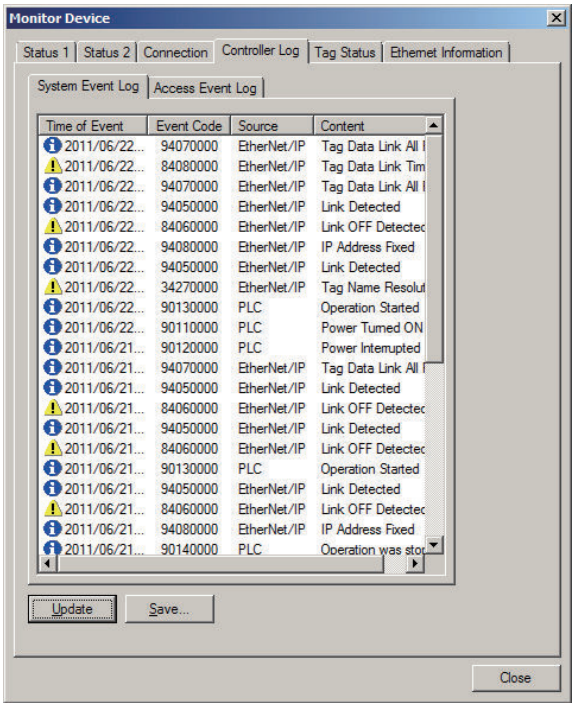
● Connection Tab Page

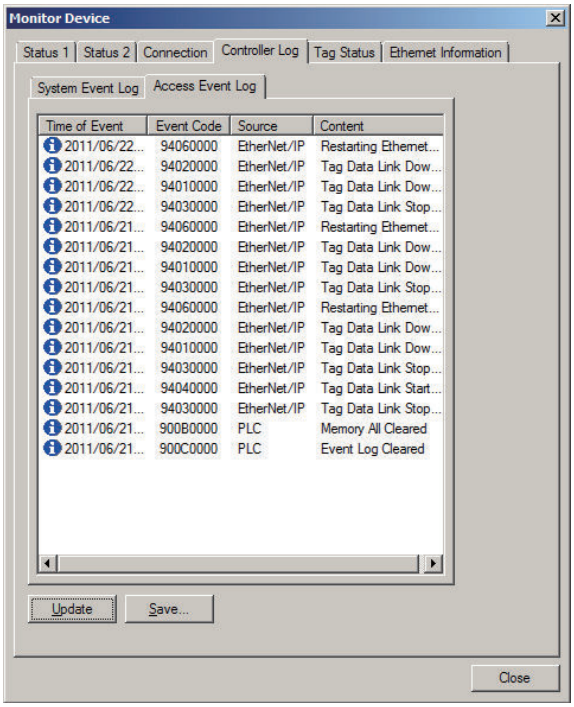
- Target Node Status
  Information about the target node that acts as the originator is displayed.
  If all tag data link connections to the node are established and normal, this information is displayed in blue. However, if any connection is broken it is displayed in red.
  However, this information is displayed in gray if the connection to the node is stopped.
- Connection Status
  The **Status** Column of the connection status shows the status of each connection that is set as the originator. The connection status can be used to identify the cause of tag data link errors.
  Refer to *15-4-2 Connection Status Codes and Troubleshooting* on page 15-249 for details on the connection status.



● Controller Log Tab Page

This tab page displays the Controller event log that is stored in the Communication Control Unit. The error history shows errors that have occurred. It can be saved in a file in the computer.



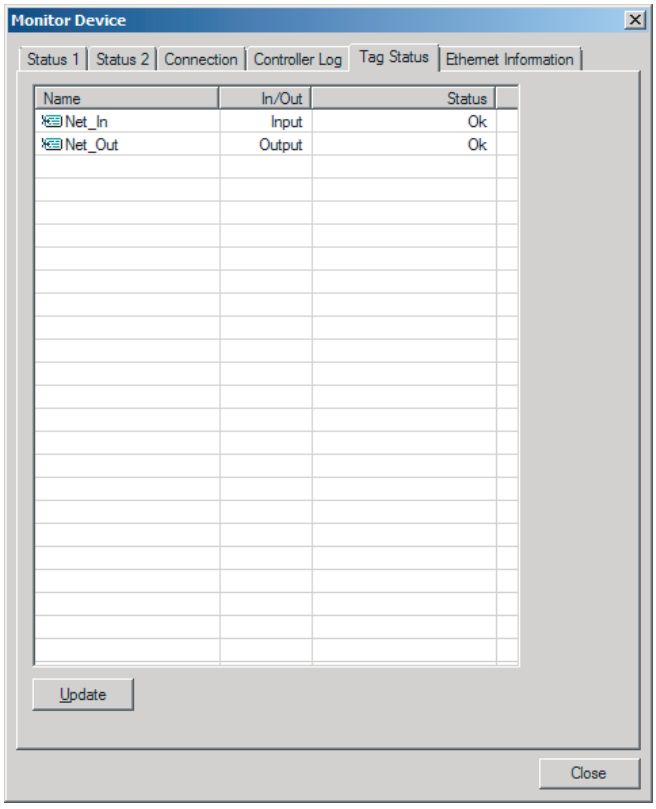


Tag Status Tab Page

This tab page displays if the tag settings for each tag for tag data links are set so that data can be exchanged with the Communication Control Unit.
The following status is displayed depending on the status that is set.

Normally resolved:	Normal data exchange is possible.
Resolving:	The variables with tags are being resolved. When the resolution is completed normally, a connection will be established and the data exchange will start.
Different sizes:	Different sizes are set for the network variables and the tag settings. A connection will not be established for a tag for which this error occurs.
No tag:	A network variable is not set in the variable table in the Communication Control Unit for the specified tag setting. Or, instead of a member of union variable, unions are specified. A connection will not be established for a tag for which this error occurs.
Attribute error:	1. Writing is not possible for Read Only and Constant attributes. 2. The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. There is an error in the setting of a Network Publish attribute for a Communication Control Unit variable. A connection will not be established for a tag for which this error occurs.

If the status is not “Normally resolved”, check the tag data link settings or the network variable settings in the variable table in the Communication Control Unit.

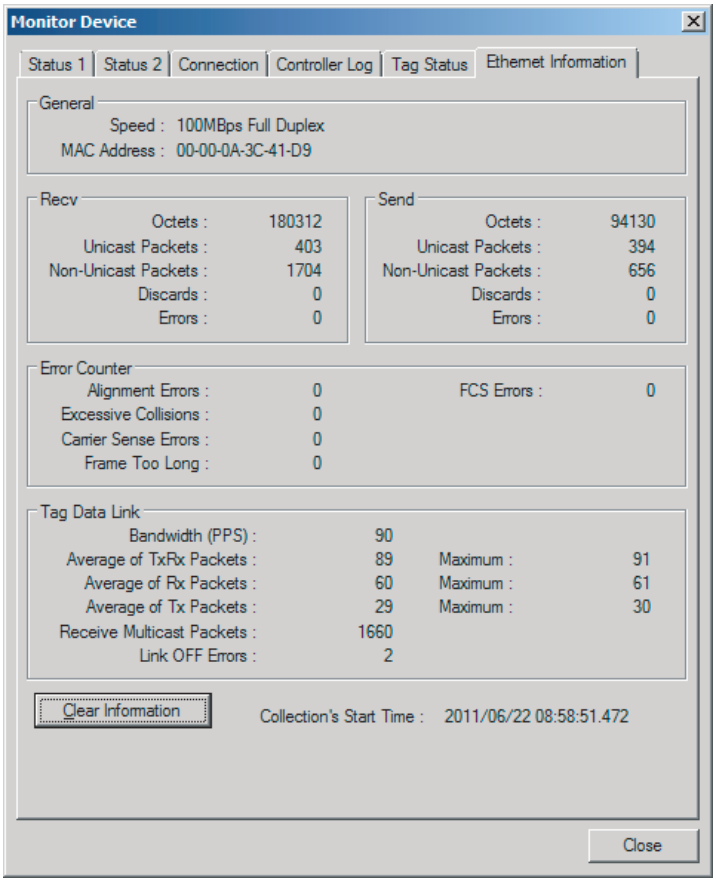


● Ethernet Information Tab Page

This tab page displays the communications status at the communications driver level of the built-in Ethernet/IP port.

The error counter information can be used to confirm whether communications problems have occurred.

The tag data link information can be used to confirm characteristics such as the Bandwidth (pps).



15-4-2 Connection Status Codes and Troubleshooting

This section explains how to identify and correct errors based on the tag data link's connection status. The connection status can be read using the **Connection** Tab Page of Monitor Device Window with the Network Configurator. Refer to *15-4-1 The Network Configurator's Device Monitor Function* on page 15-241 for details.



Additional Information

The connection status has the same meaning as the Connection Manager's General and Additional error response codes, as defined in the CIP specifications.

The following table shows the likely causes of the errors causes for each configuration and connection status (code).

	Originator	Target
Configuration 1	CS1W-EIP21, CJ1W-EIP21, CJ2H-CPU□□-EIP, CJ2M-CPU3□, NJ501-□□□□, NJ301-□□□□, NJ101-□□□□, NX701-□□□□, NX502-□□□□, NX-EIP201, NX102-□□□□, NX1P2-□□□□□□, NX-CSG□□□	CS1W-EIP21, CJ1W-EIP21, CJ2H-CPU□□-EIP, CJ2M-CPU3□, NJ501-□□□□, NJ301-□□□□, NJ101-□□□□, NX701-□□□□, NX502-□□□□, NX-EIP201, NX102-□□□□, NX1P2-□□□□□□, NX-CSG□□□
Configuration 2	CS1W-EIP21, CJ1W-EIP21, CJ2H-CPU□□-EIP, CJ2M-CPU3□, NJ501-□□□□, NJ301-□□□□, NJ101-□□□□, NX701-□□□□, NX502-□□□□, NX-EIP201, NX102-□□□□, NX1P2-□□□□□□, NX-CSG□□□	Products from other manufacturers
Configuration 3	Products from other manufacturers	CS1W-EIP21, CJ1W-EIP21, CJ2H-CPU□□-EIP, CJ2M-CPU3□, NJ501-□□□□, NJ301-□□□□, NJ101-□□□□, NX701-□□□□, NX502-□□□□, NX-EIP201, NX102-□□□□, NX1P2-□□□□□□, NX-CSG□□□

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
00	0000	Normal status code: The connection has been opened and the tag data link is communicating normally.	---	---	---
01	0100	Error code returned from target: Attempted to open multiple connections for the same connection.	This error does not occur.	Depends on the target's specifications. (This error should not occur. If it does, contact the target device's manufacturer.)	Depends on the originator's specifications. (This error should not occur. If it does, contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0103	Error code returned from target: Attempted to open a connection with an unsupported transport class.	This error does not occur.	Confirm that the target supports Class 1.	Confirm that the originator supports Class 1.
01	0106	Duplicate consumers: Attempted to open multiple connections for single-consumer data.	If the tag data link is stopped or started, this error may occur according to the timing, but the system will recover automatically.	Depends on the target's specifications. (Contact the target device's manufacturer.)	If the tag data link is stopped or started, this error may occur according to the timing, but the system will recover automatically.
01	0107	Error code returned from target: Attempted to close a connection, but that connection was already closed.	This error does not occur.	This error does not occur.	This is not an error because the connection is already closed.
01	0108	Error code returned from target: Attempted to open a connection with an unsupported connection type.	This error does not occur.	Check which connection types can be used by the target. (Contact the manufacturer.) Only multicast and point-to-point connections can be set.	Check which connection types can be used by the originator. (An error will occur if a connection other than a multicast or point-to-point connection is set.)
01	0109	Error code returned from target: The connection size settings are different in the originator and target.	Check the connection (sizes) set in the originator and target.		
01	0110	Error code returned from target: The target was unable to open the connection, because of its operating status, such as downloading settings.	Check whether the tag data link is stopped at the target. (Restart the tag data link communications with the software switch.)	Depends on the target's specifications. (Contact the target device's manufacturer.)	Check whether the tag data link is stopped at the target. (Restart the tag data link communications with the software switch.)
01	0111	Error code returned from target: The RPI was set to a value that exceeds the specifications.	This error does not occur.	Check the target's RPI setting specifications.	Set the originator's RPI setting to 10 seconds or less.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0113	Error code generated by originator or returned from target: Attempted to open more connections than allowed by the specifications.	Check the connection settings (number of connections) at the originator and target.	Check the connection settings (number of connections) at the originator and target. Check the connection specifications for devices from other manufacturers.	Check the connection settings (number of connections) at the originator and target. Check the connection specifications for devices from other manufacturers.
		The NX502 CPU Unit is set to disable CIP Safety communications.	Make sure that the NX502 CPU Unit on the CIP Safety communications path is set to enable CIP Safety communications.		
01	0114	Error code returned from target: The Vendor ID and Product Code did not match when opening connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.) Check that the target device's EDS file is correct.	Check the originator's connection settings.
01	0115	Error code returned from target: The Product Type did not match when opening connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.) Check that the target device's EDS file is correct.	Check the originator's connection settings.
01	0116	Error code returned from target: The Major/Minor Revisions did not match when opening connection.	Check the major and minor revisions set for the target device and connection. If necessary, obtain the most recent EDS file and set it again.	Depends on the target's specifications. (Contact the target device's manufacturer.) Check that the target device's EDS file is correct.	Check the originator's connection settings.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0117	Error code returned from target: The tag set specified in the connection's target variables does not exist.	Check whether the originator and target tag sets and tags are set correctly.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Check the originator's connection settings. Check whether the target tag sets and tags are set correctly.
01	011A	Error code generated by originator: Connection could not be established because the buffer was full due to high traffic.	Unexpected network traffic may have been received. Use the Ethernet Information Tab Page of the Network Configurator's device monitor to check the bandwidth usage, and correct the load. If there are places where broadcast storms occur, such as loop connections in the network connection format, then correct them.	Unexpected network traffic may have been received. Use the Ethernet Information Tab Page of the Network Configurator's device monitor to check the bandwidth usage, and correct the load. If there are places where broadcast storms occur, such as loop connections in the network connection format, then correct them.	Depends on the target's specifications. (Contact the target device's manufacturer.)
01	011B	Error code returned from target: The RPI was set to a value that is below the specifications.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Set the originator's RPI setting to 1 ms or greater.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0127	Error code returned from target: The connection data size settings are different in the originator and target. (data from originator to target)	This error does not occur.	Check the connection (sizes) set in the originator and target. (data from originator to target) Depends on the target's specifications. (Contact the manufacturer.) Check that the target device's EDS file is correct.	This error does not occur.
01	0128	The connection data size settings are different in the originator and target. (data from target to originator)	Check the connection (sizes) set in the originator and target. (data from target to originator)		
01	0203	Error code generated by originator: The connection timed out.	Tag data link communications from the target timed out. Check the power supply and cable wiring of the devices in the communications path, including the target and switches. If performance has dropped due to heavy traffic, change the performance settings. For example, increase the timeout time or RPI setting. Also, check whether the CIP message communications of the target are stopped and whether the CIP communications are permitted by Packet Filter function of the originator or the device on the route.		
01	0204	Error code generated by originator: The connection open process timed out.	There was no response from the target. Check the power supply and cable wiring of the devices in the communications path, including the target and switches. Also, check whether the CIP message communications of the target or originator are stopped and whether the CIP communications are permitted by Packet Filter function of the target device or the device on the route.		
01	0205	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0301	Error code generated by originator or returned from target: Total number of tag sets that are set to the product was exceeded.	Check the total number of the tag sets that are set to the product and set the tag sets so that the total number does not exceed the maximum of the allowable number.	Check the total number of the tag sets that are set to the product and set the tag sets so that the total number does not exceed the maximum of the allowable number.	Check the total number of the tag sets that are set to the product and set the tag sets so that the total number does not exceed the maximum of the allowable number.
01	0302	Error code generated by originator or returned from target: The tag data link's allowable bandwidth (pps) was exceeded.	Check the connection settings (number of connections and RPI) at the originator and target.	Check the target's connection settings (number of connections and RPI). Check the connection settings (number of connections and RPI) at the originator and target.	Check the connection settings (number of connections and RPI) at the originator and target.
01	0311	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0312	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0315	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0316	Error code returned from target: There was a parameter error in the frame used to close the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	031C	Error code generated by originator: Some other error occurred.	This error does not occur.	The originator generates this code when an unsupported response code is returned from the target in reply to an open request.	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
08	---	Error code returned from target: There is no Forward Open or Large Forward Open service in the target device.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
D0	0001	Error code generated by originator: The connection operation is stopped.	The connection was stopped because the Tag Data Link Stop Bit was turned ON, or the settings data is being downloaded. Either turn ON the Tag Data Link Start Switch, or wait until the settings data has been downloaded. This code includes fatal Controller errors and Unit failure. To handle these errors, refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
D0	0002	Error code generated by originator: The connection is being opened (opening processing in progress).	Wait until the opening processing is completed.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
OMRON error code					
01	0810	Error code returned from target: The latest data cannot be retrieved from the Communication Control Unit after a connection was opened. (Automatic recovery by connection open retry)	It occurs when the task period of the Communication Control Unit is too long after a connection was opened or when the Controller system stopped due to an error on the Controller. If it occurred due to a long task period, the error will be recovered automatically. If it was caused by stoppage of the Controller system, the cause of the error will be identified from the error information of the Communication Control Unit.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	The meaning of this error code is defined by each vendor, so it depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0811	Error code generated by originator: The latest data cannot be retrieved from the Communication Control Unit after a connection was opened. (Automatic recovery by connection open retry)	It occurs when the the task period of the Communication Control Unit is too long after a connection was opened. The error will be recovered automatically.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	The meaning of this error code is defined by each vendor, so it depends on the originator's specifications. (Contact the originator device's manufacturer.)

15-4-3 CIP Safety Connection Status Codes and Troubleshooting

This section explains how to identify and correct errors based on the connection status of CIP Safety connection. If the CIP Safety Originator Connection Not Established error or the CIP Safety Target

Missing error occurs with the Safety CPU Unit, the connection status of the CIP Safety connection is registered to the Attached information.



Additional Information

The connection status has the same meaning as the Connection Manager's General and Additional error response codes, as defined in the CIP specifications.

The following table shows the likely causes of the errors and the troubleshooting methods for each connection status.

Connection status		Description	Cause	Correction
General status (HEX)	Extended status (HEX)			
01	0100	Connection in use or duplicate forward open.	The connection with the CIP Safety target device is already used for connecting another originator.	Check the CIP Safety connection settings.
01	0105	Ownership Conflict or OUNID Mismatch. The configuration is already owned by another originator.	The connection with the CIP Safety target device is not available because it was used for connecting another originator.	Delete the memory of the CIP Safety target device and reconfigure the device. (The method for clearing the memory varies by the CIP Safety target devices.)
01	0106	Ownership Conflict or OUNID Mismatch. The output connection was already owned by another originator.	The connection with the CIP Safety target device is not available because it was used for connecting another originator.	Delete the memory of the CIP Safety target device and reconfigure the device. (The method for clearing the memory varies by the CIP Safety target devices.)
01	0110	Device not configured.	Attempted to open a connection for an unconfigured CIP Safety target device by selecting "Check Safety Signature (Type2a)" or "Open Only (Type2b)" for the Open Type setting.	• Use Configuration (Type1) open type for the CIP Safety target device. • Configure the CIP Safety target device accordingly. (The configuration method varies by the CIP Safety target devices.)
01	0111	RPI not supported. May also indicate problem with connection time-out multiplier, or production inhibit time.	Attempted to open a connection using an EPI that is not supported on the device.	Check the CIP Safety connection settings and the specifications of the CIP Safety target device.
01	0113	Connection Manager cannot support any more connections.	It has exceeded the maximum number of connections that can be used simultaneously. The NX502 CPU Unit is set so that CIP Safety communications cannot be used.	Check the CIP Safety connection settings and the specifications of the CIP Safety target device. Check that the NX502 CPU Unit on the path of CIP Safety communications can use for CIP Safety communications.
01	0114	Either the vendor ID or the product code in the key segment does not match the device.	Incorrect CIP Safety target device settings or IP address settings	Check the CIP Safety connection settings and the IP address settings of the CIP Safety target device.

Connection status		Description	Cause	Correction
General status (HEX)	Extended status (HEX)			
01	0116	Major or minor revision information in the key segment does not match the device.	The version of the device does not match.	Check the version of the CIP Safety target device and the CIP Safety connection settings.
01	0117	Invalid connection point.	The CIP Safety I/O assembly on the CIP Safety target device is not available.	Check the connection settings of the CIP Safety target device. (The configuration method varies by the CIP Safety target devices.) CIP Safety Target Device is a Safety CPU Unit: Check the CIP Safety I/O assembly settings on the CIP Safety target device.
01	011A	Target application cannot support any more connections.	It has exceeded the maximum number of objects that can be used simultaneously for the CIP Safety target device.	Check the CIP Safety connection settings and the specifications of the CIP Safety target device.
01	0134	Mismatched T→O Network Connection Fixvar	Attempted to open a multicast connection for the CIP Safety target device that has already opened a single-cast connection with another originator.	Check the CIP Safety connection settings.
01	0204	Unconnected_Send service timed out while waiting for a response.	The IP address settings on the CIP Safety target device are incorrect, or the Ethernet cable is disconnected. CIP Safety Target Device is a Safety CPU Unit: The node number of the Safety CPU Unit is incorrect.	Check the CIP Safety connection settings.
01	031F	No connection resources exist for the target path.	Attempted to open a single-cast connection for the CIP Safety target device that has already opened a connection with another originator.	Check the CIP Safety connection settings.
01	0801	Incompatible Multi-cast RPI. An existing connection has been established at a different RPI.	Attempted to open a multicast connection with different EPI for the CIP Safety target device that has already opened a multi-cast connection with another originator.	Check the CIP Safety connection settings.
01	0802	Invalid Safety Connection Size	The connection of the selected size is not available for the CIP Safety target device.	Check the CIP Safety connection settings and the CIP Safety target device settings.
01	0805	Invalid Ping Interval EPI Multiplier	Attempted to open a multicast connection with different timeout settings for the CIP Safety target device that has already opened a multi-cast connection with another originator.	Check the CIP Safety connection settings.

Connection status		Description	Cause	Correction
General status (HEX)	Extended status (HEX)			
01	0809	Invalid Max Consumer Number	It has exceeded the maximum number of originators that can be simultaneously connected in the multicast connection with the CIP Safety target device.	Check the CIP Safety connection settings and the specifications of the CIP Safety target device.
01	080C	SCID Mismatch. The SCID was non-zero and did not match the value in the target	Attempted to open a connection for an already configured CIP Safety target device by selecting "Check Safety Signature (Type2a)" for the Open Type setting, but the safety signature did not match.	Check the CIP Safety connection settings and the CIP Safety target device settings.
01	080D	TUNID not set. Device is out-of-box and TUNID has not been set, so connections are not allowed.	TUNID for the CIP Safety target device is not configured.	Configure TUNID of the CIP Safety target device. (The configuration method varies by the CIP Safety target devices.)
01	080E	TUNID Mismatch. The TUNID provided does not match. The message was likely routed to this node in error	TUNID for the CIP Safety target device is configured to another value.	Reconfigure TUNID for the CIP Safety target device. (The configuration method varies by the CIP Safety target devices.)
02	---	Resources needed for the object to perform the requested service were unavailable.	There was no open resource in the CIP Safety target device.	Check the CIP Safety target device settings.

16

Inspection and Maintenance

This section describes the procedures for cleaning, inspecting, and replacing Safety Network Controller.

16-1 Cleaning and Inspection 16-2
16-1-1 Cleaning 16-2
16-1-2 Periodic Inspections 16-2
16-2 Maintenance Procedures 16-5
16-2-1 Replacing the Communication Control Unit and the Safety CPU Unit 16-5
16-2-2 Replacing Safety I/O Units 16-6

16-1 Cleaning and Inspection

This section describes daily maintenance and the cleaning and inspection methods.

16-1-1 Cleaning

Clean the Communication Control Units and Safety Control Units regularly as described below in order to keep them in optimal operating condition.

- Wipe the equipment over with a soft, dry cloth when performing daily cleaning.
- If dirt remains even after wiping with a soft, dry cloth, wipe with a cloth that has been wet with a sufficiently diluted detergent (2%) and wrung dry.
- A smudge may remain on the Unit from gum, vinyl, or tape that was left on for a long time. Remove the smudge when cleaning.

Precautions for Correct Use

- Never use volatile solvents, such as paint thinner, benzene, or chemical wipes.
- Do not touch the NX bus connector.

16-1-2 Periodic Inspections

Although the major components in Communication Control Units and Safety Control Units have an extremely long life time, they can deteriorate under improper environmental conditions. Periodic inspections are thus required.

Inspection is recommended at least once every six months to a year, but more frequent inspections will be necessary in adverse environments.

Take immediate steps to correct the situation if any of the conditions in the following table are not met.

- Make sure that the Units are used within the ranges of specifications.
- Make sure that the Units are mounted and wired correctly.
- To maintain the operating reliability of the safety functions at a consistent level, diagnose the safety functions.
- Use the error log to check whether non-fatal errors have occurred.

Periodic Inspection Items

No.	Inspection item	Inspection details	Criteria	Correction
1	External power supply	Is the power supply voltage measured at the terminal block within standards?	Within the power supply voltage range	Use a voltage tester to check the power supply at the terminals. Take necessary steps to bring the power supply within the power supply voltage range.
2	I/O power supply	Is the power supply voltage measured at the I/O terminal block within standards?	Voltages must be within I/O specifications of each NX Unit.	Use a voltage tester to check the power voltage at the terminals. Take necessary steps to bring the I/O power supply within NX Unit standards.

No.	Inspection item	Inspection details	Criteria	Correction
3	Ambient environment	Is the ambient operating temperature within standards?	0 to 55°C	Use a thermometer to check the temperature and ensure that the ambient operating temperature remains within the allowed range of 0 to 55°C.
		Is the ambient operating humidity within standards?	Relative humidity must be 10% to 95% with no condensation.	Use a hygrometer to check the humidity and ensure that the ambient operating humidity remains between 10% and 95%. Make sure that condensation does not occur due to rapid changes in temperature.
		Is it subject to direct sunlight?	Not in direct sunlight	Protect the Controller if necessary.
		Is there an accumulation of dirt, dust, salt, metal powder, etc.?	No accumulation	Clean and protect the Controller if necessary.
		Is there water, oil, or chemical sprays hitting the Controller?	No spray	Clean and protect the Controller if necessary.
		Are there corrosive or flammable gases in the area of the Controller?	No gases	Check by smell or use a sensor.
		Is the Unit subject to shock or vibration?	Vibration resistance and shock resistance must be within specifications.	Install cushioning or other vibration and shock absorbing equipment if necessary.
		Are there noise sources near the Controller?	No significant noise sources	Either separate the Controller and noise source or protect the Controller.
4	Installation and wiring	Are the DIN Track mounting hooks for each NX Unit securely locked?	No looseness	Securely lock the DIN Track mounting hooks.
		Are the cable connectors fully inserted and locked?	No looseness	Correct any improperly installed connectors.
		Are there any loose screws on the End Plates (PFP-M)?	No looseness	Tighten loose screws with a Phillips-head screwdriver.
		Are the NX Units connected to each other along the hookup guides and until they touch the DIN track?	You must connect and fix the NX Units to the DIN track.	Connect the NX Units to each other along the hookup guides and insert them until they touch the DIN track.
		Are there any damaged external wiring cables?	No visible damage	Check visually and replace cables if necessary.
5	Safety validation testing (user testing)	Check to be sure that all safety functions operate correctly.	All functions must operate as intended.	Remove the cause of errors and check the operation of all safety functions again.

Tools Required for Inspections

Required Tools

- Phillips screwdriver
- Flat-blade screwdriver
- Voltage tester or digital voltmeter
- Industrial alcohol and pure cotton cloth

Tools Required Occasionally

- Oscilloscope
- Thermometer and hygrometer

16-2 Maintenance Procedures

If the inspection reveals any problems that require you to replace a Communication Control Unit or a Safety Control Unit, observe the following precautions.

- Never disassemble, repair, or modify a Unit. This will compromise the integrity of the safety function and is dangerous.
- Make sure that you can replace the Unit under safe conditions.
- Perform all replacements with the power supply turned OFF to prevent electric shock, or unexpected movement of the machinery.
- Check the new Unit to make sure that there are no errors.
- For poor contact, take a clean cotton cloth, soak the cloth in industrial alcohol, and carefully wipe the contacts clean. Be sure to remove any lint prior to remounting the Unit.

Precautions for Safe Use

After you replace the Unit, reset the program and all configuration settings that are necessary to resume operation. Make sure that the safety functions operate normally before you start actual operation.

Remove the faulty Unit, and then replace and wire the new Unit.
Refer to *Section 3 Specifications of Configuration Units* on page 3-1and to *Section 5 Installation and Wiring* on page 5-1 for information on installing, removing, and wiring Units.

The following sections give the procedures to replace the Communication Control Unit, Safety CPU Unit, and Safety I/O Units.

16-2-1 Replacing the Communication Control Unit and the Safety CPU Unit

Precautions before Replacing the Unit

- Before replacing the Unit, make sure there is a Sysmac Studio project file that corresponds to the current safety control system. Alternatively, you can upload the project file from the actual safety control system.
- Make sure that the Sysmac Studio project file is the intended file before replacing the Unit.
- Replacement work must be performed only by personnel with knowledge of safety controls.
- To ensure the safety of all workers, turn OFF the power supply to all hazard sources (i.e., actuators, etc.).

Replacement Procedure

Remove a Communication Control Unit or a Safety CPU Unit to replace, and attach a new Unit.

● When Using the Sysmac Studio

Sysmac Studio can be used only when the safety application contained in the project file is validated.

If the safety application is not validated yet, refer to *Section 9 Checking Operation and Actual Operation* on page 9-1.

1 Connect the Sysmac Studio online with the Communication Control Unit.
The NX Unit Initialization Error occurs in the Communication Control Unit because of the data mismatch between the Safety CPU Unit and the Communication Control Unit.

2 Select **Synchronization** from the **Controller** Menu. Click the **Transfer to Controller** Button in the Synchronization Window to transfer the CPU Rack configuration information and the validated safety application data to the Communication Control Unit and the Safety CPU Unit from the computer.
Refer to *9-2 Transferring the Configuration Information* on page 9-6 and *9-14 Transferring Safety Application Data* on page 9-68 for detailed procedures. The operating mode of the Safety CPU Unit changes to RUN mode after the data is transferred.

● When Using an SD Memory Card

Refer to *Section 12 Safety Unit Restore* on page 12-1 and *Section 13 Backup Functions of the Communication Control Unit* on page 13-1 for details when you use an SD Memory Card.

Checking after Replacing a Unit

- After a Unit is replaced, make sure that the intended data was transferred to the Communication Control Unit and the Safety CPU Unit by using the following methods.
  a) When you use the Sysmac Studio, make sure that the safety signature that is shown in the Properties Dialog Box for the safety project is the same as the safety signature that is shown in the Controller Status Pane.
  b) When you use an SD Memory Card, make sure that the safety signature that is shown in the seven-segment indicator of the Safety CPU Unit is the intended signature.
- After the replacement is completed, always perform user testing to make sure that the safety functions operate correctly.
- If necessary, clear the event log of any events that remain in the Communication Control Unit and the Safety CPU Unit due to the replacement work.

16-2-2 Replacing Safety I/O Units

This section describes the ACR (auto configuration restart) function.

● Precautions before Replacing the Units

- The replaced Safety I/O Units must be in the default status before the replacement.
  If you are unsure of whether the Safety I/O Units are in the default state, perform the Clear All Memory operation for all Safety I/O Units that were replaced. Refer to *9-16 Restarting and Clearing All Memory* on page 9-72 for detailed procedures.
- Replacement work must be performed only by personnel with knowledge of safety controls.

- To ensure the safety of all workers, turn OFF the power supply to all hazard sources (i.e., actuators, etc.).

● Replacement Procedure

1. Record the relationship between the wiring and the terminal numbers before you remove the terminal block from the Safety I/O Units.
2. Remove the Safety I/O Units to replace.
3. Mount the new Safety I/O Units.
4. Return the terminal block to the new Safety I/O Units.
5. Cycle the power supply to the Safety CPU Unit.

● Checking after Replacing Safety I/O Units

- After the replacement is completed, always perform user testing to make sure that the safety functions operate correctly. Make sure that the terminal block is inserted into the correct location on the Safety I/O Units, and check by performing user testing.

Precautions for Correct Use

Checking the Serial Numbers of NX Units

- If the **Serial Number Check Method** setting on the Communication Control Unit is set to **Setting = Actual** device, temporarily change this setting to **No** check, and then replace the NX Unit. Get the serial number of the new NX Unit, and then set the **Serial Number Check Method** setting on the Communication Control Unit to **Setting = Actual** device again. If you replace the NX Unit with the **Serial Number Check Method** setting set to **Setting = Actual** device, an *NX Unit Serial Number Mismatch* will occur.

A

Appendices

The appendices provide the general specifications, dimensions of the Units, application examples, and other information.

A-1 General Specifications A-3

A-2 Dimensions A-4
A-2-1 Communication Control Unit A-4
A-2-2 Safety CPU Unit A-5
A-2-3 Safety I/O Units A-5
A-2-4 End Cover A-6
A-2-5 SD Memory Card A-6

A-3 NX Objects A-7
A-3-1 Format of NX Object Descriptions A-7
A-3-2 Safety CPU Unit A-7
A-3-3 NX-SID800 Safety Input Unit A-11
A-3-4 NX-SIH400 Safety Input Unit A-16
A-3-5 NX-SOD400 Safety Output Unit A-21
A-3-6 NX-SOH200 Safety Output Unit A-25

A-4 Application Examples A-30
A-4-1 Emergency Stop Pushbutton Switches A-30
A-4-2 Safety Doors A-32
A-4-3 Safety Laser Scanners A-36
A-4-4 Safety Door Switches with Magnetic Locks and Key Selector Switches A-39
A-4-5 Enable Switches A-43
A-4-6 Two-hand Switches A-47
A-4-7 D40A Non-contact Door Switches A-50
A-4-8 D40A-2/D40Z Non-contact Door Switches A-53
A-4-9 Safety Mats and Safety Light Curtains A-56
A-4-10 Safety Edges A-61
A-4-11 Single Beam Safety Sensor A-63

A-5 Change Tracking A-67

A-6 Safety CPU Unit Status A-69

A-7 I/O Ports of Safety I/O Units A-71
A-7-1 NX-SIH400 Safety Input Unit A-71
A-7-2 NX-SID800 Safety Input Unit A-73
A-7-3 NX-SOH200 Safety Output Unit A-74
A-7-4 NX-SOD400 Safety Output Unit A-75

A-8 CIP Response Codes A-78
A-8-1 General Status Codes A-78

A-8-2 Extended Status Codes A-80

A-9 Icon list for Safety Slave Unit Parameters A-83
A-9-1 External Device Icons for Input Devices A-83
A-9-2 Contact Icons for Input Devices A-87
A-9-3 External Device Icons for Output Devices A-89
A-9-4 Contact Icons for Output Devices A-90

A-10 Printing A-91
A-10-1 Selecting the Items to Print A-91
A-10-2 Items that are Printed A-91

A-11 List of Screwless Clamping Terminal Block Models A-93
A-11-1 Model Notation A-93
A-11-2 List of Terminal Block Models A-93

A-12 I/O Refreshing between NX Units A-95
A-12-1 I/O Refreshing from the Communication Control Unit to NX Units A-95
A-12-2 Methods of I/O Refreshing between the Communication Control Unit and NX Units A-95
A-12-3 I/O Response Time for Communications between NX Units A-101

A-13 Units That Support Communications between NX Units A-103

A-14 Checking the Signature Code on the Seven-segment Indicator A-104

A-15 Execution Scenarios for the Simple Automatic Test A-105

A-16 Differences in Checking Operation between the Simulator and Safety CPU Unit A-108

A-17 I/O Data Enable Flag for CIP Safety Connections A-109

A-18 Safety: Update Configurations and Setup Transfer Data A-111

A-19 CIP Safety Target Device Operation A-112

A-20 Version Information A-115
A-20-1 Relationship between the Unit Versions and Sysmac Studio Versions A-115

A-1 General Specifications

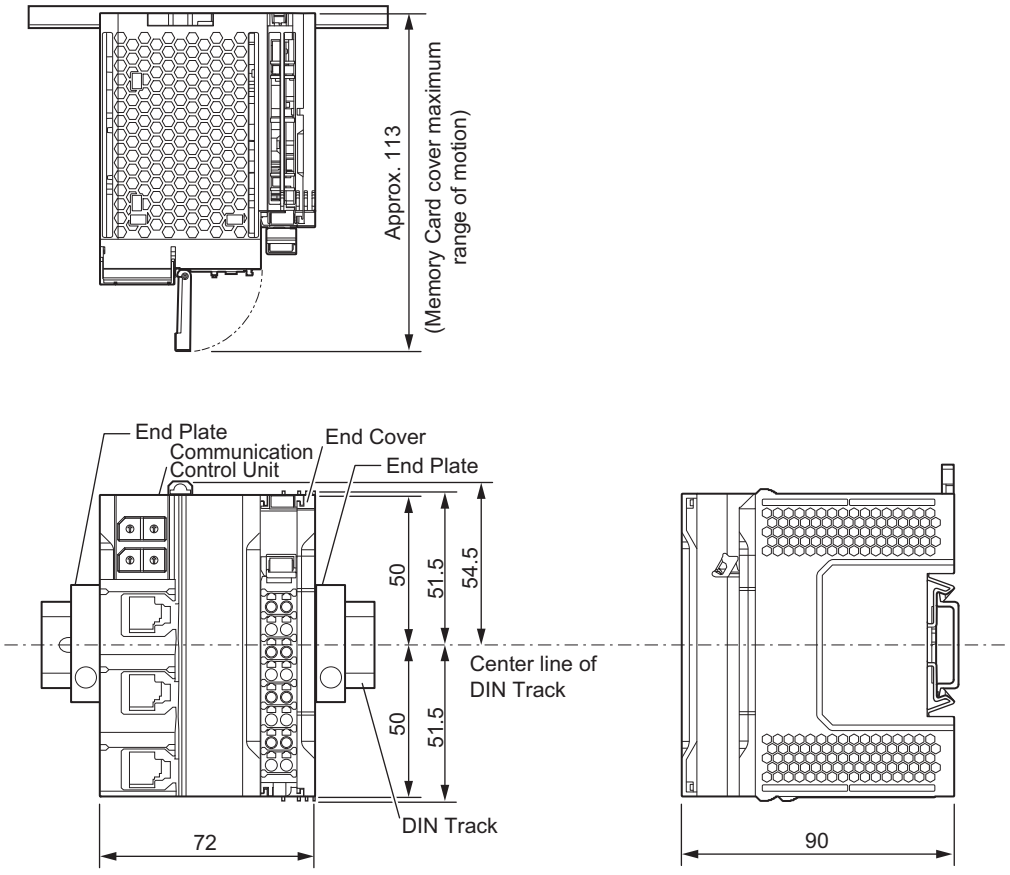
Refer to *General Specifications* on page 3-3 for the general specifications of Communication Control Unit.
Refer to *General Specifications* on page 3-22 for the general specifications of Safety CPU Unit.
Refer to *General Specifications* on page 3-32 for the general specifications of Safety Input Unit.
Refer to *General Specifications* on page 3-45 for the general specifications of Safety Output Unit.

A-2 Dimensions

Dimensions of the Units are shown as follows. The unit of dimension is millimeter.

A-2-1 Communication Control Unit

NX-CSG320

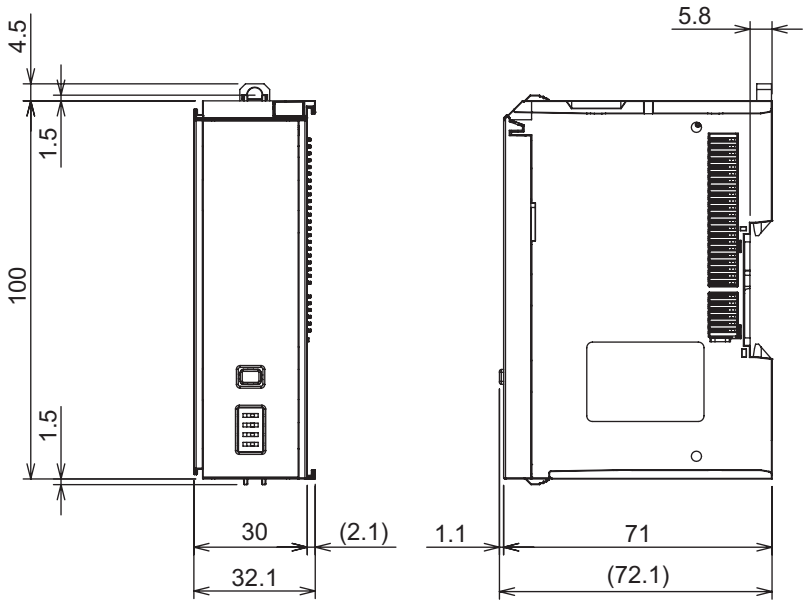


Unit: mm

For dimensions with the communications cable connected, refer to *5-2-11 Assembled Appearance and Dimensions* on page 5-28.

A-2-2 Safety CPU Unit

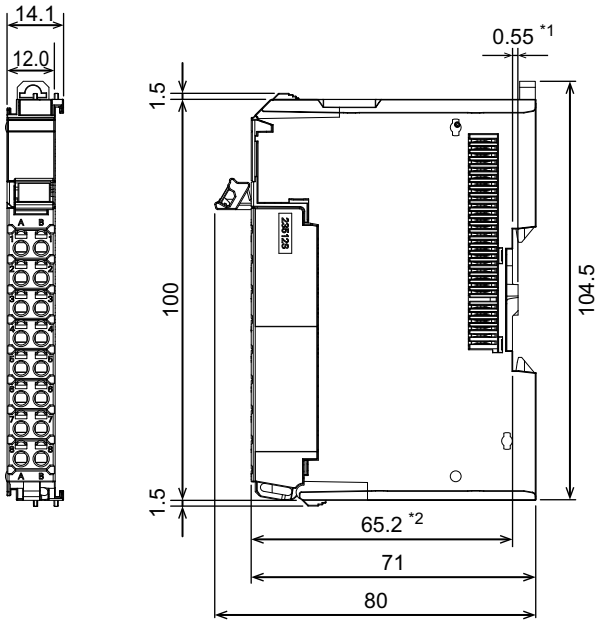
NX-SL5500/NX-SL5700



Unit: mm

A-2-3 Safety I/O Units

NX-SID800/NX-SIH400/NX-SOD400/NX-SOH200

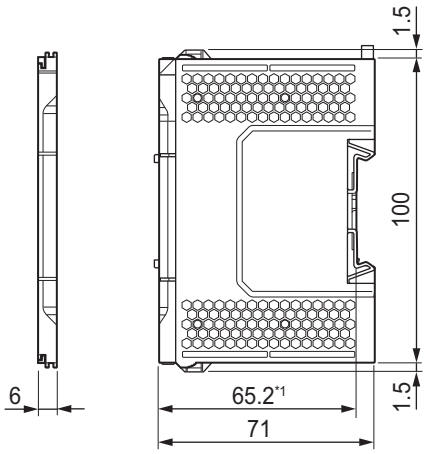


Unit: mm

*1. The dimension is 1.35 mm for Units with lot numbers through December 2014.
*2. The dimension from the attachment surface of the DIN Track to the front surface of the Safety I/O Unit.

A-2-4 End Cover

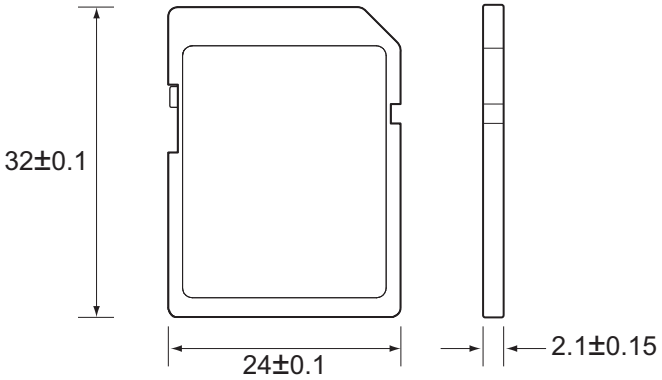
NX-END02



Unit: [mm]

*1. The dimension from the attachment surface of the DIN Track to the front surface of the end cover.

A-2-5 SD Memory Card



Unit: [mm]

A-3 NX Objects

A-3-1 Format of NX Object Descriptions

In this manual, NX objects are described with the following format.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute

Index (hex) : This is the index of the NX object that is expressed as a four-digit hexadecimal number.
Subindex (hex) : This is the subindex of the NX object that is expressed as a two-digit hexadecimal number.
Object name : This is the name of the object. For a subindex, this is the name of the subindex.
Default value : This is the value that is set by default.
Data range : For a read-only (RO) NX object, this is the range of the data you can read. For a read-write (RW) NX object, this is the setting range of the data.
Unit : The unit is the physical units.
Data Type : This is the data type of the object.
Access : This data tells if the object is read-only or read/write.
RO: Read-only
RW: Read/write
I/O allocation : This tells whether I/O allocation is allowed.
Data attribute : This is the timing when changes to writable NX objects are enabled.
Y: Enabled by restarting
N: Enabled at all times
---: Write-prohibited

A-3-2 Safety CPU Unit

Unit Information Object

This object gives the product information.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
1000	---	NX Bus Identity	---	---	---	---	---	---	---
	00	Number of Entries	7	7	---	USINT	RO	Not supported	---
	02	Model	*1	---	---	ARRAY [0..11] OF BYTE	RO	Not supported	---
	03	Device Type	00000A00 hex	---	---	UDINT	RO	Not supported	---
	04	Product Code	*2	---	---	UDINT	RO	Not supported	---
	05	Vendor Code	1	---	---	UDINT	RO	Not supported	---
	06	Unit Version	*3	---	---	UDINT	RO	Not supported	---
	07	Serial Number	*4	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
1001	---	Production Info	---	---	---	---	---	---	---
	00	Number of Entries	4	4	---	USINT	RO	Not supported	---
	01	Lot Number	*5	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
	02	Hardware Version	*6	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---
	03	Software Version	*7	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---

*1. The product models are assigned in ascending order from the lowest number of array elements. Unused elements are padded with spaces.

*2. The product codes are assigned for each product model.

NX-SL5700: 00A05700 hex

*3. Bits 24 to 31: Integer part of the Unit version
Bits 16 to 23: Fractional part of the Unit version
Bits 0 to 15: Reserved
(Example) For Ver.1.0, 0100□□□□ hex

*4. The unique serial number of the product is given.
Bits 0 to 31: Serial number

*5. The date of manufacture is given for the "lot number".
Bits 24 to 31: Day of manufacture
Bits 16 to 23: Month of manufacture
Bits 8 to 15: Year of manufacture
Bits 0 to 7: Reserved

*6. The hardware version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

*7. The software version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

Objects That Accept I/O Allocations

These objects accept I/O allocations.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6004	---	Status	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety CPU Status	0000 hex	0000 to 007F hex*1	---	WORD	RO	Supported	---

*1. The details of the Safety CPU Status are as follows:
Bit 0: Normal Operating, All safety master connections established
Bit 1: Program Operating
Bit 2: Program No Fault
Bit 3: Safety Master Connection Status
Bit 4: FSoE Master Connection Status
Bit 5: CIP Safety Originator Connection Status
Bit 6: CIP Safety Target Connection Status
Bits 7 to 15: Reserved

Other Objects

This section lists other objects.

● Safety Signature Objects

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5002	---	Safety Signature	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Last Modified*1	0x0000000000000000	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	---	ULINT	RO	Not supported	---
	02	Signature*2	0x0000	0xFFFF	---	UINT	RO	Not supported	---

*1. The default value is given if it is not validated. If safety validation is executed, the elapsed number of seconds from 00:00:00 on January 1, 1970 (UTC) is entered as the update time of the safety signature.

*2. The default value is given if it is not validated.

● Node Name Objects

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5003	---	Node name	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Node name*1	0	---	---	ARRAY [0..79] OF BYTE	RO	Not supported	---

*1. If the node name is not set, the default value is given.
If the node name is specified, the node name in the ASCII code will be entered.

● Status Objects

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5001	---	Status	---	---	---	---	---	---	---
	00	Number of Entries	8	8	---	USINT	RO	Not supported	---
	01	Safety CPU Status	0000 hex	0000 to 007F hex	---	WORD	RO	Not supported	---
	02	Normal Operating	0	0-1	---	BOOL	RO	Not supported	---
	03	Program Operating	0	0-1	---	BOOL	RO	Not supported	---
	04	Program No Fault	0	0-1	---	BOOL	RO	Not supported	---
	05	Safety Master Connection Status	0	0-1	---	BOOL	RO	Not supported	---
	06	FSoE Master Connection Status	0	0-1	---	BOOL	RO	Not supported	---
	07	CIP Safety Originator Connection Status	0	0-1	---	BOOL	RO	Not supported	---
	08	CIP Safety Target Connection Status	0	0-1	---	BOOL	RO	Not supported	---

A-3-3 NX-SID800 Safety Input Unit

Unit Information Objects

These objects give the product information.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
1000	---	NX Bus Identity	---	---	---	---	---	---	---
	00	Number of Entries	7	7	---	USINT	RO	Not supported	---
	02	Model	NX-SID800	---	---	ARRAY [0..11] OF BYTE	RO	Not supported	---
	03	Device Type	00000A01 hex	---	---	UDINT	RO	Not supported	---
	04	Product Code	00A10800 hex	---	---	UDINT	RO	Not supported	---
	05	Vendor Code	1	---	---	UDINT	RO	Not supported	---
	06	Unit Version	*1	---	---	UDINT	RO	Not supported	---
	07	Serial Number	*2	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
1001	---	Production Info	---	---	---	---	---	---	---
	00	Number of Entries	4	4	---	USINT	RO	Not supported	---
	01	Lot Number	*3	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
	02	Hardware Version	*4	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---
	03	Software Version	*5	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---

*1. Bits 24 to 31: Integer part of the Unit version
Bits 16 to 23: Fractional part of the Unit version
Bits 0 to 15: Reserved

(Example) For Ver.1.0, 0100□□□□ hex

*2. The unique serial number of the product is given.
Bits 0 to 31: Serial number

*3. The date of manufacture is given for the "lot number".
Bits 24 to 31: Day of manufacture
Bits 16 to 23: Month of manufacture
Bits 8 to 15: Year of manufacture
Bits 0 to 7: Reserved

*4. The hardware version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

*5. The software version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

Objects That Accept I/O Allocations

These objects accept I/O allocations.
They cannot be accessed through message communications.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6000	---	FSoE Slave Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Slave CMD	00 hex	00 to FF hex	---	BYTE	RO	Supported	---
	02	FSoE Slave Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---
	03	FSoE Slave CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6001	---	Safety Input Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Input 1st Byte	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6002	---	Standard Input Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Input 1st Word	0000 hex	0000 to FFFF hex*1	---	WORD	RO	Supported	---
	02	Standard Input 2nd Byte	00 hex	00 to FF hex*2	---	BYTE	RO	Supported	---

*1. The details of the "Standard Input 1st Word" are as follows:
Bit 0: Si00 Logical Value
Bit 1: Si01 Logical Value
Bit 2: Si02 Logical Value
Bit 3: Si03 Logical Value
Bit 4: Si04 Logical Value
Bit 5: Si05 Logical Value
Bit 6: Si06 Logical Value
Bit 7: Si07 Logical Value
Bit 8: Safety Connection Status
Bit 9: Safety Input Terminal Status
Bit 10: Unit Normal Status
Bit 11: IO Power Supply Error Flag
Bits 12 to 15: Reserved

*2. The details of the "Standard Input 2nd Byte" are as follows:
Bit 0: Si00 Status
Bit 1: Si01 Status
Bit 2: Si02 Status
Bit 3: Si03 Status
Bit 4: Si04 Status
Bit 5: Si05 Status
Bit 6: Si06 Status
Bit 7: Si07 Status

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7000	---	FSoE Master Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Master CMD	00 hex	00 to FF hex	---	BYTE	RW	Supported	---
	02	FSoE Master Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---
	03	FSoE Master CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7001	---	Safety Output Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Output 1st Word	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7002	---	Standard Output Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Output 1st Word	0000 hex	0000 hex*1	---	WORD	RW	Supported	---
	02	Standard Output 2nd Byte	00 hex	00 hex*2	---	BYTE	RW	Supported	---

*1. "Standard Output 1st Word" is reserved by the system.

*2. "Standard Output 2nd Byte" is reserved by the system.

Other Objects

This section lists other objects.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5000	---	Device Safety Address	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Address	0000 hex	0000 to FFFF hex	---	UINT	RO	Not supported	---

A-3-4 NX-SIH400 Safety Input Unit

Unit Information Objects

This object gives the product information.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
1000	---	NX Bus Identity	---	---	---	---	---	---	---
	00	Number of Entries	7	7	---	USINT	RO	Not supported	---
	02	Model	NX-SIH400	---	---	ARRAY [0..11] OF BYTE	RO	Not supported	---
	03	Device Type	00000A02 hex	---	---	UDINT	RO	Not supported	---
	04	Product Code	00A20400 hex	---	---	UDINT	RO	Not supported	---
	05	Vendor Code	1	---	---	UDINT	RO	Not supported	---
	06	Unit Version	*1	---	---	UDINT	RO	Not supported	---
	07	Serial Number	*2	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
1001	---	Production Info	---	---	---	---	---	---	---
	00	Number of Entries	4	4	---	USINT	RO	Not supported	---
	01	Lot Number	*3	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
	02	Hardware Version	*4	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---
	03	Software Version	*5	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---

*1. Bits 24 to 31: Integer part of the Unit version
Bits 16 to 23: Fractional part of the Unit version
Bits 0 to 15: Reserved

(Example) For Ver.1.0, 0100□□□□ hex

*2. The unique serial number of the product is given.
Bits 0 to 31: Serial number

*3. The date of manufacture is given for the "lot number".
Bits 24 to 31: Day of manufacture
Bits 16 to 23: Month of manufacture
Bits 8 to 15: Year of manufacture
Bits 0 to 7: Reserved

*4. The hardware version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

*5. The software version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

Objects That Accept I/O Allocations

These objects accept I/O allocations.
They cannot be accessed through message communications.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6000	---	FSoE Slave Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Slave CMD	00 hex	00 to FF hex	---	BYTE	RO	Supported	---
	02	FSoE Slave Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---
	03	FSoE Slave CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6001	---	Safety Input Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Input 1st Byte	00 hex	00 to FF hex	---	BYTE	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6002	---	Standard Input Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Input 1st Byte	00 hex	00 to FF hex*1	---	BYTE	RO	Supported	---
	02	Standard Input 2nd Byte	00 hex	00 to FF hex*2	---	BYTE	RO	Supported	---

*1. The details of the "Standard Input 1st Byte" are as follows:
Bit 0: Si00 Logical Value
Bit 1: Si01 Logical Value
Bit 2: Si02 Logical Value
Bit 3: Si03 Logical Value
Bit 4: Safety Connection Status
Bit 5: Safety Input Terminal Status
Bit 6: Unit Normal Status
Bit 7: IO Power Supply Error Flag

*2. The details of the "Standard Input 2nd Byte" are as follows:
Bit 0: Si00 Status
Bit 1: Si01 Status
Bit 2: Si02 Status
Bit 3: Si03 Status
Bits 4 to 7: Reserved

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7000	---	FSoE Master Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Master CMD	00 hex	00 to FF hex	---	BYTE	RW	Supported	---
	02	FSoE Master Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---
	03	FSoE Master CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7001	---	Safety Output Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Output 1st Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7002	---	Standard Output Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Output 1st Byte	00 hex	00 hex *1	---	BYTE	RW	Supported	---
	02	Standard Output 2nd Byte	00 hex	00 hex *2	---	BYTE	RW	Supported	---

*1. "Standard Output 1st Byte" is reserved by the system.
*2. "Standard Output 2nd Byte" is reserved by the system.

Other Objects

This section lists other objects.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5000	---	Device Safety Address	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Address	0000 hex	0000 to FFFF hex	---	UINT	RO	Not supported	---

A-3-5 NX-SOD400 Safety Output Unit

Unit Information Objects

These objects give the product information.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
1000	---	NX Bus Identity	---	---	---	---	---	---	---
	00	Number of Entries	7	7	---	USINT	RO	Not supported	---
	02	Model	NX-SOD400	---	---	ARRAY [0..11] OF BYTE	RO	Not supported	---
	03	Device Type	00000A03 hex	---	---	UDINT	RO	Not supported	---
	04	Product Code	00A30400 hex	---	---	UDINT	RO	Not supported	---
	05	Vendor Code	1	---	---	UDINT	RO	Not supported	---
	06	Unit Version	*1	---	---	UDINT	RO	Not supported	---
	07	Serial Number	*2	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
1001	---	Production Info	---	---	---	---	---	---	---
	00	Number of Entries	4	4	---	USINT	RO	Not supported	---
	01	Lot Number	*3	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
	02	Hardware Version	*4	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---
	03	Software Version	*5	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---

*1. Bits 24 to 31: Integer part of the Unit version
Bits 16 to 23: Fractional part of the Unit version
Bits 0 to 15: Reserved
(Example) For Ver.1.0, 0100□□□□ hex

*2. The unique serial number of the product is given.
Bits 0 to 31: Serial number

*3. The date of manufacture is given for the "lot number".
Bits 24 to 31: Day of manufacture
Bits 16 to 23: Month of manufacture
Bits 8 to 15: Year of manufacture
Bits 0 to 7: Reserved

*4. The hardware version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

*5. The software version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

Objects That Accept I/O Allocations

These objects accept I/O allocations.
They cannot be accessed through message communications.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6000	---	FSoE Slave Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Slave CMD	00 hex	00 to FF hex	---	BYTE	RO	Supported	---
	02	FSoE Slave Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---
	03	FSoE Slave CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6001	---	Safety Input Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Input 1st Byte	00 hex	00 to FF hex	---	BYTE	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6002	---	Standard Input Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Input 1st Byte	00 hex	00 to FF hex *1	---	BYTE	RO	Supported	---
	02	Standard Input 2nd Byte	00 hex	00 to FF hex *2	---	BYTE	RO	Supported	---

*1. The details of the "Standard Input 1st Byte" are as follows:
Bit 0: So00 Monitor Value
Bit 1: So01 Monitor Value
Bit 2: So02 Monitor Value

Bit 3: So03 Monitor Value
Bit 4: Safety Connection Status
Bit 5: Safety Output Terminal Status
Bit 6: Unit Normal Status
Bit 7: IO Power Supply Error Flag

*2. The details of the "Standard Input 2nd Byte" are as follows:
Bit 0: So00 Status
Bit 1: So01 Status
Bit 2: So02 Status
Bit 3: So03 Status
Bits 4 to 7: Reserved

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7000	---	FSoE Master Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Master CMD	00 hex	00 to FF hex	---	BYTE	RW	Supported	---
	02	FSoE Master Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---
	03	FSoE Master CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7001	---	Safety Output Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Output 1st Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7002	---	Standard Output Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Output 1st Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---
	02	Standard Output 2nd Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---

Other Objects

This section lists other objects.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5000	---	Device Safety Address	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Address	0000 hex	0000 to FFFF hex	---	UINT	RO	Not supported	---

A-3-6 NX-SOH200 Safety Output Unit

Unit Information Objects

These objects give the product information.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
1000	---	NX Bus Identity	---	---	---	---	---	---	---
	00	Number of Entries	7	7	---	USINT	RO	Not supported	---
	02	Model	NX-SOH200	---	---	ARRAY [0..11] OF BYTE	RO	Not supported	---
	03	Device Type	00000A04 hex	---	---	UDINT	RO	Not supported	---
	04	Product Code	00A40200 hex	---	---	UDINT	RO	Not supported	---
	05	Vendor Code	1	---	---	UDINT	RO	Not supported	---
	06	Unit Version	*1	---	---	UDINT	RO	Not supported	---
	07	Serial Number	*2	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
1001	---	Production Info	---	---	---	---	---	---	---
	00	Number of Entries	4	4	---	USINT	RO	Not supported	---
	01	Lot Number	*3	00000000 to FFFFFFFF hex	---	UDINT	RO	Not supported	---
	02	Hardware Version	*4	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---
	03	Software Version	*5	---	---	ARRAY [0..19] OF BYTE	RO	Not supported	---

*1. Bits 24 to 31: Integer part of the Unit version
Bits 16 to 23: Fractional part of the Unit version
Bits 0 to 15: Reserved

(Example) For Ver.1.0, 0100□□□□ hex

*2. The unique serial number of the product is given.
Bits 0 to 31: Serial number

*3. The date of manufacture is given for the "lot number".
Bits 24 to 31: Day of manufacture
Bits 16 to 23: Month of manufacture
Bits 8 to 15: Year of manufacture
Bits 0 to 7: Reserved

*4. The hardware version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

*5. The software version is given in order in the lowest elements of the array. Unused elements are padded with spaces.

Objects That Accept I/O Allocations

These objects accept I/O allocations.
They cannot be accessed through message communications.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6000	---	FSoE Slave Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Slave CMD	00 hex	00 to FF hex	---	BYTE	RO	Supported	---
	02	FSoE Slave Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---
	03	FSoE Slave CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6001	---	Safety Input Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Input 1st Byte	00 hex	00 to FF hex	---	BYTE	RO	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
6002	---	Standard Input Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Input 1st Byte	00 hex	00 to FF hex *1	---	BYTE	RO	Supported	---
	02	Standard Input 2nd Byte	00 hex	00 to FF hex *2	---	BYTE	RO	Supported	---

*1. The details of the "Standard Input 1st Byte" are as follows:
Bit 0: So00 Monitor Value
Bit 1: So01 Monitor Value
Bit 2: Safety Connection Status
Bit 3: Safety Output Terminal Status
Bit 4: Unit Normal Status
Bit 5: IO Power Supply Error Flag
Bits 6 to 7: Reserved

*2. The details of the "Standard Input 2nd Byte" are as follows:
Bit 0: So00 Status
Bit 1: So01 Status
Bits 2 to 7: Reserved

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7000	---	FSoE Master Frame Elements	---	---	---	---	---	---	---
	00	Number of Entries	3	3	---	USINT	RO	Not supported	---
	01	FSoE Master CMD	00 hex	00 to FF hex	---	BYTE	RW	Supported	---
	02	FSoE Master Conn_ID	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---
	03	FSoE Master CRC_0	0000 hex	0000 to FFFF hex	---	WORD	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7001	---	Safety Output Data	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Output 1st Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
7002	---	Standard Output Data	---	---	---	---	---	---	---
	00	Number of Entries	2	2	---	USINT	RO	Not supported	---
	01	Standard Output 1st Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---
	02	Standard Output 2nd Byte	00 hex	00 to FF hex	---	BYTE	RW	Supported	---

Other Objects

This section lists other objects.

Index (hex)	Subindex (hex)	Object name	Default value	Data range	Unit	Data type	Access	I/O allocation	Data attribute
5000	---	Device Safety Address	---	---	---	---	---	---	---
	00	Number of Entries	1	1	---	USINT	RO	Not supported	---
	01	Safety Address	0000 hex	0000 to FFFF hex	---	UINT	RO	Not supported	---

A-4 Application Examples

Refer to the *NX-series Safety Control Unit Instructions Reference Manual (Cat. No. Z931) for details on the instructions that are used in each example.*

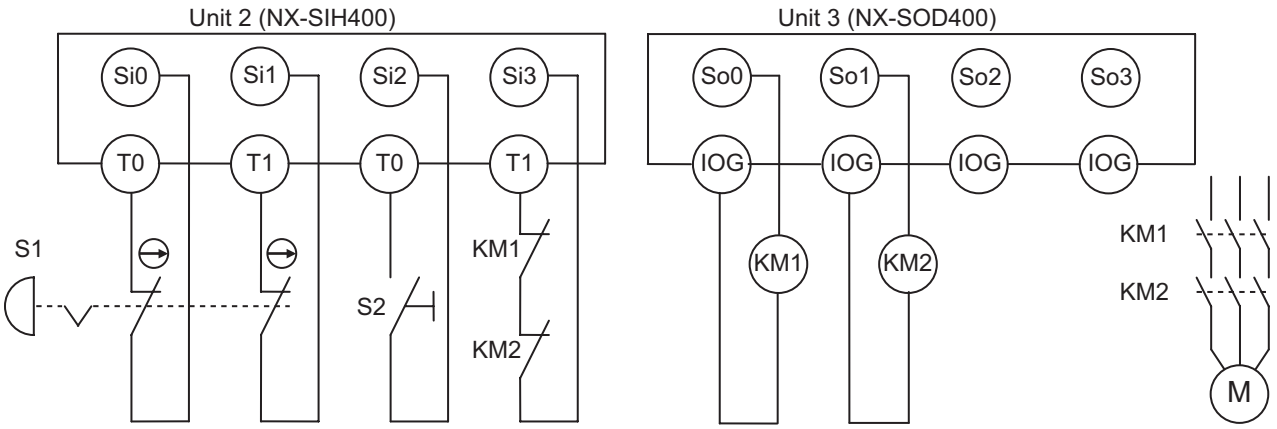
A-4-1 Emergency Stop Pushbutton Switches

Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe	Emergency stop pushbutton	0	Manual

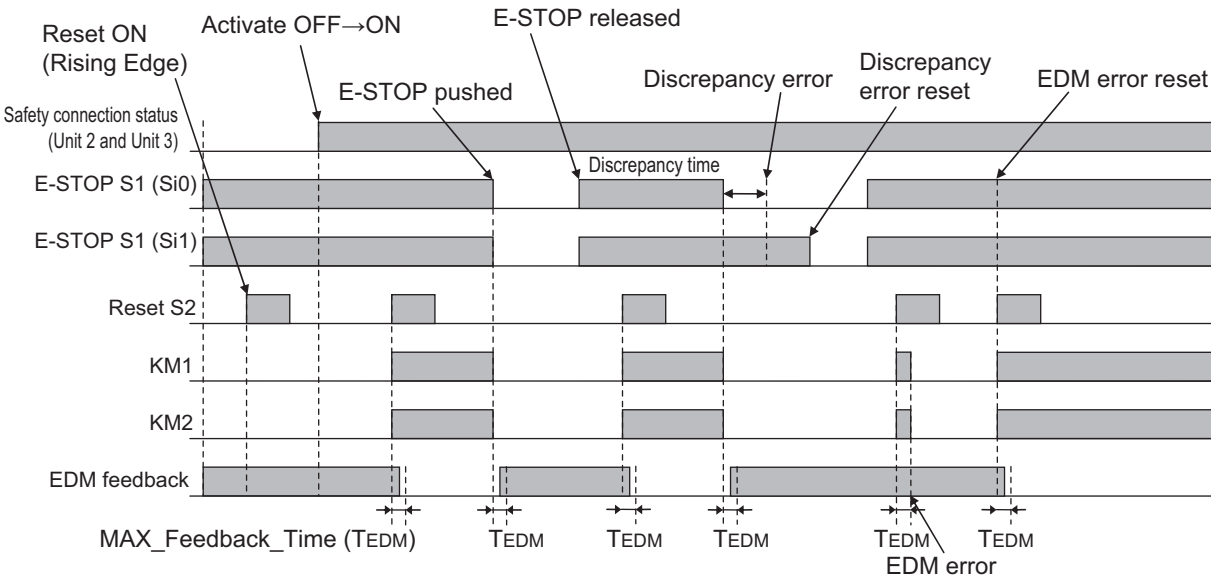
Motor M stops when emergency stop pushbutton S1 is pressed.

Wiring



S1: Emergency stop pushbutton
S2: Reset switch
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SOD400 (N3 : Instance1)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

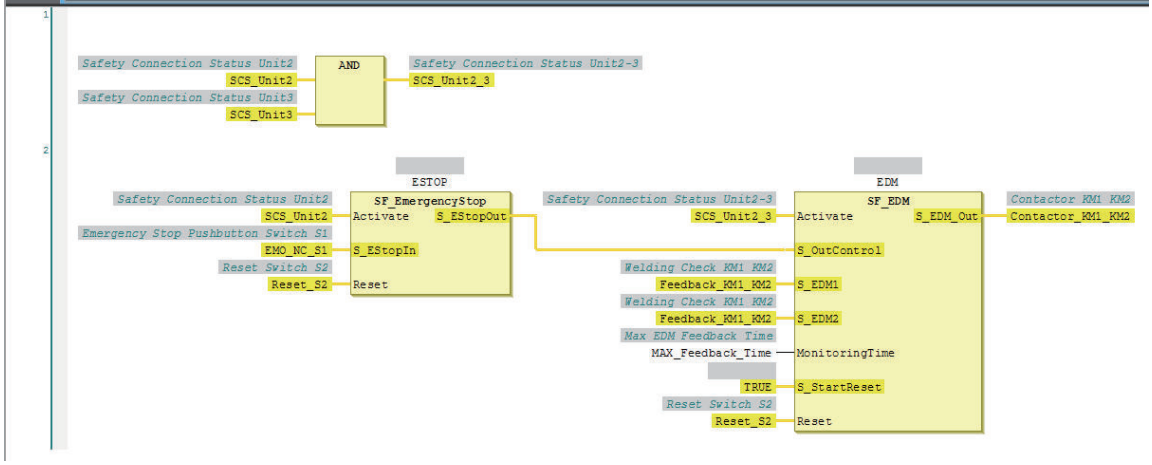
● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	NX-SOD400					
	Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program

Internals / Externals

Name	Data Type	Initial Value	Constant	Comment
MAX_Feedback_Time	TIME	t#300ms	☑	Max EDM Feedback Time
SCS_Unit2_3	SAFEBOOL	FALSE	☐	Safety Connection Status Unit2-3
ESTOP	SF_EmergencyStop		☐	
EDM	SF_EDM		☐	



Precautions for Safe Use

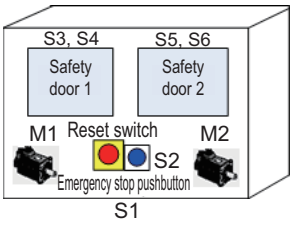
- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

A-4-2 Safety Doors

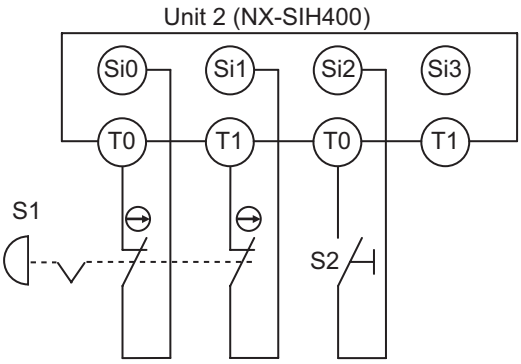
Application Overview

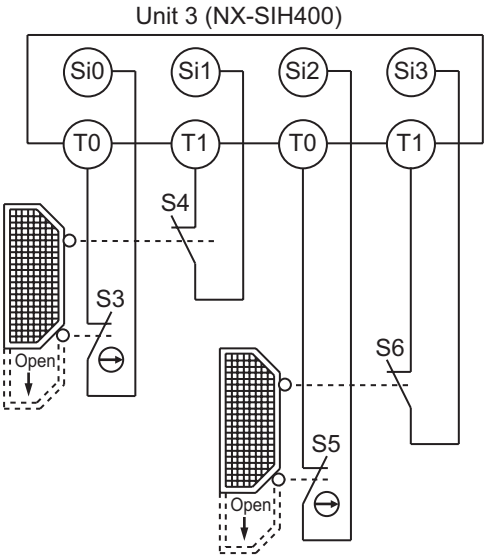
Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe (Safety Door)	Safety limit switches 1 and 2	0	Auto
	Emergency stop pushbutton	0	Manual

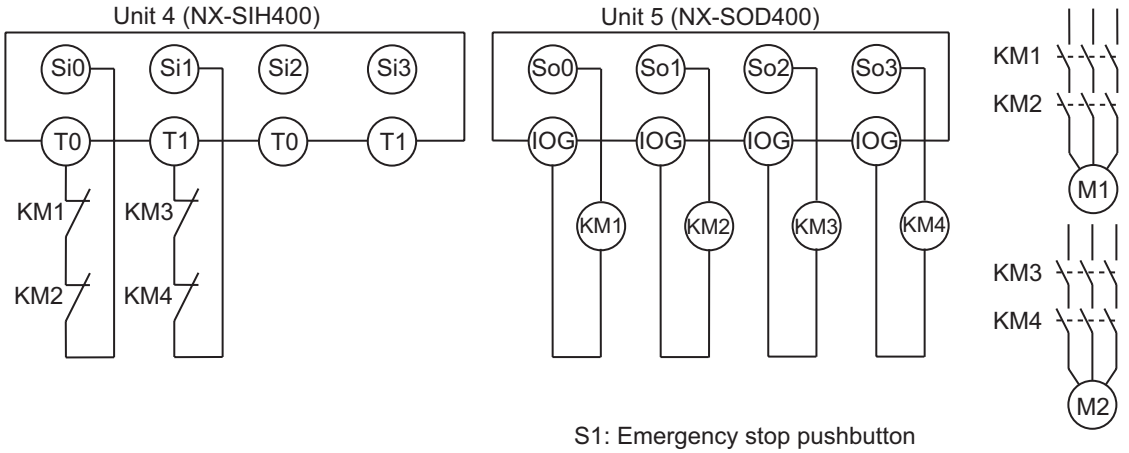
M1 stops when safety door 1 (S3, S4) is opened.
M2 stops when safety door 2 (S5, S6) is opened.
Both M1 and M2 stop when the emergency stop pushbutton S1 is pressed.



Wiring

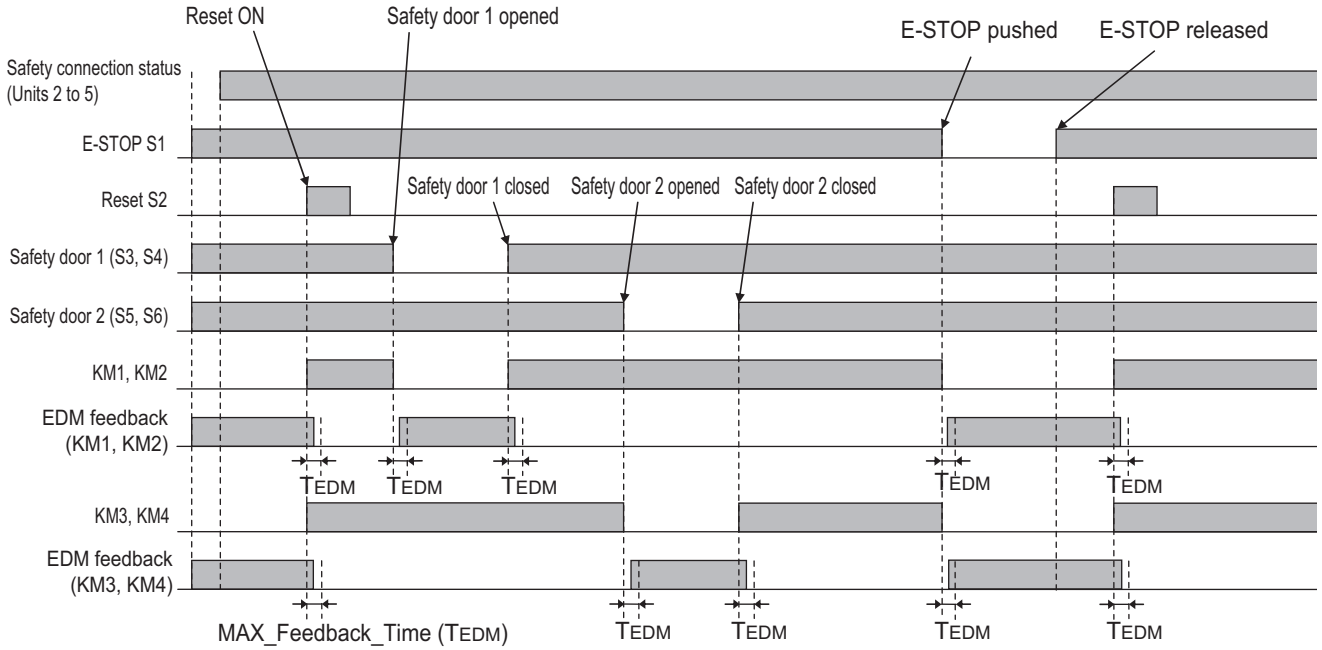






S1: Emergency stop pushbutton
S2: Reset switch
S3, S5: Safety limit switches
S4, S6: Limit switches (NO contacts)
KM1, KM2, KM3, KM4: Contactors
M1, M2: Motors

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
	Si 3					

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact For Single Channel	Si 0	0ms	0ms	0ms	T0	Safety Limit Switch(NC)
Mechanical Contact For Single Channel	Si 1	0ms	0ms	0ms	T1	Limit Switch(NO)
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Safety Limit Switch(NC)
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	Limit Switch(NO)

Node1/Unit4 : NX-SIH400 (N4 : Instance2)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact For Single Channel	Si 0	0ms	0ms	0ms	T0	EDM(Contact Welding Detection)
Mechanical Contact For Single Channel	Si 1	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)
	Si 2					
	Si 3					

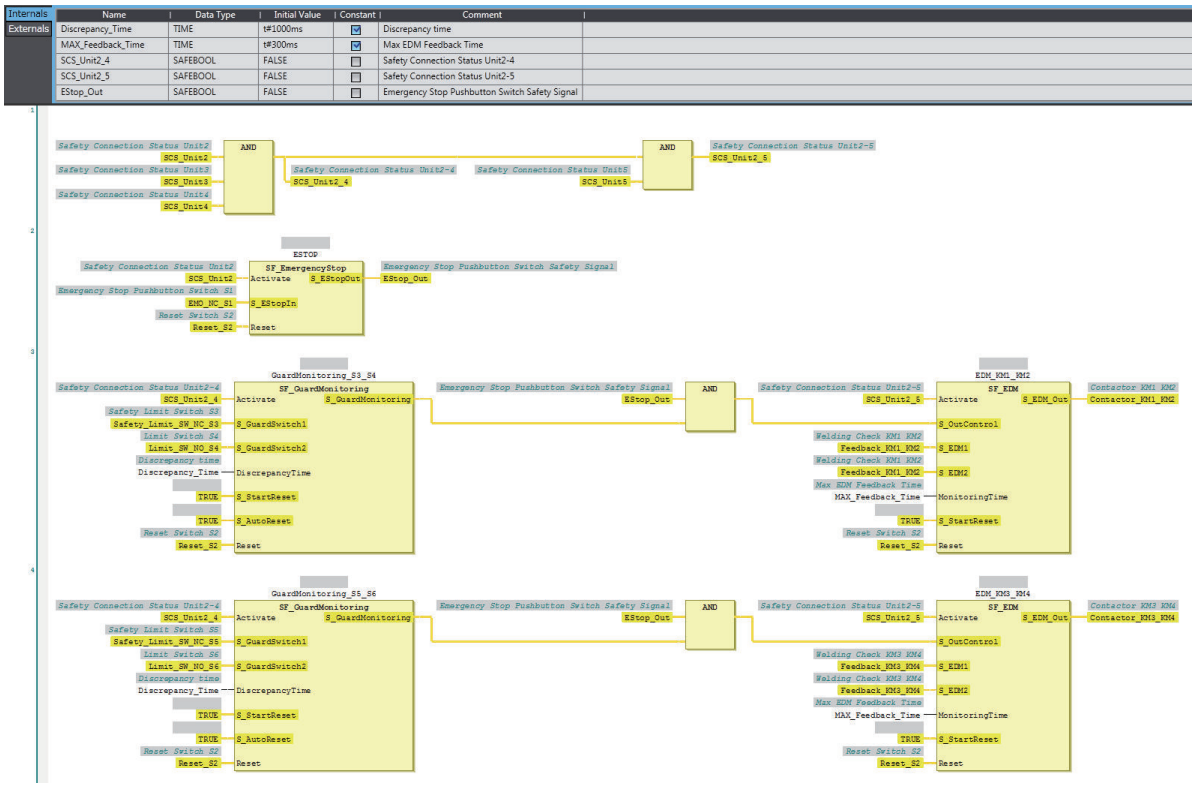
Node1/Unit5 : NX-SOD400 (N5 : Instance3)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
Dual Output with Test Pulse	So 2	2 Safety Relays w/ Welding Check
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch(2NC)	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch	Global Variables
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Safety_Limit_SW_NC_S3	Safety Limit Switch(NC)	Global Variables
	Si01 Logical Value	R	SAFEBOOL	Limit_SW_NO_S4	Limit Switch(NO)	Global Variables
	Si02 Logical Value	R	SAFEBOOL	Safety_Limit_SW_NC_S5	Safety Limit Switch(NC)	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Limit_SW_NO_S6	Limit Switch(NO)	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	EDM(Contact Welding Detection)	Global Variables
	Si01 Logical Value	R	SAFEBOOL	Feedback_KM3_KM4	EDM(Contact Welding Detection)	Global Variables
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit5	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit5	Safety Connection Status Unit5	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	2 Safety Relays w/ Welding Check	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL	Contactor_KM3_KM4	2 Safety Relays w/ Welding Check	Global Variables
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.
- Refer to ISO 14119:2013 for additional measures to minimize the possibility of interlocking devices associated with guards from being disabled.

A-4-3 Safety Laser Scanners

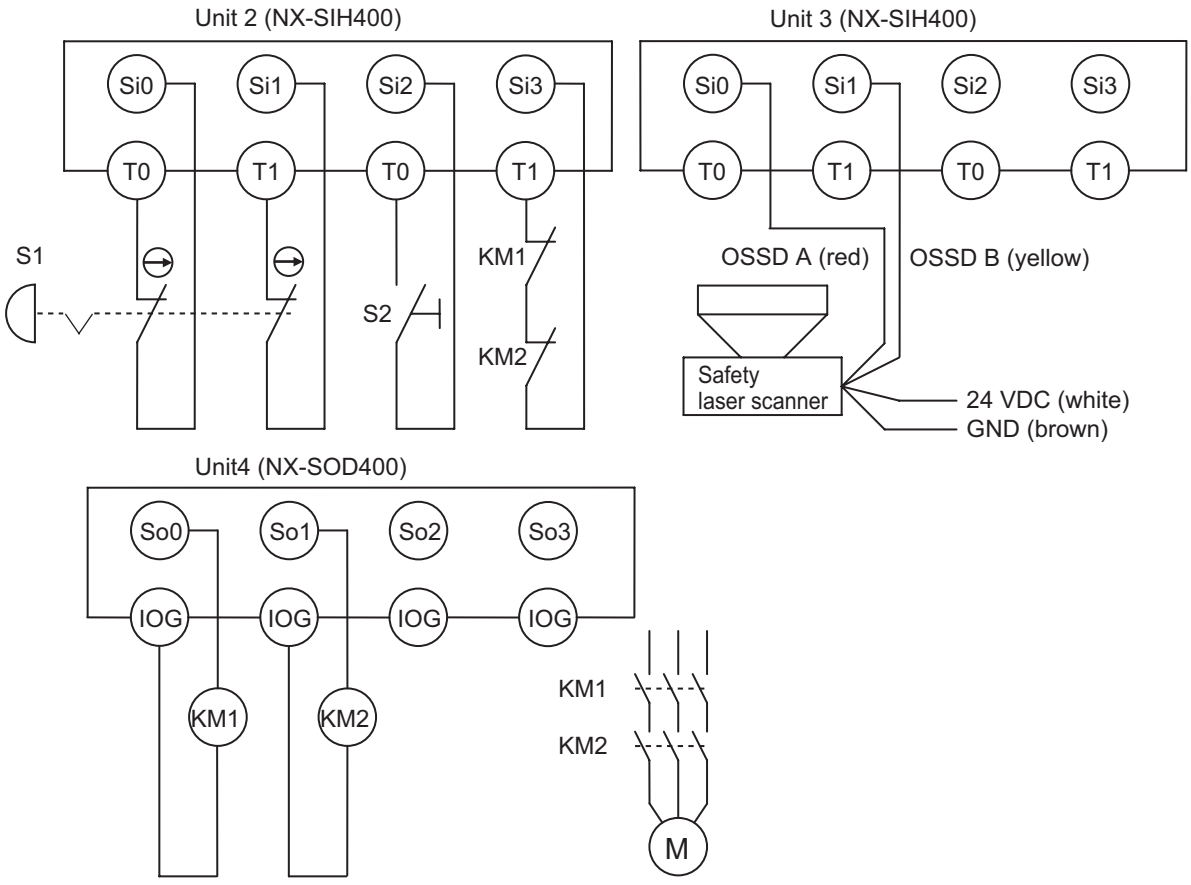
Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 3/PLd (Laser Scanner)	Laser scanner	0	Auto
	Emergency stop pushbutton	0	Manual

AGV stops when emergency stop pushbutton S1 is pressed.

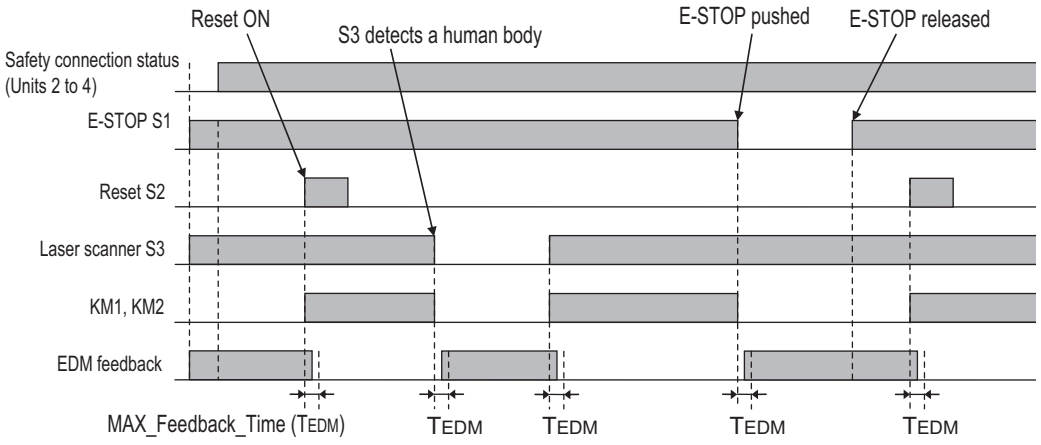
AGV stops when laser scanner S3 detects that persons or objects approach into the safety zone.

Wiring



S1: Emergency stop pushbutton
S2: Reset switch
S3: Safety laser scanner
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Semiconductor Output for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	Not Used	Dual Safety Semiconductor Output(Equivalent)
	Si 1	500ms	0ms	0ms	Not Used	
	Si 2					
	Si 3					

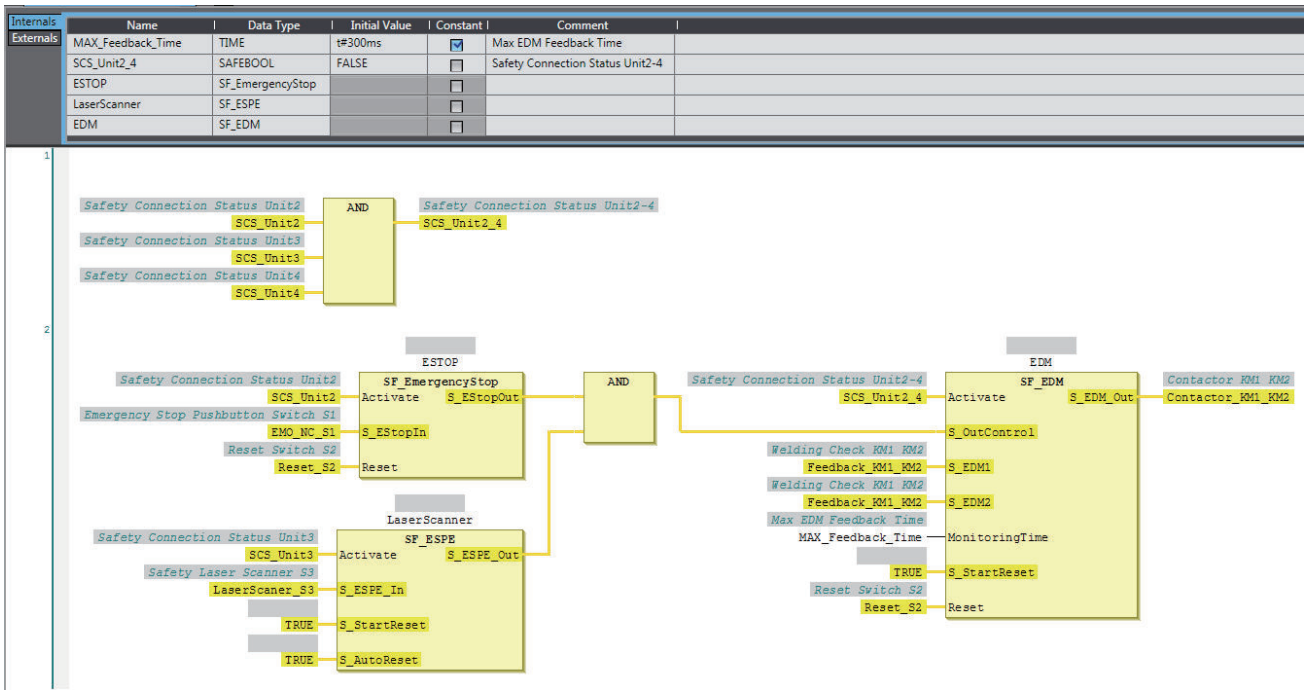
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	LaserScaner_S3	Safety Laser Scanner S3	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

A-4-4 Safety Door Switches with Magnetic Locks and Key Selector Switches

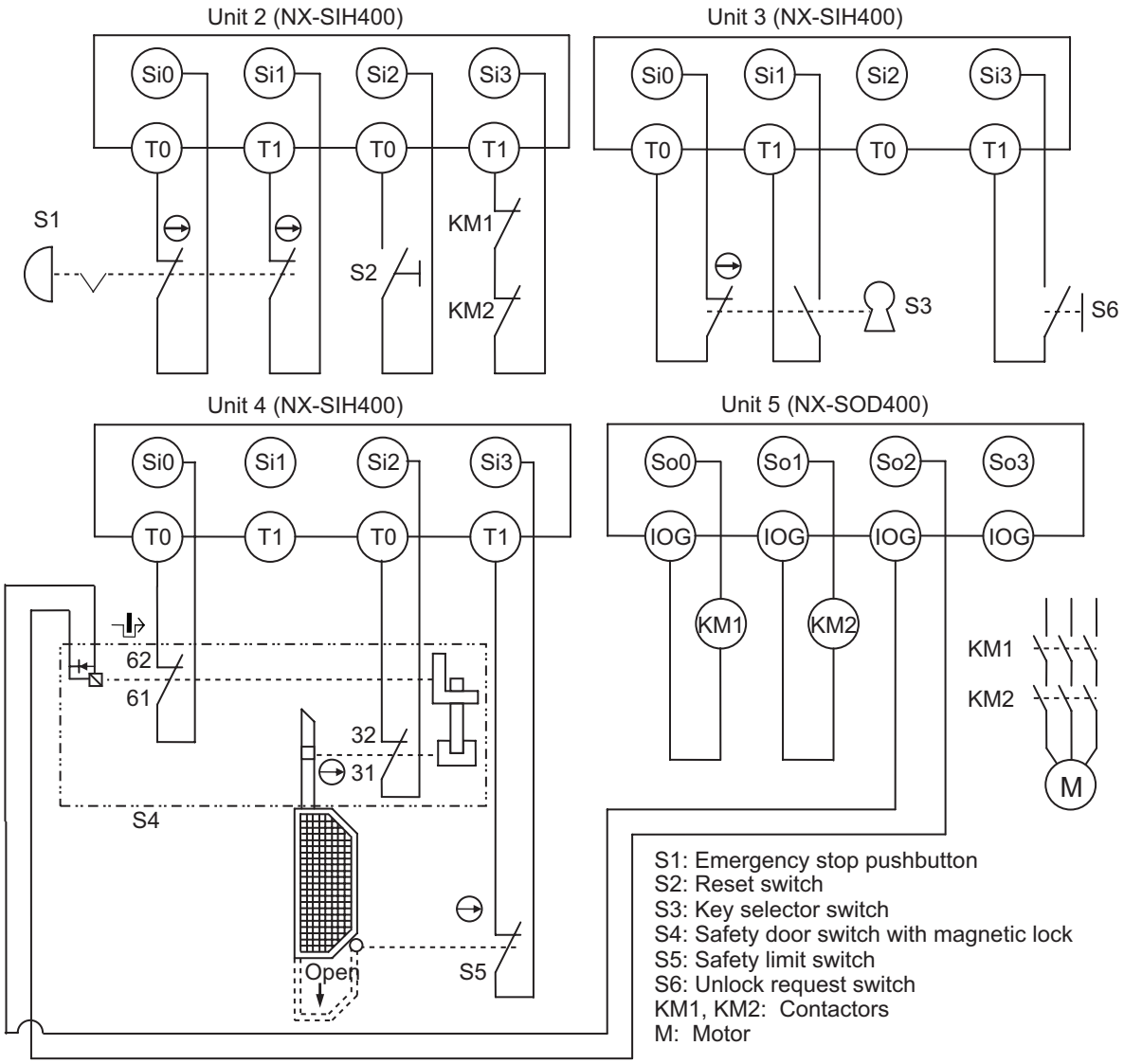
Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe (Safety Door Switches with Magnetic Locks)	• Emergency stop pushbutton • Safety door switch with magnetic lock (mechanical lock type) • Key selector switch	0	Manual

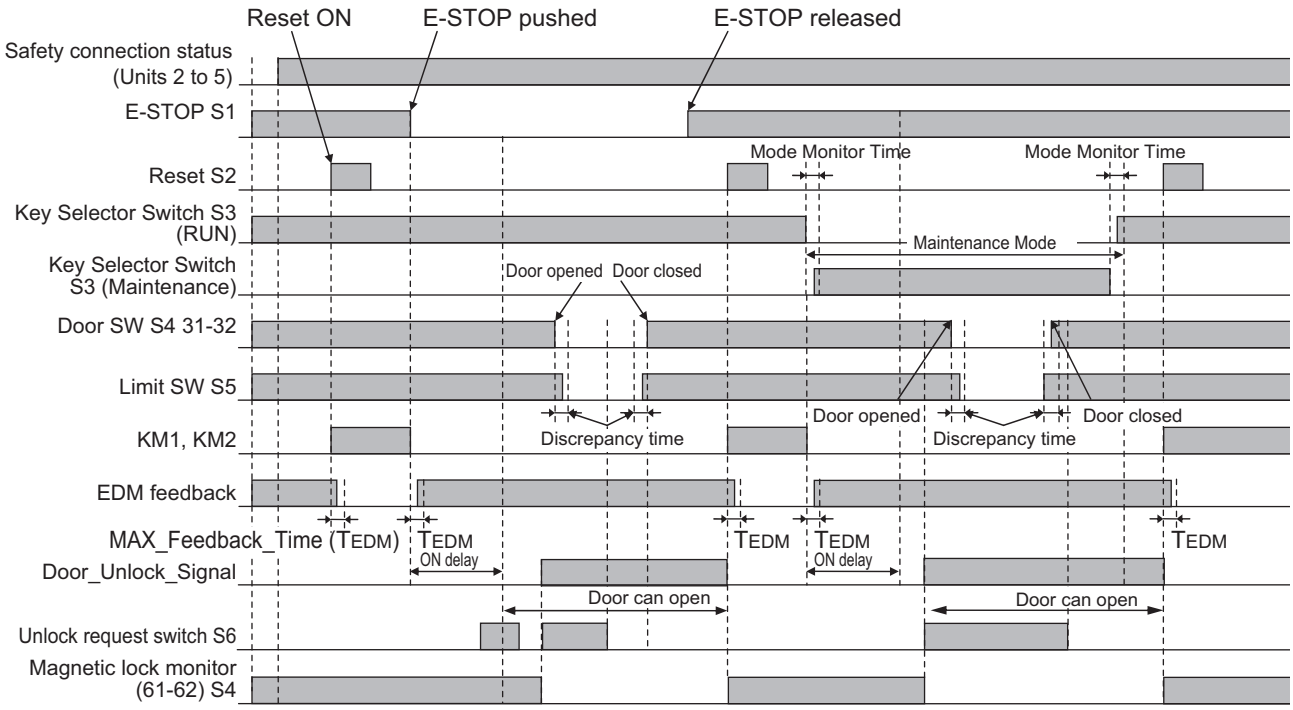
Safety doors S4 and S5 cannot be opened while the user mode is set for normal operation. The outputs are turned OFF by changing to maintenance mode and the safety doors can be opened 5 seconds later.

The outputs also turn OFF when emergency pushbutton S1 is pressed.

Wiring


Unit 2 (NX-SIH400)
Si0
Si1
Si2
Si3
T0
T1
T0
T1
S1
KM1
S2
KM2
Unit 3 (NX-SIH400)
Si0
Si1
Si2
Si3
T0
T1
T0
T1
S3
S6
Unit 4 (NX-SIH400)
Si0
Si1
Si2
Si3
T0
T1
T0
T1
62
61
32
31
S4
Open
S5
Unit 5 (NX-SOD400)
So0
So1
So2
So3
IOG
IOG
IOG
IOG
KM1
KM2
KM1
KM2
M
S1: Emergency stop pushbutton
S2: Reset switch
S3: Key selector switch
S4: Safety door switch with magnetic lock
S5: Safety limit switch
S6: Unlock request switch
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact For Single Channel	Si 0	0ms	0ms	0ms	T0	Single Contact
Mechanical Contact For Single Channel	Si 1	0ms	0ms	0ms	T1	Single Contact
	Si 2					
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	Single Contact

Node1/Unit4 : NX-SIH400 (N4 : Instance2)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact For Single Channel	Si 0	0ms	0ms	0ms	T0	Safety Switch(NC)
	Si 1					
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Safety Switch(NC)
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	Safety Limit Switch(NC)

Node1/Unit5 : NX-SOD400 (N5 : Instance3)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
Single Channel with Test Pulse	So 2	Door Unlock Signal
	So 3	

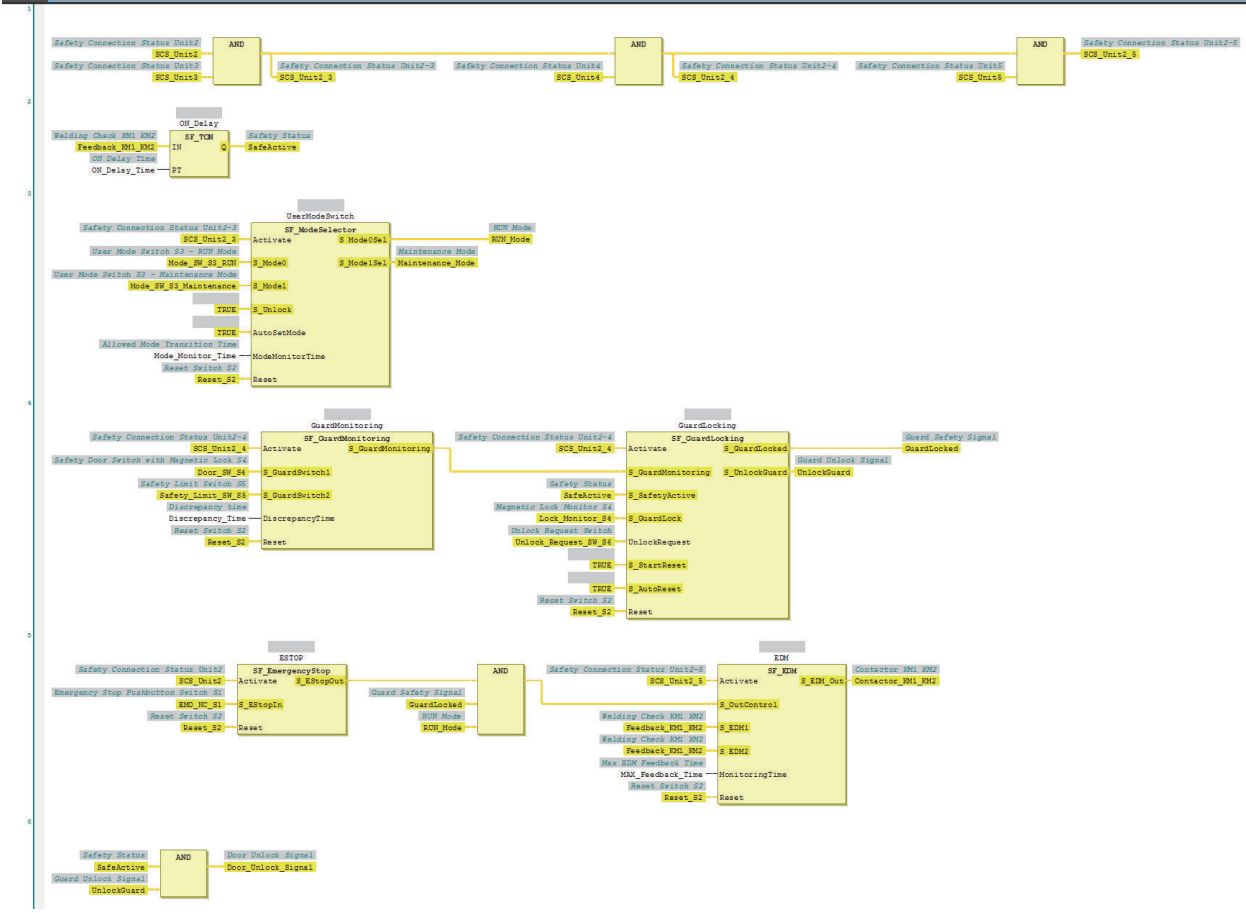
I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch(2NC)	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	EDM(Contact Welding Detection)	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Mode_SW_S3_RUN	Single Contact	Global Variables
	Si01 Logical Value	R	SAFEBOOL	Mode_SW_S3_Maintenance	Single Contact	Global Variables
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL	Unlock_Request_SW_S6	Single Contact	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Lock_Monitor_S4	Safety Switch(NC)	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Door_SW_S4	Safety Switch(NC)	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Safety_Limit_SW_S5	Safety Limit Switch(NC)	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit5	NX-SOD400					
	Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit5	Safety Connection Status Unit5	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	2 Safety Relays w/ Welding Check	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL	Door_Unlock_Signal	Door Unlock Signal	Global Variables
	So03 Output Value	W	SAFEBOOL			

Program

Internals / Externals

Name	Data Type	Initial Value	Constant	Comment
Mode_Monitor_Time	TIME	t#2s	☑	Allowed Mode Transition Time
MAX_Feedback_Time	TIME	t#300ms	☑	Max EDM Feedback Time
ON_Delay_Time	TIME	t#5s	☑	ON Delay Time
Discrepancy_Time	TIME	t#1000ms	☑	Discrepancy time
RUN_Mode	SAFEBOOL	FALSE	☐	RUN Mode
Maintenance_Mode	SAFEBOOL	FALSE	☐	Maintenance Mode
SafeActive	SAFEBOOL	FALSE	☐	Safety Status
GuardLocked	SAFEBOOL	FALSE	☐	Guard Safety Signal
UnlockGuard	SAFEBOOL	FALSE	☐	Guard Unlock Signal
SCS_Unit2_3	SAFEBOOL	FALSE	☐	Safety Connection Status Unit2-3
SCS_Unit2_4	SAFEBOOL	FALSE	☐	Safety Connection Status Unit2-4
SCS_Unit2_5	SAFEBOOL	FALSE	☐	Safety Connection Status Unit2-5



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.
- Refer to ISO 14119:2013 for additional measures to minimize the possibility of interlocking devices associated with guards from being disabled.

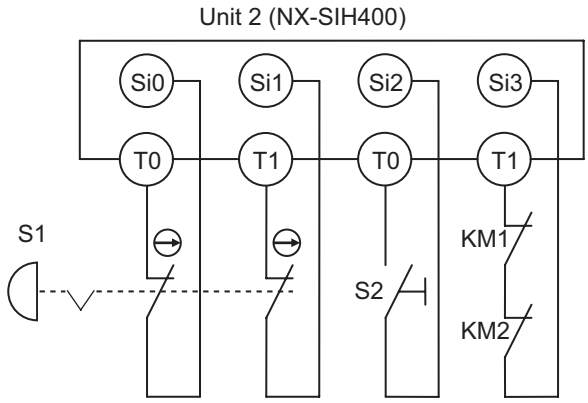
A-4-5 Enable Switches

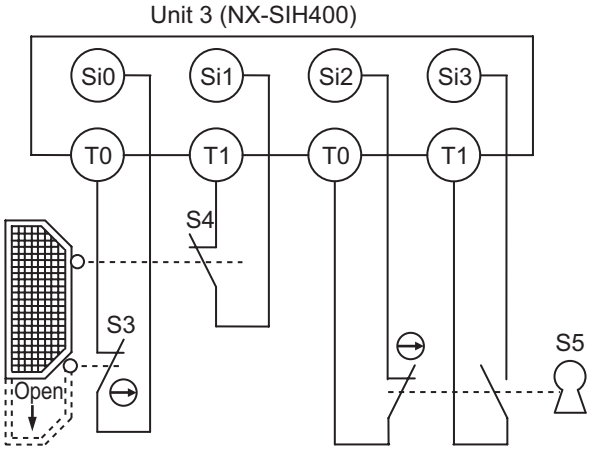
Application Overview

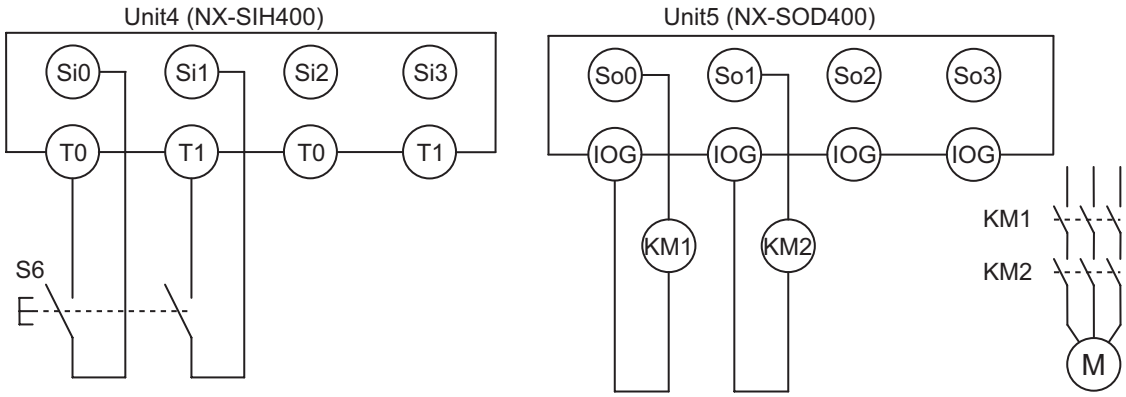
Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe (Enable Switch)	• Emergency stop pushbutton • Safety limit switch • Key selector switch • Enable switch	0	Manual

Motor M stops when safety doors S3 and S4 are opened or key Selector switch S5 is maintenance mode.
However, even if key selector switch S5 is set to maintenance mode, motor M will operate if enable switch S6 is ON.

Wiring

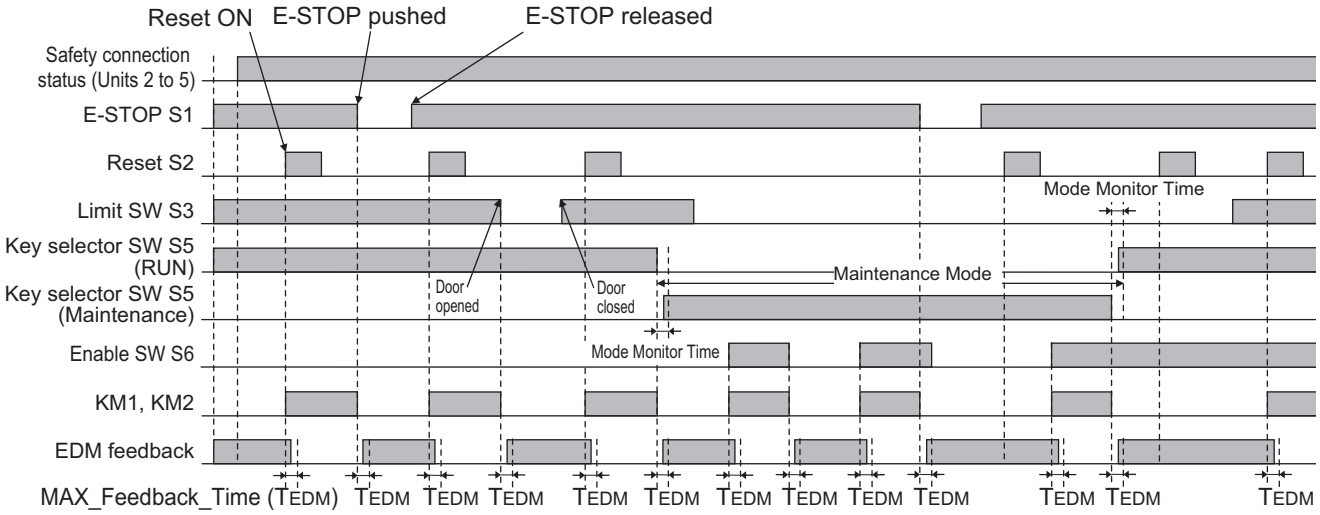






S1: Emergency stop pushbutton
S2: Reset switch
S3: Safety limit switch
S4: Limit switch (NO contacts)
S5: Key selector switch
S6: Enabling switch (When OMRON enabling switch A4E or A4EG is used)
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact For Single Channel	Si 0	0ms	0ms	0ms	T0	Safety Limit Switch(NC)
Mechanical Contact For Single Channel	Si 1	0ms	0ms	0ms	T1	Limit Switch(NO)
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Single Contact
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	Single Contact

Node1/Unit4 : NX-SIH400 (N4 : Instance2)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Enable Switch(2NO)
	Si 1	500ms	0ms	0ms	T1	
	Si 2					
	Si 3					

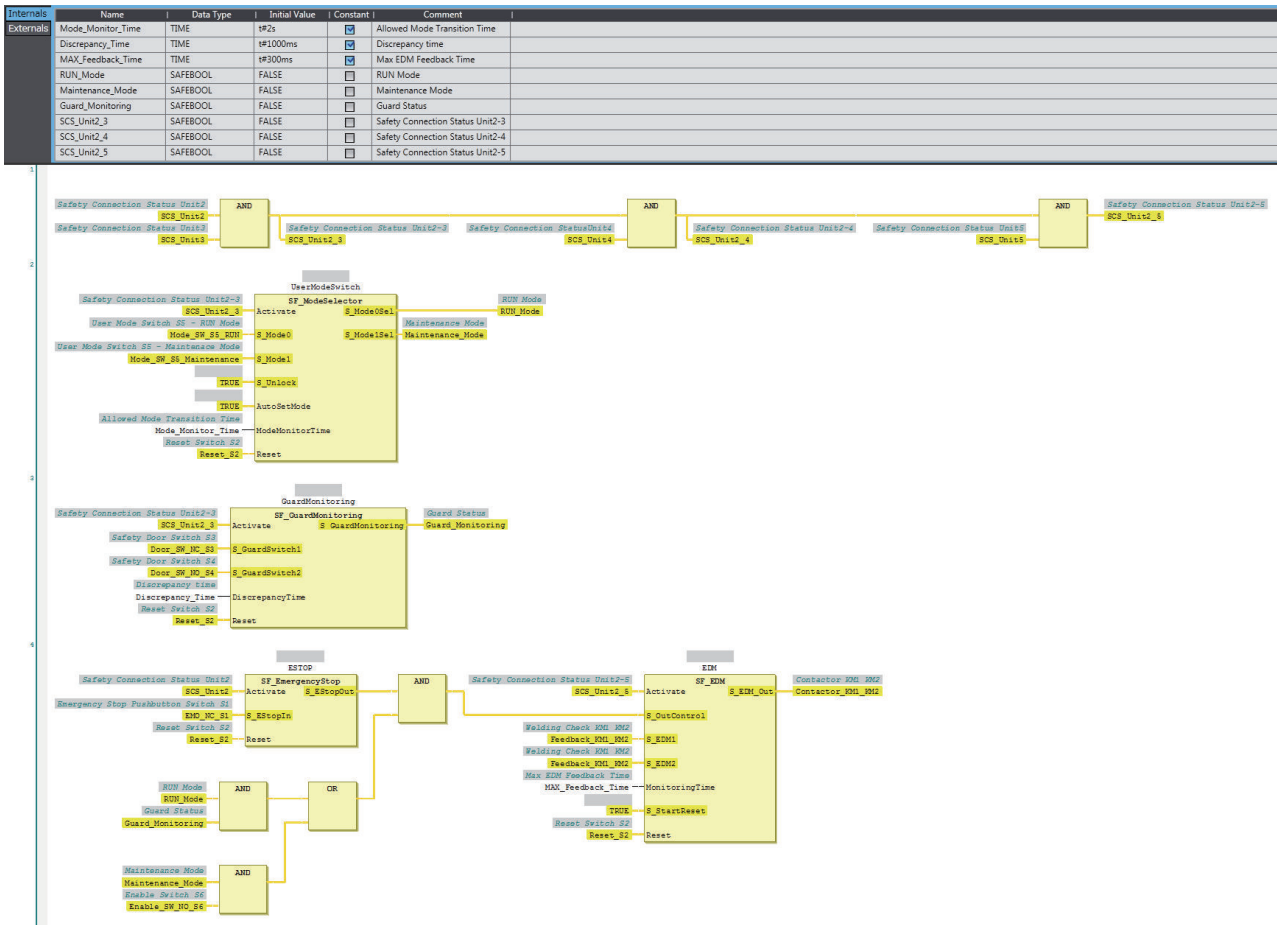
Node1/Unit5 : NX-SOD400 (N5 : Instance3)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch(2NC)	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	EDM(Contact Welding Detection)	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Door_SW_NC_S3	Safety Limit Switch(NC)	Global Variables
	Si01 Logical Value	R	SAFEBOOL	Door_SW_NO_S4	Limit Switch(NO)	Global Variables
	Si02 Logical Value	R	SAFEBOOL	Mode_SW_S5_RUN	Single Contact	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Mode_SW_S5_Maintenance	Single Contact	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Enable_SW_NO_S6	Enable Switch(2NO)	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit5	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit5	Safety Connection Status Unit5	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	2 Safety Relays w/ Welding Check	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.
- Refer to ISO 14119:2013 for additional measures to minimize the possibility of interlocking devices associated with guards from being disabled.

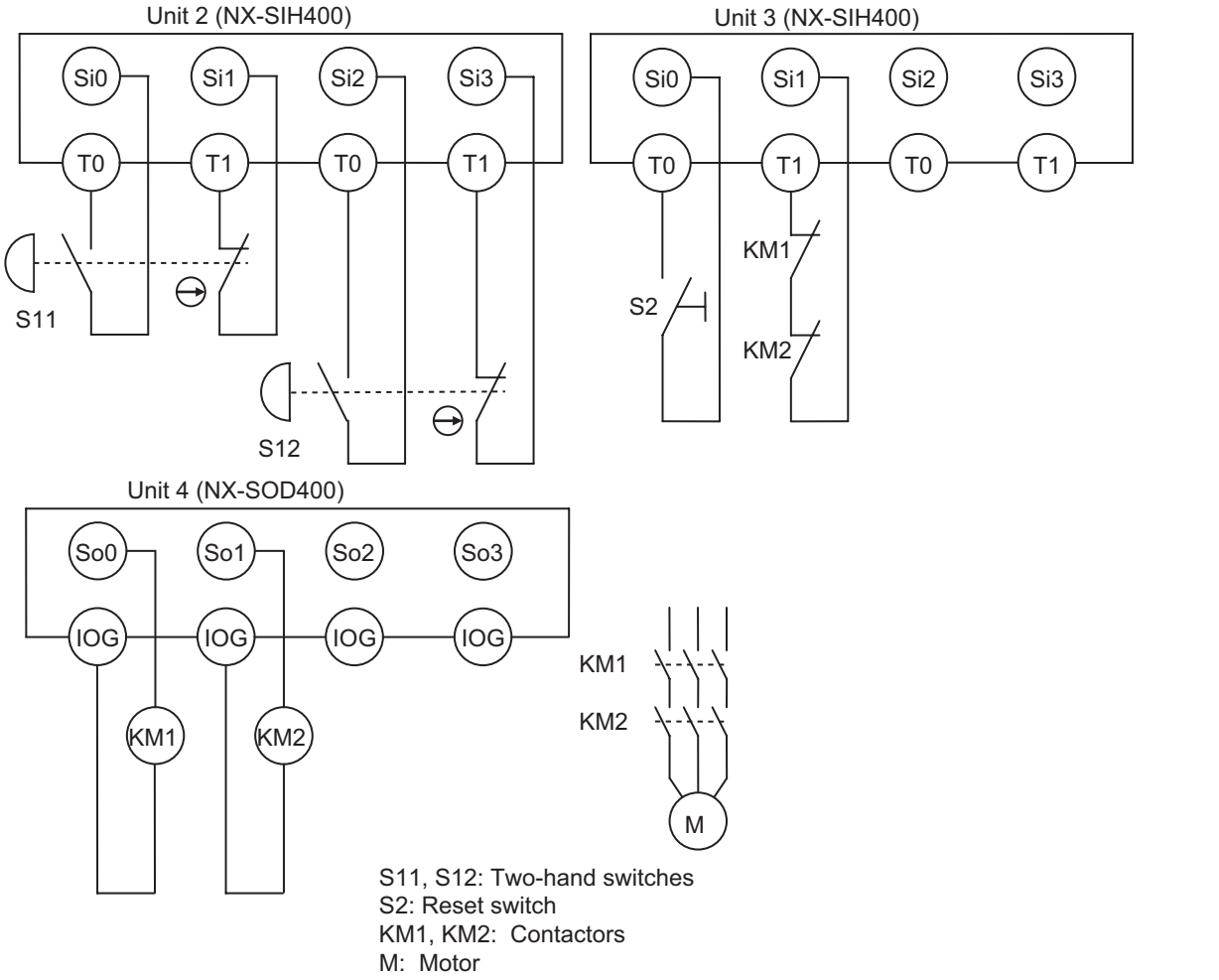
A-4-6 Two-hand Switches

Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe	Two-hand control switch	0	Auto

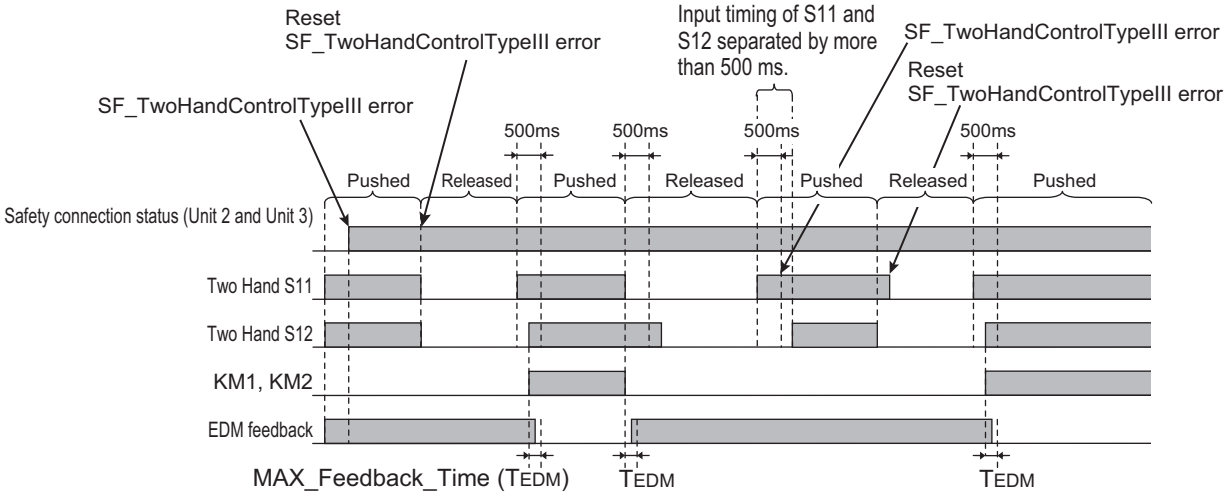
Motor M operates when two-hand control switches S11 and S12 are pressed at the same time.

Wiring



S11, S12: Two-hand switches
S2: Reset switch
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Complementary	Si 0	500ms	0ms	0ms	T0	Two-hand Control Switch
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact for Dual Channel Complementary	Si 2	500ms	0ms	0ms	T0	Two-hand Control Switch
	Si 3	500ms	0ms	0ms	T1	

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact For Single Channel	Si 0	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 1	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)
	Si 2					
	Si 3					

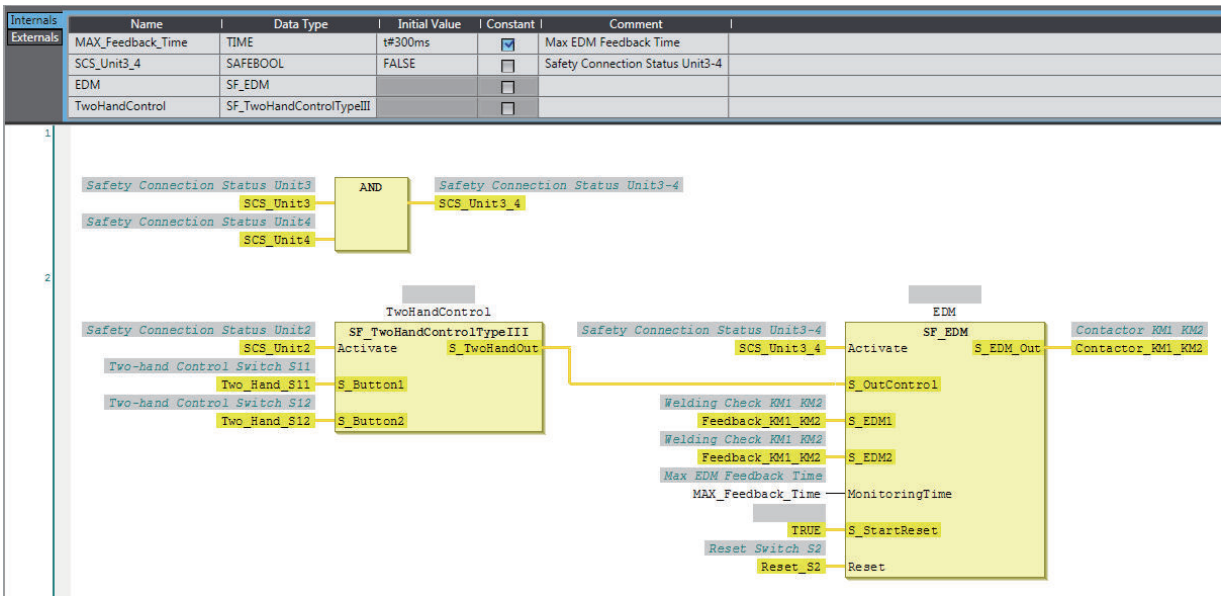
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Two_Hand_S11	Two-hand Control Switch S11	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Two_Hand_S12	Two-hand Control Switch S12	Global Variables
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si01 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

Additional Information

In this example, a reset switch is used to reset EDM errors.

A-4-7 D40A Non-contact Door Switches

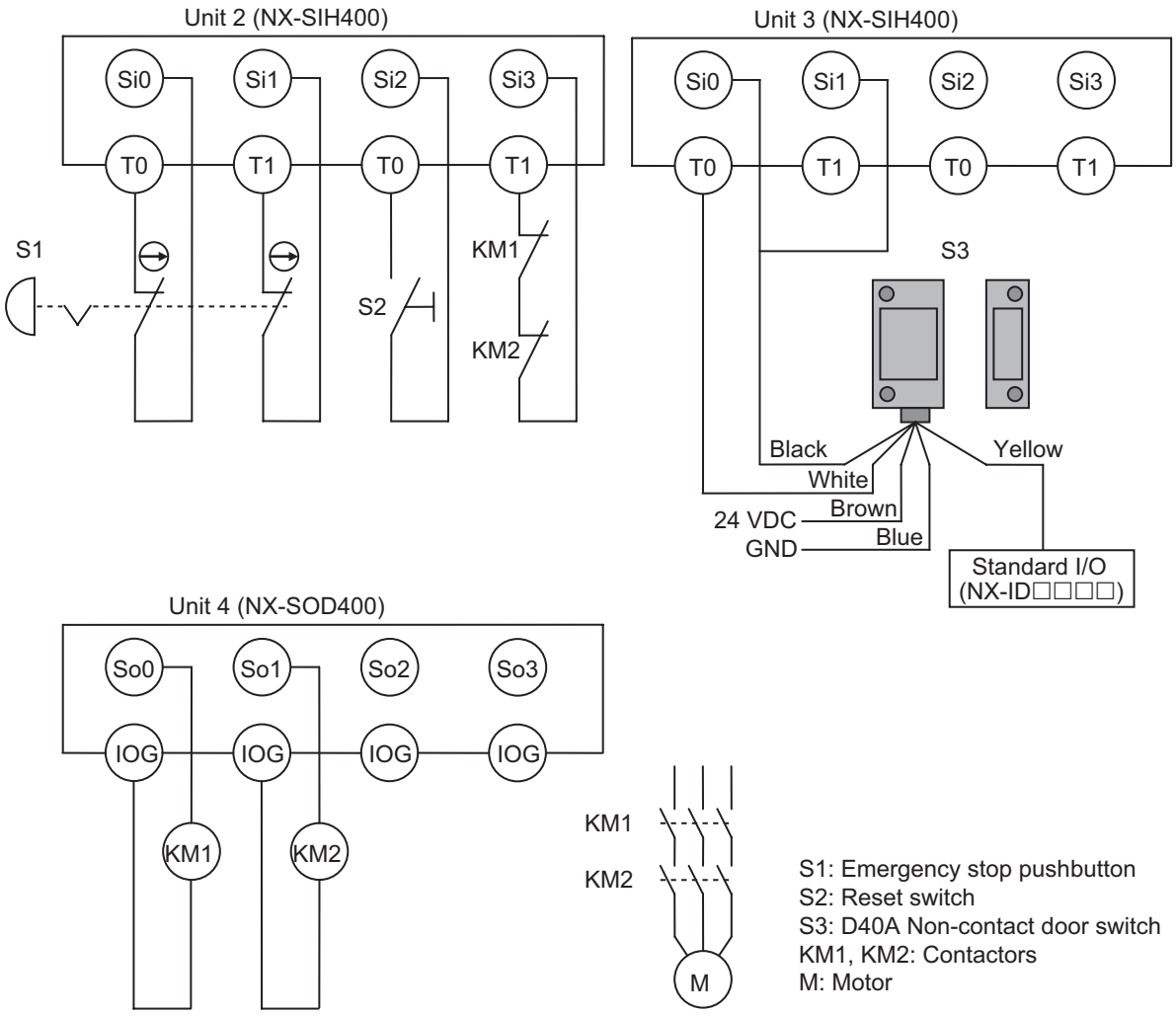
Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 3/PLd (Non-contact Door Switch)	• Emergency stop pushbutton • D40A Non-contact Door Switch	0	Manual

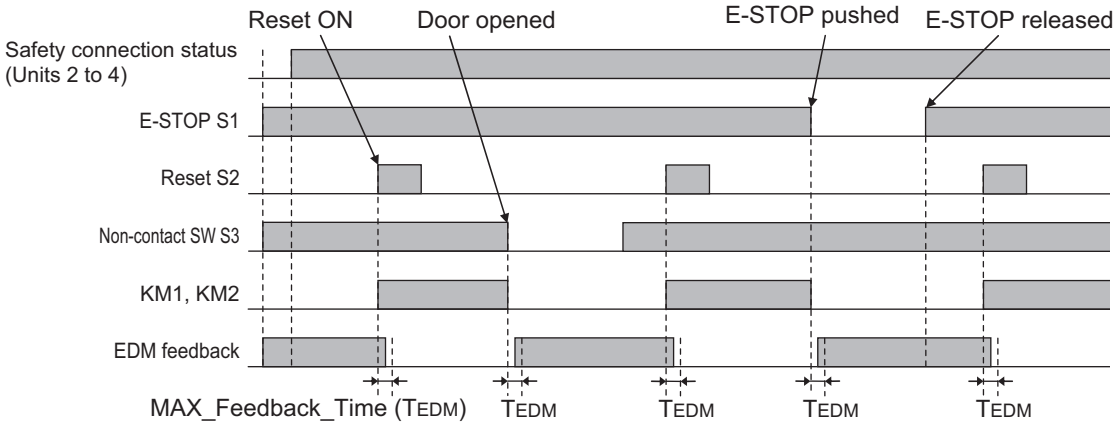
Motor M stops when emergency stop pushbutton S1 is pressed.

If either of the S3 safety doors (D40A Non-contact Door Switches) is opened, motor M will stop.

Wiring



Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Non-contact switch	Si 0	0ms	0ms	0ms	T0	Non-contact Door Switch
	Si 1	0ms	0ms	0ms	T0	
	Si 2					
	Si 3					

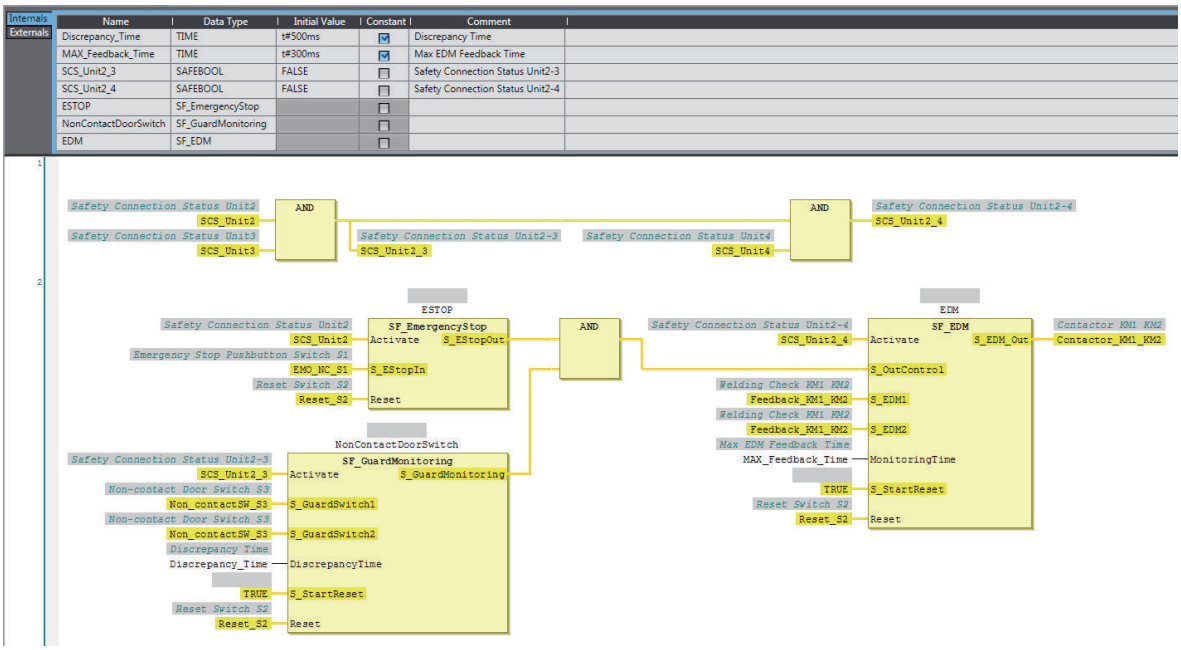
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	Non_contactSW_S3	Non-contact Door Switch S3	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.
- Refer to ISO 14119:2013 for additional measures to minimize the possibility of interlocking devices associated with guards from being disabled.

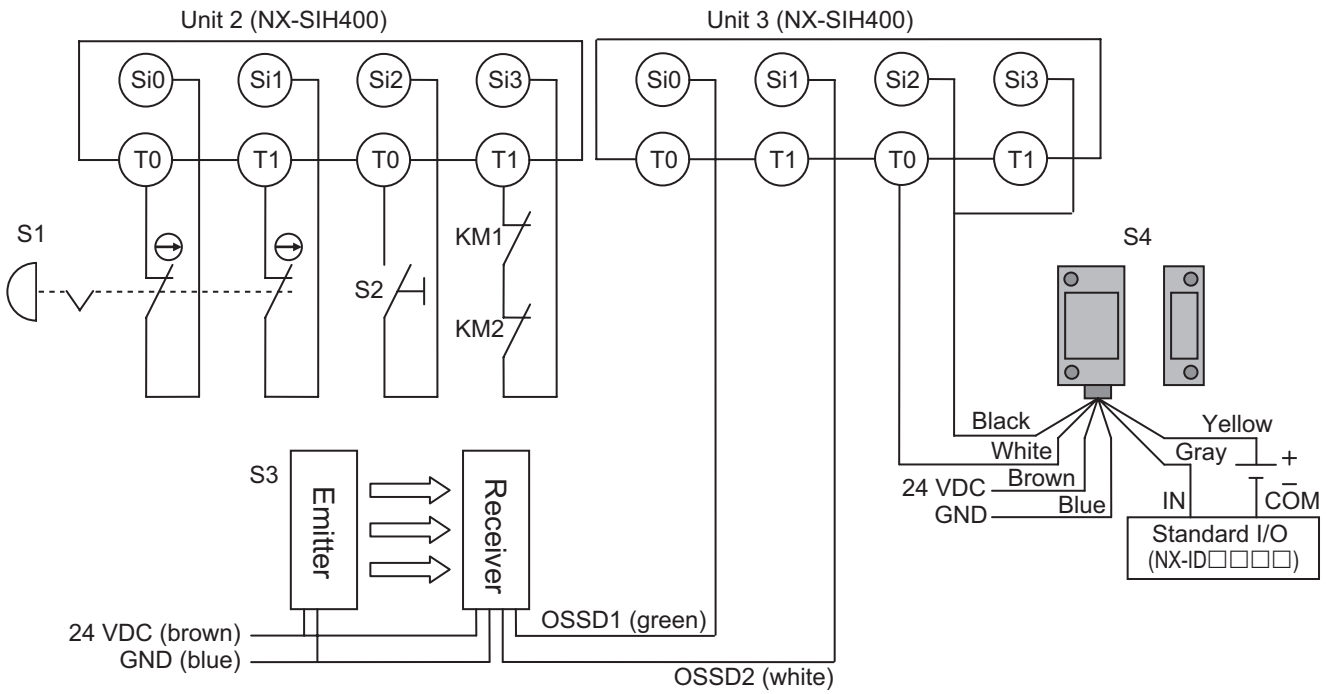
A-4-8 D40A-2/D40Z Non-contact Door Switches

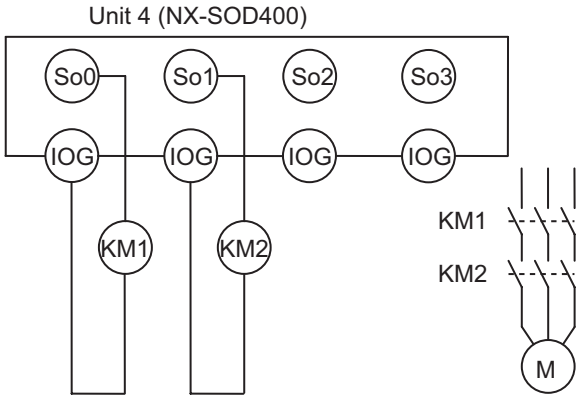
Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 4/PLe (Safety Light Curtain)	• Safety light curtain • Emergency stop pushbutton	0	Manual

If the light in the safety light curtain S3 is interrupted and the non-contact door switch S4 turns OFF at the same time, the outputs are turned OFF.
The outputs also turn OFF when emergency pushbutton S1 is pressed.

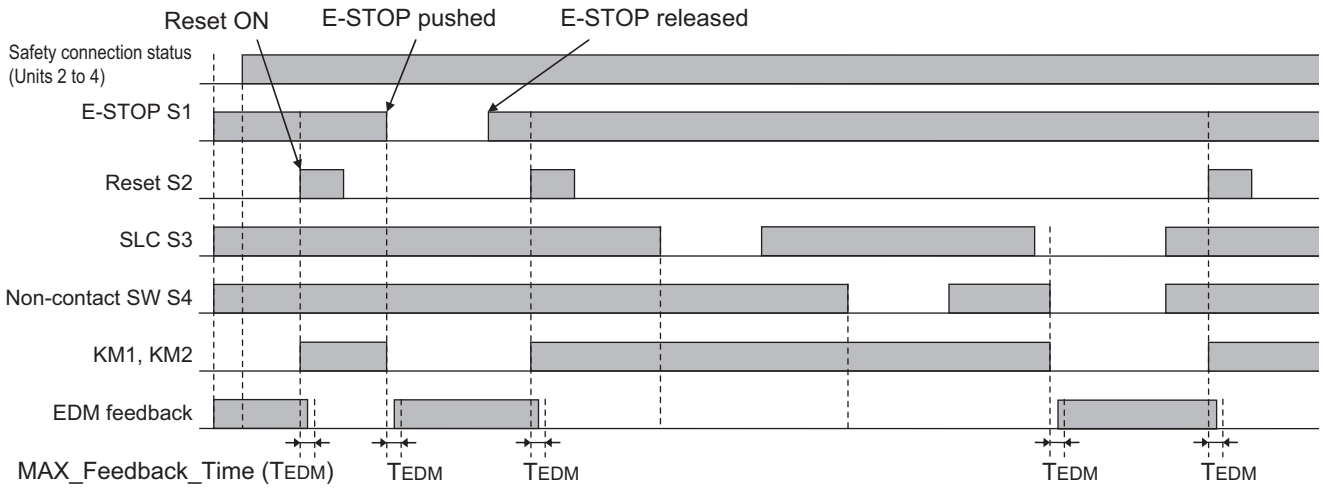
Wiring





S1: Emergency stop pushbutton
S2: Reset switch
S3: Safety light curtain
S4: D40A-2D□ or D40Z Non-contact door switch
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Semiconductor Output for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	Not Used	Safety Light Curtain
	Si 1	500ms	0ms	0ms	Not Used	
Non-contact switch	Si 2	0ms	0ms	0ms	T0	Non-contact Door Switch
	Si 3	0ms	0ms	0ms	T0	

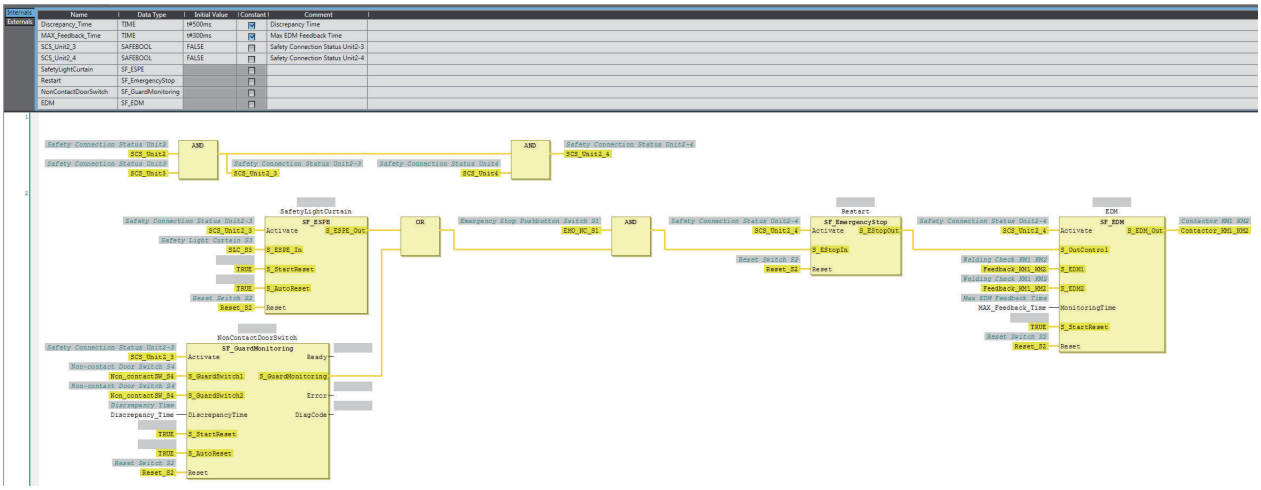
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	SLC_S3	Safety Light Curtain S3	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Non_contactSW_S4	Non-contact Door Switch S4	Global Variables
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	NX-SOD400					
	Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

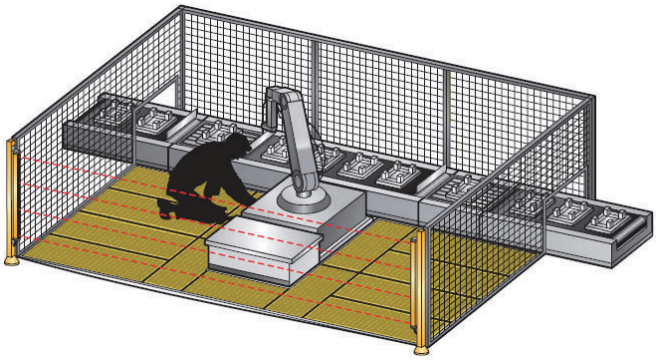
- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

A-4-9 Safety Mats and Safety Light Curtains

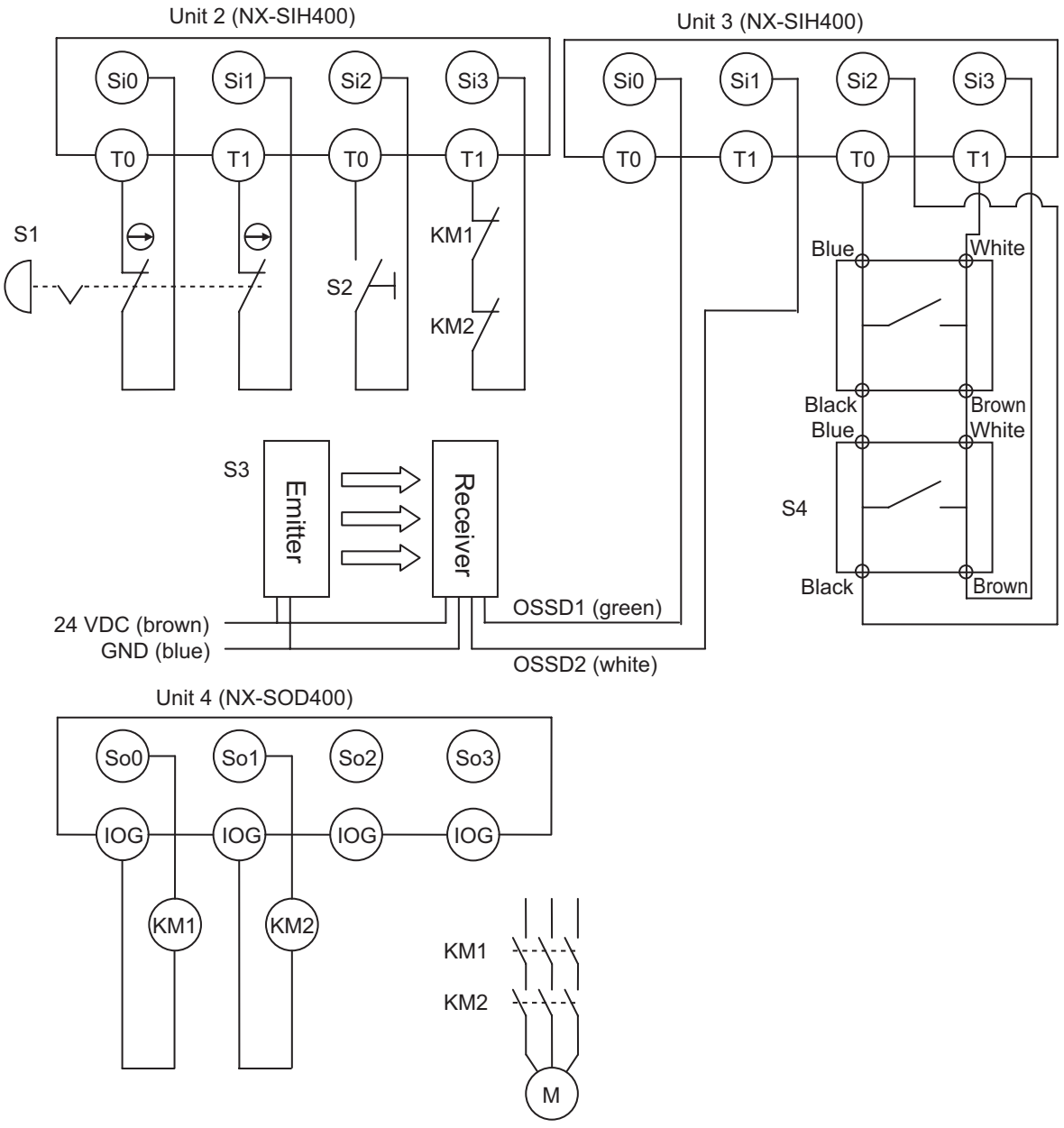
Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 3/PLd (Safety Mat)	• Emergency stop pushbutton • Safety light curtain • Safety mat	0	Manual

Safety light curtain monitors apertural area of safeguarded space and safety mat monitors inside of safeguarded space.
If the light in safety light curtain S3 is interrupted or safety mat S4 detects a person or object, motor M will stop.

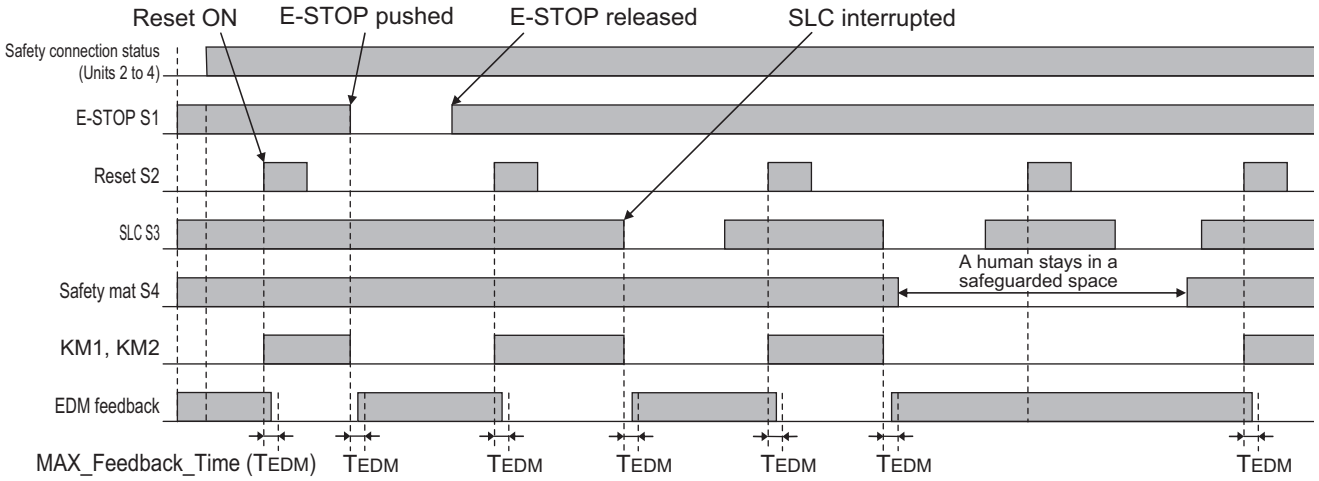


Wiring



S1: Emergency stop pushbutton
S2: Reset switch
S3: Safety light curtain
S4: Safety mat
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Semiconductor Output for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	Not Used	Dual Safety Semiconductor Output(Equivalent)
	Si 1	500ms	0ms	0ms	Not Used	
Safety Mat/Safety Edge	Si 2	0ms	0ms	0ms	T0	Safety Mat
	Si 3	0ms	0ms	0ms	T1	

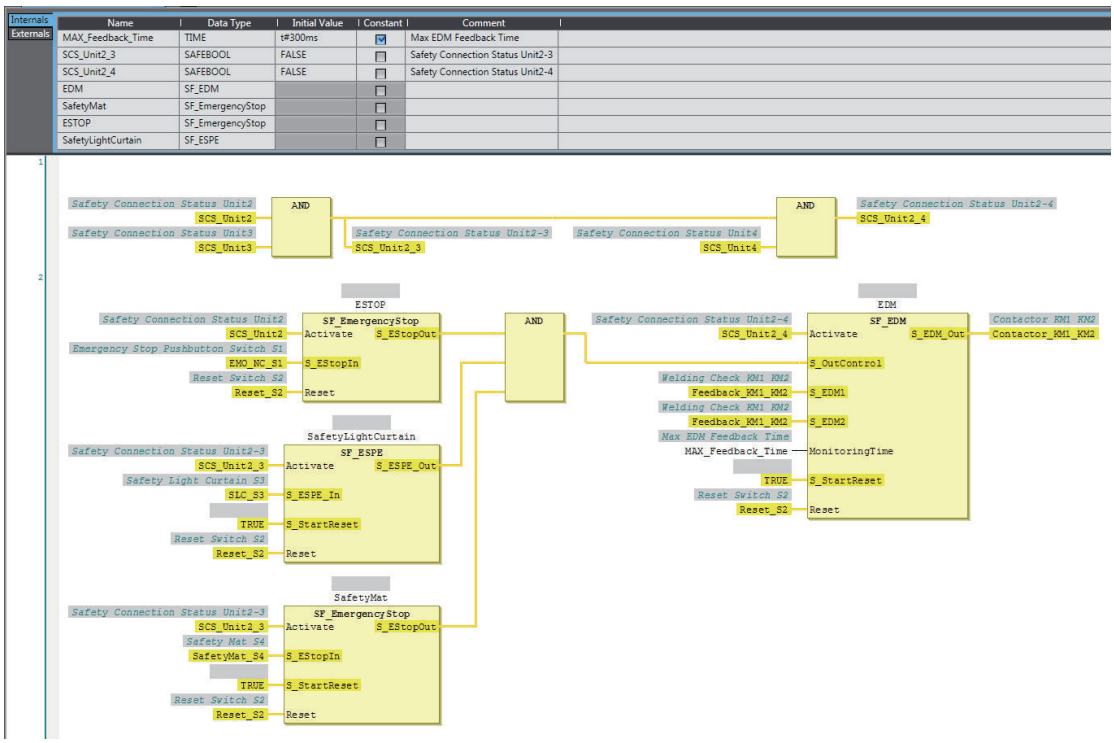
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	SLC_S3	Safety Light Curtain S3	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	SafetyMat_S4	Safety Mat S4	Global Variables
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

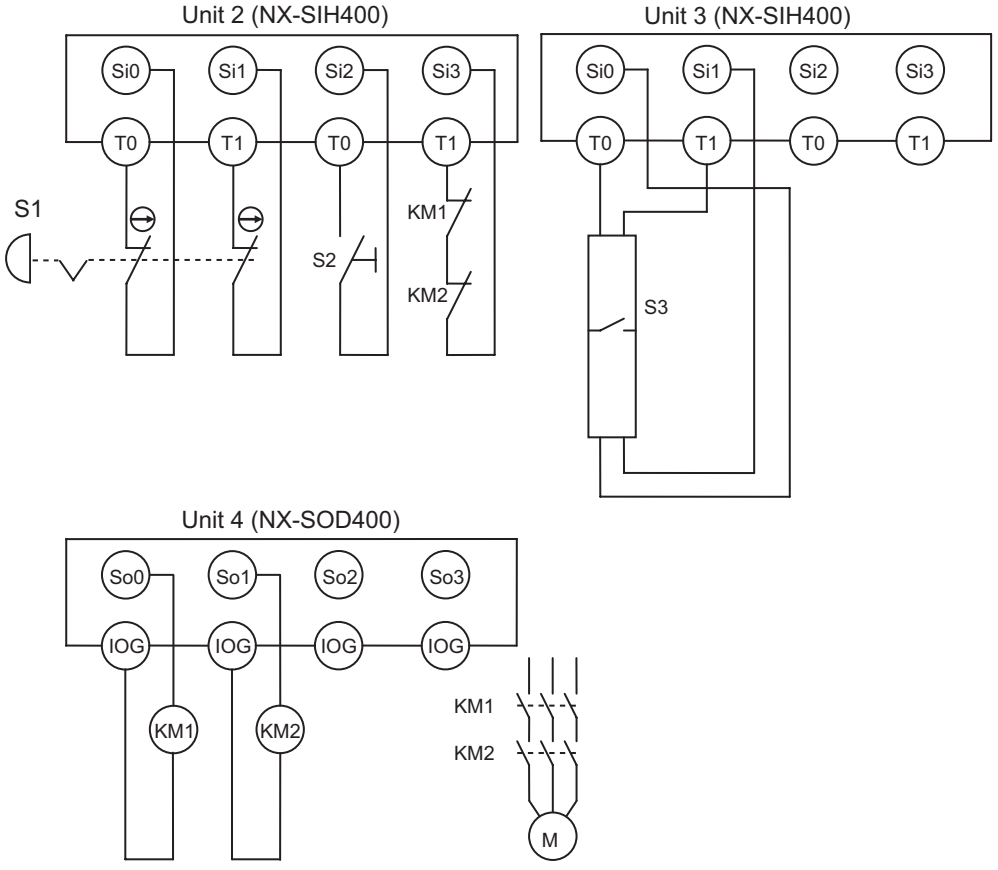
A-4-10 Safety Edges

Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 3/PLd (Safety Edge)	• Emergency stop pushbutton • Safety edge (2-wire cable on both sides)	0	Manual

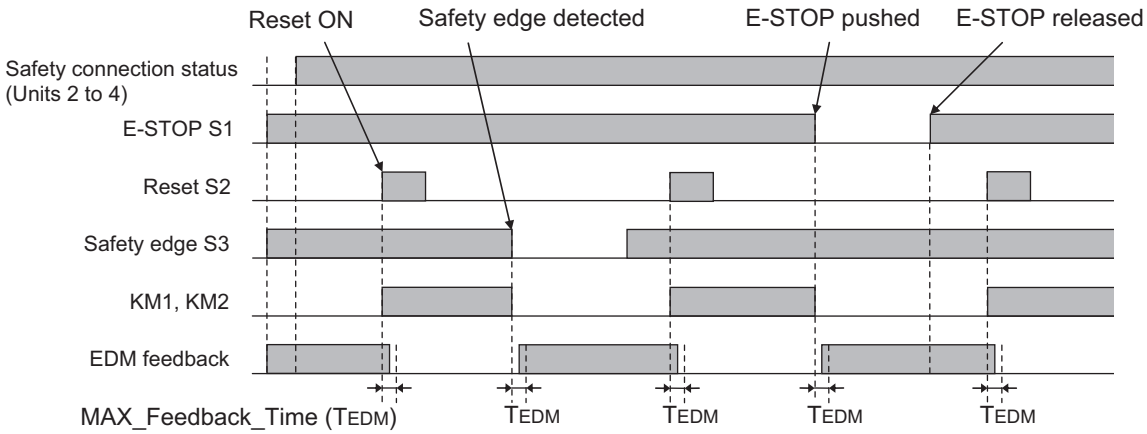
Motor M stops when emergency stop pushbutton S1 is pressed or when edge sensor detects a contact with persons or objects.

Wiring



S1: Emergency stop pushbutton
S2: Reset switch
S3: Safety edge
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Safety Mat/Safety Edge	Si 0	0ms	0ms	0ms	T0	Safety Edge
	Si 1	0ms	0ms	0ms	T1	
	Si 2					
	Si 3					

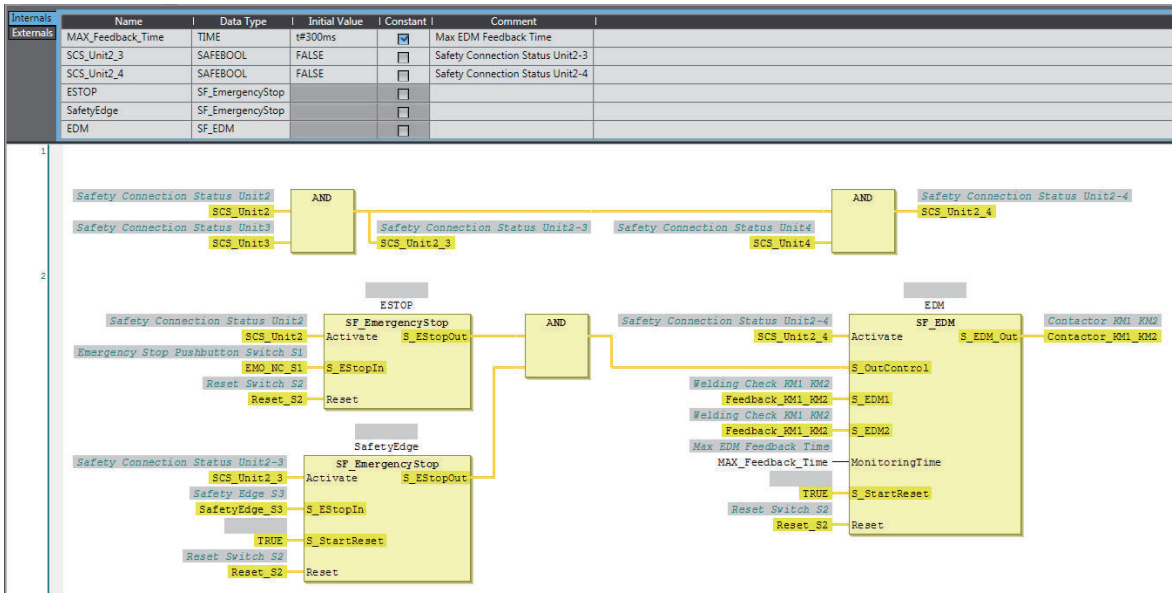
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	NX-SIH400					
	Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	NX-SOD400					
	Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

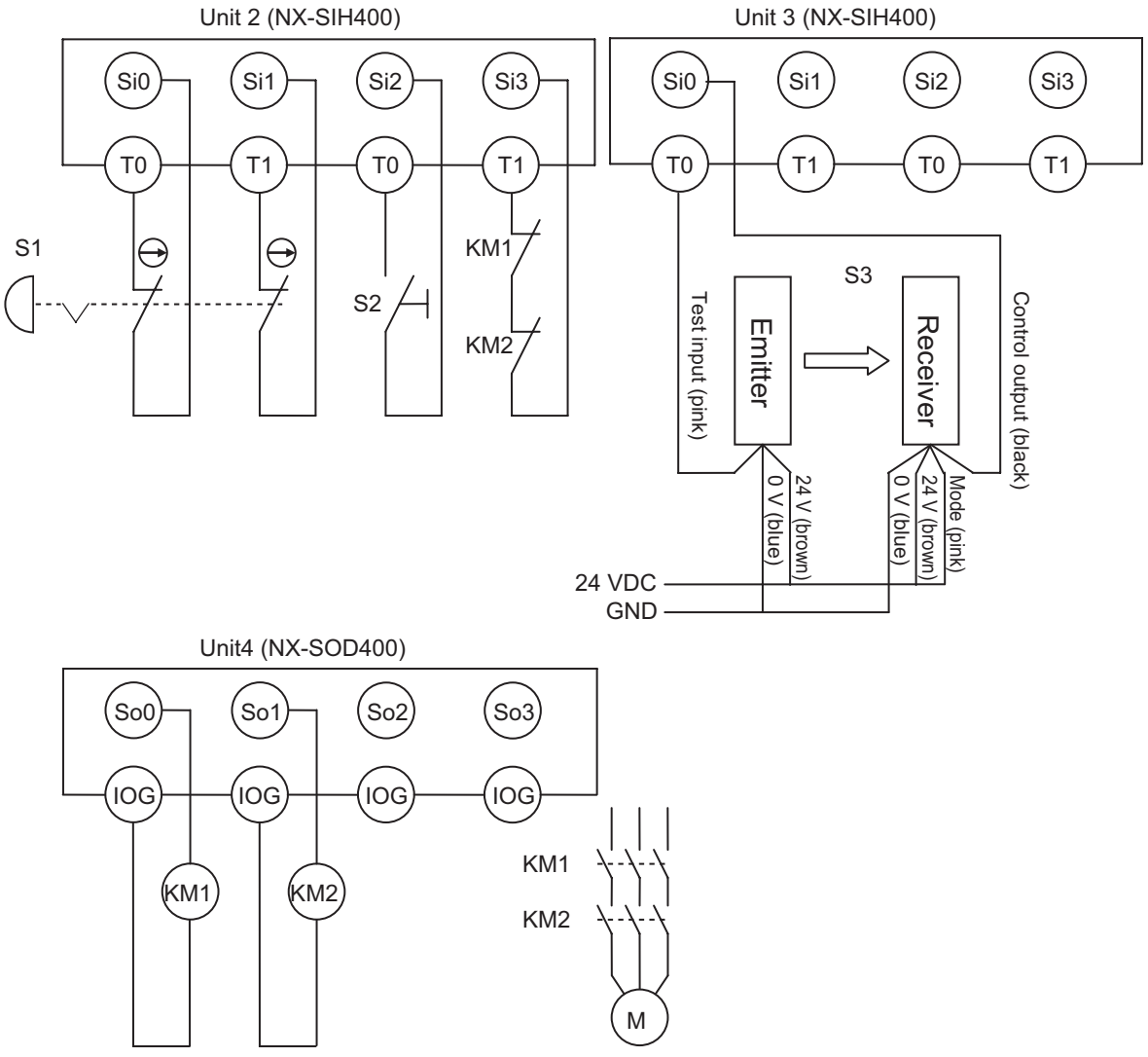
A-4-11 Single Beam Safety Sensor

Application Overview

Safety category/PL	Safety device	Stop category	Reset
Equivalent to 2/PLc (Single Beam Safety Sensor)	• Emergency stop pushbutton • Single beam safety sensor	0	Manual

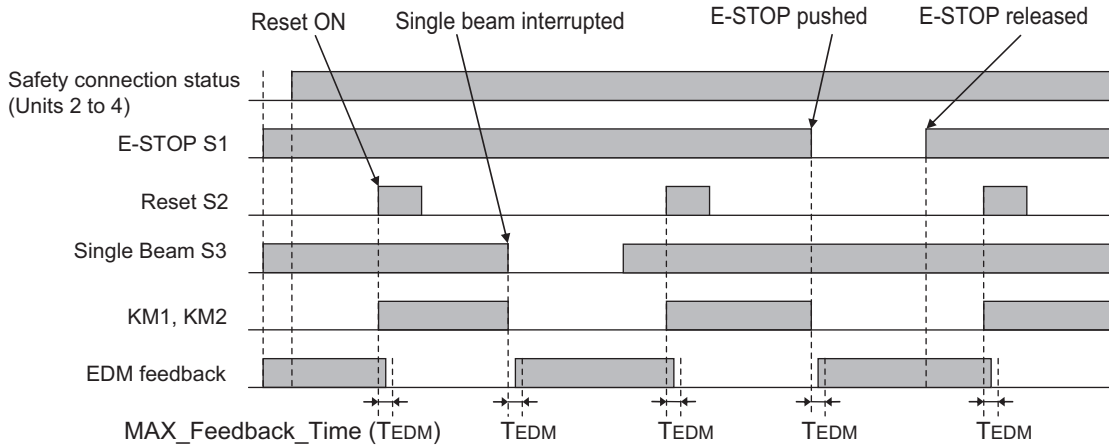
Motor M stops when emergency stop pushbutton S1 is pressed.
Motor M stops when the light in the single beam safety sensor is interrupted.

Wiring



S1: Emergency stop pushbutton
S2: Reset switch
S3: Single beam safety sensor
KM1, KM2: Contactors
M: Motor

Timing Chart



Safety I/O Terminal & I/O Map Setting

● Safety I/O Terminal Settings

Node1/Unit2 : NX-SIH400 (N2 : Instance0)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Mechanical Contact for Dual Channel Equivalent	Si 0	500ms	0ms	0ms	T0	Emergency Stop Pushbutton Switch(2NC)
	Si 1	500ms	0ms	0ms	T1	
Mechanical Contact For Single Channel	Si 2	0ms	0ms	0ms	T0	Reset Switch
Mechanical Contact For Single Channel	Si 3	0ms	0ms	0ms	T1	EDM(Contact Welding Detection)

Node1/Unit3 : NX-SIH400 (N3 : Instance1)

External Device	Channel	Discrepancy	On-Off	Off-On	Test Source	Comment
Single Beam Safety Sensor	Si 0	0ms	0ms	0ms	T0	Single Beam Safety Sensor
	Si 1					
	Si 2					
	Si 3					

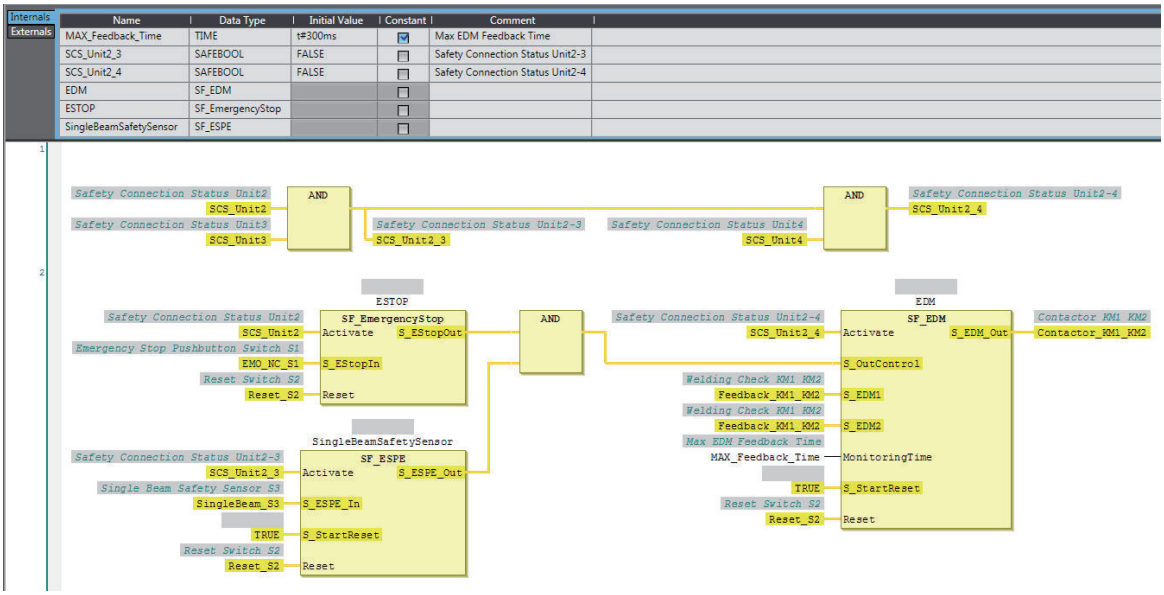
Node1/Unit4 : NX-SOD400 (N4 : Instance2)

External Device	Channel	Comment
Dual Output with Test Pulse	So 0	2 Safety Relays w/ Welding Check
	So 1	
	So 2	
	So 3	

● I/O Map Settings

Position	Port	R/W	Data Type	Variable	Variable Comment	Variable Type
	▼ EtherCAT Network					
EtherCAT Master	Master					
Node1/Unit2	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	EMO_NC_S1	Emergency Stop Pushbutton Switch S1	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL	Reset_S2	Reset Switch S2	Global Variables
	Si03 Logical Value	R	SAFEBOOL	Feedback_KM1_KM2	Welding Check KM1_KM2	Global Variables
	Safety Connection Status	R	SAFEBOOL	SCS_Unit2	Safety Connection Status Unit2	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit3	▼ NX-SIH400					
	▼ Safety Inputs and Status					
	Si00 Logical Value	R	SAFEBOOL	SingleBeam_S3	Single Beam Safety Sensor S3	Global Variables
	Si01 Logical Value	R	SAFEBOOL			
	Si02 Logical Value	R	SAFEBOOL			
	Si03 Logical Value	R	SAFEBOOL			
	Safety Connection Status	R	SAFEBOOL	SCS_Unit3	Safety Connection Status Unit3	Global Variables
	Safety Input Terminal Status	R	SAFEBOOL			
Node1/Unit4	▼ NX-SOD400					
	▼ Status					
	Safety Connection Status	R	SAFEBOOL	SCS_Unit4	Safety Connection Status Unit4	Global Variables
	Safety Output Terminal Status	R	SAFEBOOL			
	▼ Safety Outputs					
	So00 Output Value	W	SAFEBOOL	Contactor_KM1_KM2	Contactor KM1_KM2	Global Variables
	So01 Output Value	W	SAFEBOOL			
	So02 Output Value	W	SAFEBOOL			
	So03 Output Value	W	SAFEBOOL			

Program



Precautions for Safe Use

- Test the functionality every six months to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

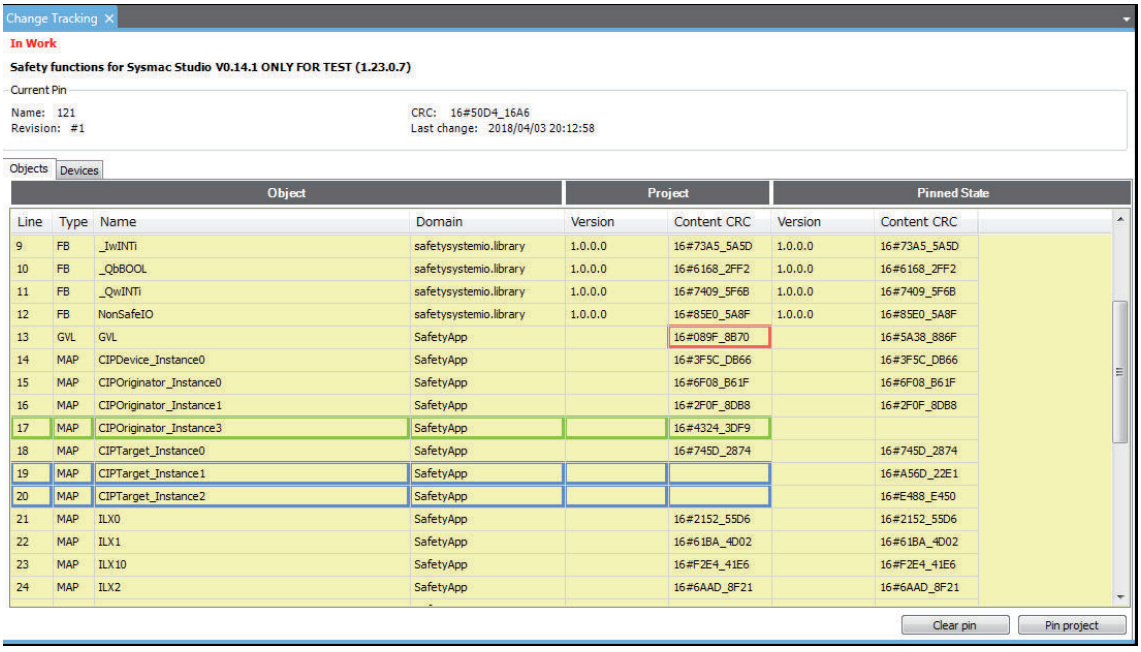
A-5 Change Tracking

What is Change Tracking?

Change Tracking is used to display and manage changes in the safety application data after the pin is created.
Tracking information is property information in safety application data. The storage of the safety application data settings at a given point in time is referred to as "creating a pin".
It is primarily used for version management after the safety application data is debugged.

Change Tracking Procedure and Contents

1 From the Safety CPU Unit Setup and Programming View, select **Change Tracking** from the **Project** Menu.
The **Change Tracking** Tab Page is displayed.



The outer frames of the cells for each item are displayed in the following colors if a pin has not been created or a change was made after it was created.

Color	Description
Green	• The pin has not been created yet. • Items were added after the pin was created.
Red	• Changes were made after the pin was created.
Blue	• The pin was deleted after it was created.

● Description of Type

The type of configuration data is displayed in the **Type** column.

Objects tab

Type Name	Description
APP	Safety Application
TASK	Safety Task
PRG	Programs
FB	Function Blocks
GVL	Global Variables
MAP	I/O Map and exposed variables
CNF	Safety process data communications

Devices tab

Type Name	Description
SAFEPLC	Safety CPU Unit
SAFEDEV	Safety I/O Unit
XVARDEF	Exposed variables

Pin Operations

This section describes the procedures to create and delete pins, and the jump function.

● Creating Pins

When you click the **Pin project** Button, a dialog box to enter the current status name is displayed. The name that you set is shown as the pin information in the upper part of the **Change Tracking** Tab Page.

If the data changes from the data that is in effect at this point, the contents of the change are displayed in the tab page.

● Deleting a Pin

When you click the **Clear Pin** Button, the status that you created with the **Pin project** Button is deleted.

● Jump Function

When you double-click information on the **Change Tracking** Tab Page, the global variable table, FBD editor, or other corresponding tab page is displayed.

A-6 Safety CPU Unit Status

The Safety CPU Unit status gives the operating status of the Safety CPU Unit. When a Safety CPU Unit is placed on the NX bus of the Communication Control Unit, the status is displayed as an I/O port in the I/O Map of the Communication Control Unit.
If you set a device variable for the I/O port and allocate it to a tag set, you can monitor the status of the Safety CPU Unit from the standard controller.

I/O port		Description	Conditions	R/W	Data type
Safety CPU Status		Status monitoring data for the Safety CPU Unit	This is a UNIT variable that contains the following status.	R	UINT
D00	Normal Operating	Safety programs operating with no errors. All safety master connections established.	This variable is TRUE when all of the following conditions are met. If even one condition is not met, it is FALSE. Conditions • The safety programs are in RUN status (RUN mode or DEBUG mode (RUN)). • No event with a level of minor fault or higher currently exists for the safety programs. • All FSoE connections are established. • All CIP Safety Originator connections are established. • No error is present in the CIP Safety Target connections.	R	BOOL
D01	Program Operating	Safety programs operating	This variable is TRUE when the following condition is met. If the condition is not met, it is FALSE. Condition • The safety programs are in RUN status (RUN mode or DEBUG mode (RUN)).	R	BOOL
D02	Program No Fault	No event with a level of minor fault or higher currently exists for the safety programs.	This variable is TRUE when the following condition is met. If the condition is not met, it is FALSE. Condition • No event with a level of minor fault or higher currently exists for the safety programs.	R	BOOL
D03	Safety Master Connection Status	All safety master connections established.	This variable is TRUE when all of the following conditions are met. If even one condition is not met, it is FALSE. Conditions • All FSoE connections are established. • All CIP Safety Originator connections are established.	R	BOOL
D04	FSoE Master Connection Status	All FSoE safety master connections established.	This variable is TRUE when the following condition is met. If the condition is not met, it is FALSE. Condition • All FSoE connections are established.	R	BOOL
D05	CIP Safety Originator Connection Status	All CIP Safety Originator connections established.	This variable is TRUE when the following condition is met. If the condition is not met, it is FALSE. Condition • All CIP Safety Originator connections are established.	R	BOOL

I/O port		Description	Conditions	R/W	Data type
D06	CIP Safety Target Connection Status	No error in entire CIP Safety Target connections	This variable is TRUE when the following condition is met. If the condition is not met, it is FALSE. Condition • No error is present in the entire CIP Safety Target connections.	R	BOOL

A-7 I/O Ports of Safety I/O Units

The I/O ports of the Safety I/O Units are displayed on the I/O Map of the Communication Control Unit if you place the Safety I/O Units on the Communication Control Unit.
The names of the I/O ports that correspond to the data in the I/O Map of the Safety CPU Unit are given in the "Corresponding port name" Column. "Same" means that the same name is used.

A-7-1 NX-SIH400 Safety Input Unit

Port	Data type	R/W	Name	Description	Default	Corresponding port name
Standard Input 1st Byte	BYTE	R	Standard Input 1st Byte	---	00 hex	---
Si00 Logical Value	BOOL	R	Si00 Logical Value	Gives the status of safety input terminal Si00. 0: OFF, 1: ON	0	Same
Si01 Logical Value	BOOL	R	Si01 Logical Value	Gives the status of safety input terminal Si01. 0: OFF, 1: ON	0	Same
Si02 Logical Value	BOOL	R	Si02 Logical Value	Gives the status of safety input terminal Si02. 0: OFF, 1: ON	0	Same
Si03 Logical Value	BOOL	R	Si03 Logical Value	Gives the status of safety input terminal Si03. 0: OFF, 1: ON	0	Same
Safety Connection Status	BOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0	Same
Safety Input Terminal Status	BOOL	R	Safety Input Terminal Status	This flag indicates the status of the safety input terminals. 0: An error has occurred on one of the safety input terminals. 1: All of the safety input terminals are normal (no errors).	0	Same
Unit Normal Status	BOOL	R	Unit Normal Status	This flag indicates the status of the Unit. 0: An error has occurred. 1: Normal (no errors)	0	---
IO Power Supply Error Flag	BOOL	R	IO Power Supply Error Flag	This flag indicates the status of the I/O power supply voltage. 0: The I/O power supply voltage is normal. 1: The I/O power supply voltage is incorrect or the I/O power supply is OFF.	0	---
Standard Input 2nd Byte	BYTE	R	Standard Input 2nd Byte	---	00 hex	---

Port	Data type	R/W	Name	Description	Default	Corresponding port name
Si00 Status	BOOL	R	Si00 Status	Gives the status of safety input terminal 00. 0: Error 1: No error	0	---
Si01 Status	BOOL	R	Si01 Status	Gives the status of safety input terminal 01. 0: Error 1: No error	0	---
Si02 Status	BOOL	R	Si02 Status	Gives the status of safety input terminal 02. 0: Error 1: No error	0	---
Si03 Status	BOOL	R	Si03 Status	Gives the status of safety input terminal 03. 0: Error 1: No error	0	---

A-7-2 NX-SID800 Safety Input Unit

Port	Data type	R/W	Name	Description	Default	Corresponding port name
Standard Input 1st Word	WORD	R	Standard Input 1st Word	---	0000 hex	---
Si00 Logical Value	BOOL	R	Si00 Logical Value	Gives the status of safety input terminal Si00. 0: OFF, 1: ON	0	Same
Si01 Logical Value	BOOL	R	Si01 Logical Value	Gives the status of safety input terminal Si01. 0: OFF, 1: ON	0	Same
Si02 Logical Value	BOOL	R	Si02 Logical Value	Gives the status of safety input terminal Si02. 0: OFF, 1: ON	0	Same
Si03 Logical Value	BOOL	R	Si03 Logical Value	Gives the status of safety input terminal Si03. 0: OFF, 1: ON	0	Same
Si04 Logical Value	BOOL	R	Si04 Logical Value	Gives the status of safety input terminal Si04. 0: OFF, 1: ON	0	Same
Si05 Logical Value	BOOL	R	Si05 Logical Value	Gives the status of safety input terminal Si05. 0: OFF, 1: ON	0	Same
Si06 Logical Value	BOOL	R	Si06 Logical Value	Gives the status of safety input terminal Si06. 0: OFF, 1: ON	0	Same
Si07 Logical Value	BOOL	R	Si07 Logical Value	Gives the status of safety input terminal Si07. 0: OFF, 1: ON	0	Same
Safety Connection Status	BOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0	Same
Safety Input Terminal Status	BOOL	R	Safety Input Terminal Status	This flag indicates the status of the safety input terminals. 0: An error has occurred on one of the safety input terminals. 1: All of the safety input terminals are normal (no errors).	0	Same
Unit Normal Status	BOOL	R	Unit Normal Status	This flag indicates the status of the Unit. 0: An error has occurred. 1: Normal (no errors)	0	---

Port	Data type	R/W	Name	Description	Default	Corresponding port name
IO Power Supply Error Flag	BOOL	R	IO Power Supply Error Flag	This flag indicates the status of the I/O power supply voltage. 0: The I/O power supply voltage is normal. 1: The I/O power supply voltage is incorrect or the I/O power supply is OFF.	0	---
Standard Input 2nd Byte	BYTE	R	Standard Input 2nd Byte	---	00 hex	---
Si00 Status	BOOL	R	Si00 Status	Gives the status of safety input terminal 00. 0: Error 1: No error	0	---
Si01 Status	BOOL	R	Si01 Status	Gives the status of safety input terminal 01. 0: Error 1: No error	0	---
Si02 Status	BOOL	R	Si02 Status	Gives the status of safety input terminal 02. 0: Error 1: No error	0	---
Si03 Status	BOOL	R	Si03 Status	Gives the status of safety input terminal 03. 0: Error 1: No error	0	---
Si04 Status	BOOL	R	Si04 Status	Gives the status of safety input terminal 04. 0: Error 1: No error	0	---
Si05 Status	BOOL	R	Si05 Status	Gives the status of safety input terminal 05. 0: Error 1: No error	0	---
Si06 Status	BOOL	R	Si06 Status	Gives the status of safety input terminal 06. 0: Error 1: No error	0	---
Si07 Status	BOOL	R	Si07 Status	Gives the status of safety input terminal 07. 0: Error 1: No error	0	---

A-7-3 NX-SOH200 Safety Output Unit

Port	Data type	R/W	Name	Description	Default	Corresponding port name
Standard Input 1st Byte	BYTE	R	Standard Input 1st Byte	---	00 hex	---

Port	Data type	R/W	Name	Description	Default	Corresponding port name
So00 Monitor Value	BOOL	R	So00 Monitor Value	Gives the status of safety output terminal So00. 0: OFF, 1: ON	0	So00 Output Value
So01 Monitor Value	BOOL	R	So01 Monitor Value	Gives the status of safety output terminal So01. 0: OFF, 1: ON	0	So01 Output Value
Safety Connection Status	BOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0	Same
Safety Output Terminal Status	BOOL	R	Safety Output Terminal Status	This flag indicates the status of the safety output terminals. 0: An error has occurred on one of the safety output terminals. 1: All of the safety output terminals are normal (no errors).	0	Same
Unit Normal Status	BOOL	R	Unit Normal Status	This flag indicates the status of the Unit. 0: An error has occurred. 1: Normal (no errors)	0	---
IO Power Supply Error Flag	BOOL	R	IO Power Supply Error Flag	This flag indicates the status of the I/O power supply voltage. 0: The I/O power supply voltage is normal. 1: The I/O power supply voltage is incorrect or the I/O power supply is OFF.	0	---
Standard Input 2nd Byte	BYTE	R	Standard Input 2nd Byte	---	00 hex	---
So00 Status	BOOL	R	So00 Status	Gives the status of safety output terminal 00. 0: Error 1: No error	0	---
So01 Status	BOOL	R	So01 Status	Gives the status of safety output terminal 01. 0: Error 1: No error	0	---

A-7-4 NX-SOD400 Safety Output Unit

Port	Data type	R/W	Name	Description	Default	Corresponding port name
Standard Input 1st Byte	BYTE	R	Standard Input 1st Byte	---	00 hex	---

Port	Data type	R/W	Name	Description	Default	Corresponding port name
So00 Monitor Value	BOOL	R	So00 Monitor Value	Gives the status of safety output terminal So00. 0: OFF, 1: ON	0	So00 Output Value
So01 Monitor Value	BOOL	R	So01 Monitor Value	Gives the status of safety output terminal So01. 0: OFF, 1: ON	0	So01 Output Value
So02 Monitor Value	BOOL	R	So02 Monitor Value	Gives the status of safety output terminal So02. 0: OFF, 1: ON	0	So02 Output Value
So03 Monitor Value	BOOL	R	So03 Monitor Value	Gives the status of safety output terminal So03. 0: OFF, 1: ON	0	So03 Output Value
Safety Connection Status	BOOL	R	Safety Connection Status	This flag indicates when a safety connection is active. Use it for an input to the Activate terminal on a safety FB or for safety connection/disconnection applications.	0	Same
Safety Output Terminal Status	BOOL	R	Safety Output Terminal Status	This flag indicates the status of the safety output terminals. 0: An error has occurred on one of the safety output terminals. 1: All of the safety output terminals are normal (no errors).	0	Same
Unit Normal Status	BOOL	R	Unit Normal Status	This flag indicates the status of the Unit. 0: An error has occurred. 1: Normal (no errors)	0	---
IO Power Supply Error Flag	BOOL	R	IO Power Supply Error Flag	This flag indicates the status of the I/O power supply voltage. 0: The I/O power supply voltage is normal. 1: The I/O power supply voltage is incorrect or the I/O power supply is OFF.	0	---
Standard Input 2nd Byte	BYTE	R	Standard Input 2nd Byte	---	00 hex	---
So00 Status	BOOL	R	So00 Status	Gives the status of safety output terminal 00. 0: Error 1: No error	0	---
So01 Status	BOOL	R	So01 Status	Gives the status of safety output terminal 01. 0: Error 1: No error	0	---
So02 Status	BOOL	R	So02 Status	Gives the status of safety output terminal 02. 0: Error 1: No error	0	---

Port	Data type	R/W	Name	Description	Default	Corresponding port name
So03 Status	BOOL	R	So03 Status	Gives the status of safety output terminal 03. 0: Error 1: No error	0	---

A-8 CIP Response Codes

This section provides information on the response codes that are defined in the CIP specifications. They are stored in the received data of CIP messages that are sent to the Communication Control Unit or Safety CPU Unit. In case of the CIP Safety or tag data link not established error, an extended code supplementing the event information may be registered.

A-8-1 General Status Codes

General Status Code (hex)	Status Name	Description of Status
00	Success	Service was successfully performed by the object specified.
01	Connection failure	A connection related to service failed along the connection path.
02	Resource unavailable	Resources needed for the object to perform the requested service were unavailable.
03	Invalid parameter value	See Status Code 20 hex.
04	Path segment error	The path segment identifier or the segment syntax was not understood by the processing node. Path processing stops when a path segment error occurs.
05	Path destination unknown	The path is referencing an object class, instance, or structure element that is not known or is not contained in the processing node. Path processing stops when a Path Destination Unknown Error occurs.
06	Partial transfer	Only part of the expected data was transferred.
07	Connection lost	The message connection was lost.
08	Service not supported	The requested service was not supported or was not defined for this object class/instance.
09	Invalid attribute value	Invalid attribute data was detected.
0 A	Attribute list error	An attribute in the Get_Attribute_List or Set_Attribute_List response has a non-zero status.
0B	Already in requested mode/state	The object is already in the mode/state being requested by the service.
0C	Object state conflict	The object cannot perform the requested service in its current mode/state.
0D	Object already exists	The requested instance of object to be created already exists.
0E	Attribute not settable	A request to modify a non-modifiable attribute was received.
0F	Privilege violation	A permission/privilege check failed.
10	Device state conflict	The device’s current mode/state prohibits the execution of the requested service.
11	Reply data too large	The data to be transmitted in the response buffer is larger than the allocated response buffer.
12	Fragmentation of a primitive value	The service specified an operation that is going to fragment a primitive data value, i.e. half a REAL data type.
13	Not enough data	The requested service did not supply enough data to perform the specified operation.
14	Attribute not supported	The attribute specified in the request is not supported.
15	Too much data	The service supplied more data than was expected.

General Status Code (hex)	Status Name	Description of Status
16	Object does not exist	An object that does not exist was specified for the requested service.
17	Service fragmentation sequence not in progress	The fragmentation sequence for this service is not currently active for this data.
18	No stored attribute data	The attribute data of this object was not saved prior to the requested service.
19	Store operation failure	The attribute data of this object was not saved due to a failure during the attempt.
1A	Routing failure (request packet too large)	The service request packet was too large for transmission on a network in the path to the destination. The routing device was forced to abort the service.
1B	Routing failure (response packet too large)	The service response packet was too large for transmission on a network in the path from the destination. The routing device was forced to abort the service.
1C	Missing attribute list entry data	The service did not supply an attribute in a list of attributes that was needed by the service to perform the requested behavior.
1D	Invalid attribute value list	The service is returning the list of attributes supplied with status information for those attributes that were invalid.
1E	Embedded service error	An embedded service resulted in an error.
1F	Vendor specific error	A vendor-specific error occurred. The Additional Code Field of the error response defines the error. This is a general error code that is used only for errors that do not correspond to any of the error codes in this table and are not in an object class definition.
20	Invalid parameter	A parameter for the requested service is invalid. This code is used when a parameter does not meet the requirements of the specification and/or the requirements defined in an application object specification.
21	Write-once value or medium already written	An attempt was made to write to a write-once medium (e.g. WORM drive or PROM) that was previously written or cannot be changed.
22	Invalid Reply Received	An invalid reply was received. (For example, the reply service code does not match the request service code, or the reply message is shorter than the minimum expected reply size.) This status code is used for other causes of invalid replies.
23	Buffer Overflow	The message received is larger than the receiving buffer can handle. The entire message was discarded.
24	Message Format Error	The format of the received message is not supported by the server.
25	Key Failure in path	The key segment that was included as the first segment in the path does not match the destination module. The object specific status must indicate which part of the key check failed.
26	Path Size Invalid	The size of the path that was sent with the service request is either too large or too small for the request to be routed to an object.
27	Unexpected attribute in list	An attempt was made to set an attribute that is not able to be set at this time.
28	Invalid Member ID	The member ID specified in the request does not exist in the specified class, instance, and attribute.
29	Member not settable	A request to modify a non-modifiable member was received.
2 A	Group 2 only server general failure	This error code is reported only by group 2 only servers with 4K or less of code space and only in place of Service not supported, Attribute not supported, or Attribute not settable.

General Status Code (hex)	Status Name	Description of Status
2B	Unknown Modbus Error	A CIP to Modbus translator received an unknown Modbus Exception Code.
2C	Attribute not gettable	A request to read a non-readable attribute was received.
2D	Instance Not Deletable	The requested object instance cannot be deleted.
2E	Service Not Supported for Specified Path	The object supports the service, but not for the designated application path (e.g. attribute). NOTE: Not to be used for any set service (use General Status Code 0x0E or 0x29 instead)
2F-CF		Reserved by CIP for future extensions.
D0-FF	Reserved for Object Class and service errors	This range of error codes is to be used to indicate object class-specific errors. This code range is used only when none of the error codes in this table accurately reflect the error that occurred. The additional code field is used to describe the general error code in more detail.

A-8-2 Extended Status Codes

General Status (hex)	Additional Status (hex)	Explanation
01	0100	Connection in use or duplicate forward open.
01	0103	Transport class and trigger combination not supported.
01	0105	Ownership Conflict or OUNID Mismatch. The configuration is already owned by another originator.
01	0106	Ownership Conflict or OUNID Mismatch. The output connection was already owned by another originator.
01	0107	Connection not found at target application.
01	0108	Invalid connection type. There is a problem with either the connection type or priority of the connection.
01	0109	Invalid connection size.
01	0110	Device not configured.
01	0111	RPI not supported. May also indicate problem with connection time-out multiplier, or production inhibit time.
01	0112	RPI VALUE(S) not acceptable
01	0113	Connection Manager cannot support any more connections.
01	0114	Either the vendor ID or the product code in the key segment does not match the device.
01	0115	Device type in the key segment does not match the device.
01	0116	Major or minor revision information in the key segment does not match the device.
01	0117	Invalid connection point.
01	0118	Invalid configuration format.
01	0119	Connection request failed because there is no controlling connection currently open.
01	011A	Target application cannot support any more connections.
01	011B	RPI is smaller than the production inhibit time.
01	011C	Transport Class not supported

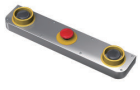
General Status (hex)	Additional Status (hex)	Explanation
01	011D	T->O Production Trigger not supported
01	011E	Direction not supported
01	011F	Invalid originator to target Network Connection Fixvar
01	0120	Invalid target to originator Network Connection Fixvar
01	0121	Invalid originator to target Network Connection Priority
01	0122	Invalid target to originator Network Connection Priority
01	0123	Invalid originator to target Network Connection Type
01	0124	Invalid target to originator Network Connection Type
01	0125	Invalid originator to target Network Connection Redundant_Owner
01	0126	Invalid configuration size
01	0127	Invalid originator to target Network Connection Size
01	0128	Invalid target to originator Network Connection Size
01	0129	Invalid Configuration Application Path
01	012A	Invalid Consuming Application Path
01	012B	Invalid Producing Application Path
01	012C	Configuration Symbol does not exist
01	012D	Consuming Symbol does not exist
01	012E	Producing Symbol does not exist
01	012F	Inconsistent Application Path combination
01	0130	Inconsistent Consume Data Format
01	0131	Inconsistent Produce Data Format
01	0132	Null Forward Open function not supported
01	0133	Connection Timeout Multiplier not acceptable
01	0134	Mismatched T->O Network Connection Size
01	0135	Mismatched T->O Network Connection Fixvar
01	0136	Mismatched T->O Network Connection Priority
01	0137	Mismatched Transport Class
01	0138	Mismatched T->O Production Trigger
01	0139	Mismatched T->O Production Inhibit Time Segment
01	0203	Connection cannot be closed because the connection has timed out.
01	0204	Unconnected_Send service timed out while waiting for a response.
01	0205	Parameter Error in Unconnected Send Service or Parameter Error in SafetyOpen or SafetyClose
01	0206	Message too large for unconnected message service.
01	0207	Unconnected acknowledgement without reply.
01	0301	No buffer memory available.
01	0302	Network bandwidth not available for data.
01	0303	No tag filters available.
01	0304	Not configured to send real-time data.
01	0305	Schedule Signature mismatch
01	0306	Schedule Signature validation not possible
01	0311	Port that was specified in port segment is not available.
01	0312	Link address that was specified in port segment is not available.
01	0315	Invalid segment type or segment value in path.
01	0316	Path and connection were not equal when closing the connection.

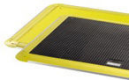
General Status (hex)	Additional Status (hex)	Explanation
01	0317	Either the segment is not present or the encoded value in the network segment is invalid.
01	0318	Link address to self is invalid.
01	0319	Resources on secondary are unavailable.
01	031A	Connection is already established.
01	031B	Direct connection is already established.
01	031C	Others
01	031D	Redundant connection mismatch.
01	031E	There are no more reception resources available on the sending module.
01	031F	No connection resources exist for the target path.
01	0320 - 07FF	Vendor specific.
01	0801	Incompatible Multicast RPI. An existing connection has been established at a different RPI.
01	0802	Invalid Safety Connection Size
01	0803	Invalid Safety Connection Format
01	0804	Invalid Time Correction Connection Parameters
01	0805	Invalid Ping Interval EPI Multiplier
01	0806	Time Coordination Msg Min Multiplier
01	0807	Network Time Expectation Multiplier
01	0808	Timeout Multiplier
01	0809	Invalid Max Consumer Number
01	080A	Invalid CPCRC
01	080B	Time Correction Connection Id Invalid
01	080C	SCID Mismatch. The SCID was non-zero and did not match the value in the target
01	080D	TUNID not set. Device is out-of-box and TUNID has not been set, so connections are not allowed.
01	080E	TUNID Mismatch. The TUNID provided does not match. The message was likely routed to this node in error
01	080F	Configuration operation not allowed
01	0810	No target application data available
01	0811	No originator application data available
01	0812	Node address has changed since the network was scheduled
01	0813	Not configured for off-subnet multicast
01	0814	Invalid Produce/Consume Data Format

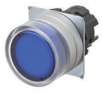
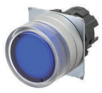
A-9 Icon list for Safety Slave Unit Parameters

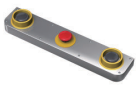
The icons that you can set or change for Safety Slave Unit parameters are listed in the following table.

A-9-1 External Device Icons for Input Devices

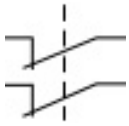
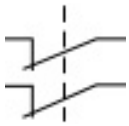
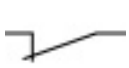
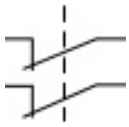
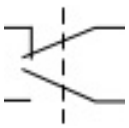
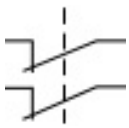
Category	Device	Settable external device icons			
Safety Switch	Emergency stop switch for dual channel equivalent input				
	Emergency stop switch for single channel				
	Safety door switch for dual-channel equivalent input				
	Safety door switch for dual-channel complementary input				
	Safety door switch for single channel				
	Safety limit switch for dual-channel equivalent input				
	Safety limit switch for dual-channel complementary input				
	Safety limit switch for single channel				
	Two-hand switches				

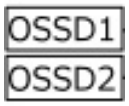
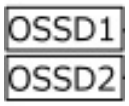
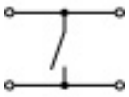
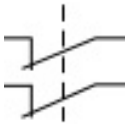
Category	Device	Settable external device icons			
Safety Switch	Safety key selector switch for dual-channel equivalent input				
	Safety key selector switch for dual-channel complementary input				
	Safety key selector switch for single channel				
	Enabling switch				
Safety Sensor	Safety light curtain				
	Safety laser scanner				
	High-Coded Door Switch				
	High-Coded Door Switch (Guard Lock Model)				
	High-Coded Door Switch (For Gate)				
Specialty devices	Non-contact Door Switch				
	Single Beam Safety Sensor				
	Safety Mat/Safety Edge				
EDM Feedback	EDM Feedback	Feedback			

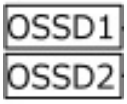
Category	Device	Settable external device icons			
Standard Input Device	Reset switch with test pulse				
	Reset switch without test pulse				

Category	Device	Settable external device icons			
Generic Device	Mechanical Contact for Single Channel				
					
		Feedback			
	Mechanical Contact for Dual Channel Equivalent				
					
					
	Mechanical Contact for Dual Channel Complementary				
					
	Semiconductor Output for Single Channel				
	Semiconductor Output for Dual Channel Equivalent				
					
	Semiconductor Output for Dual Channel Complementary				

A-9-2 Contact Icons for Input Devices

Category	Device	Settable contact icons		
Safety Switch	Emergency stop switch for dual-channel equivalent input	 2NC		
	Emergency stop switch for single channel	 1NC		
	Safety door switch for dual-channel equivalent input	 2NC	 2NO	
	Safety door switch for dual-channel complementary input	 1NC/1NO	 1NO/1NC	
	Safety door switch for single channel	 1NC	 1NO	
	Safety limit switch for dual-channel equivalent input	 2NC	 2NO	
	Safety limit switch for dual-channel complementary input	 1NC/1NO	 1NO/1NC	
	Safety limit switch for single channel	 1NC	 1NO	
	Two-hand switches	 1NO/1NC	 1NC/1NO	
	Safety key selector switch for dual-channel equivalent input	 2NC	 2NO	
	Safety key selector switch for dual-channel complementary input	 1NC/1NO	 1NO/1NC	

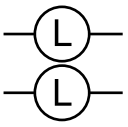
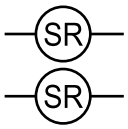
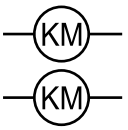
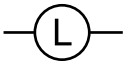
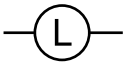
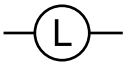
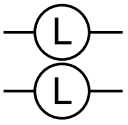
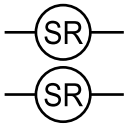
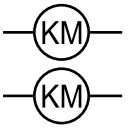
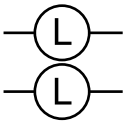
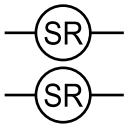
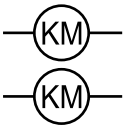
Category	Device	Settable contact icons		
Safety Switch	Safety key selector switch for single channel	 1NC	 1NO	
	Enabling switch	 2NO		
Safety Sensor	Safety light curtain	 OSSD1/OSSD2		
	Safety laser scanner	 OSSD1/OSSD2		
Specialty devices	Non-contact Door Switch			
	Single Beam Safety Sensor	 OSSD1		
	Safety Mat/Safety Edge	 SafetyMat/ SafetyEdge		
EDM Feedback	EDM Feedback	 1NC		
Standard Input Device	Reset switch with test pulse	 1NO	 1NC	
	Reset switch without test pulse	 1NO	 1NC	
Generic Device	Mechanical Contact for Single Channel	 1NC	 1NO	
	Mechanical Contact for Dual Channel Equivalent	 2NC	 2NO	

Category	Device	Settable contact icons		
Generic Device	Mechanical Contact for Dual Channel Complementary	 1NC/1NO	 1NO/1NC	
	Semiconductor Output for Single Channel	 OSSD1		
	Semiconductor Output for Dual Channel Equivalent	 OSSD1/OSSD2		
	Semiconductor Output for Dual Channel Complementary			

A-9-3 External Device Icons for Output Devices

Category	Device	Settable external device icons		
Relays with Forcibly Guided Contacts	Relays with Forcibly Guided Contacts for Dual Channel			
	Relays with Forcibly Guided Contacts for Single Channel			
Generic Device	Single Channel with Test Pulse			
	Single Channel without Test Pulse			
	Dual Output with Test Pulse			
	Dual Output without Test Pulse			

A-9-4 Contact Icons for Output Devices

Category	Device	Settable contact icons		
Relays with Forcibly Guided Contacts	Relays with Forcibly Guided Contacts for Dual Channel	 Load	 Relays with Forcibly Guided Contacts	 Contactor
	Relays with Forcibly Guided Contacts for Single Channel	 Load	 Relays with Forcibly Guided Contacts	 Contactor
Generic Device	Single Channel with Test Pulse	 Load	 Relays with Forcibly Guided Contacts	 Contactor
	Single Channel without Test Pulse	 Load	 Relays with Forcibly Guided Contacts	 Contactor
	Dual Output with Test Pulse	 Load	 Relays with Forcibly Guided Contacts	 Contactor
	Dual Output without Test Pulse	 Load	 Relays with Forcibly Guided Contacts	 Contactor

A-10 Printing

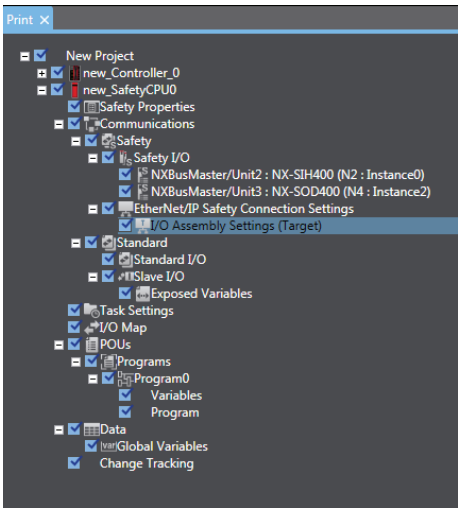
This section describes how to print information related to Safety Control Units from the Sysmac Studio. Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for basic printing procedures for the Sysmac Studio.

A-10-1 Selecting the Items to Print

Use the following procedure to set up printing for a Safety Control Unit.

1 Select **File** - **Print**.
The items that you can print will be displayed.

2 Select the items for the Safety Control Unit.
The Safety Control Unit will be set up for printing.

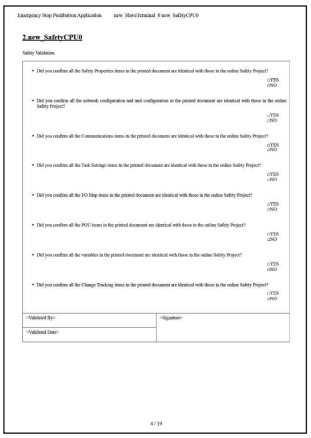


A-10-2 Items that are Printed

The items that you selected for printing are printed in the order in which the printing items were displayed.
Samples of the information that is printed for a Safety Control Unit are provided below.

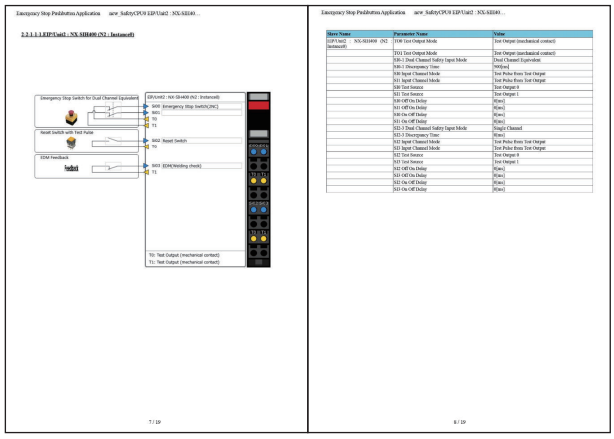
● Signature and Validation Boxes

This information is printed on the first page of the Safety Control Unit information.
Validation and signature boxes for safety validation are printed.



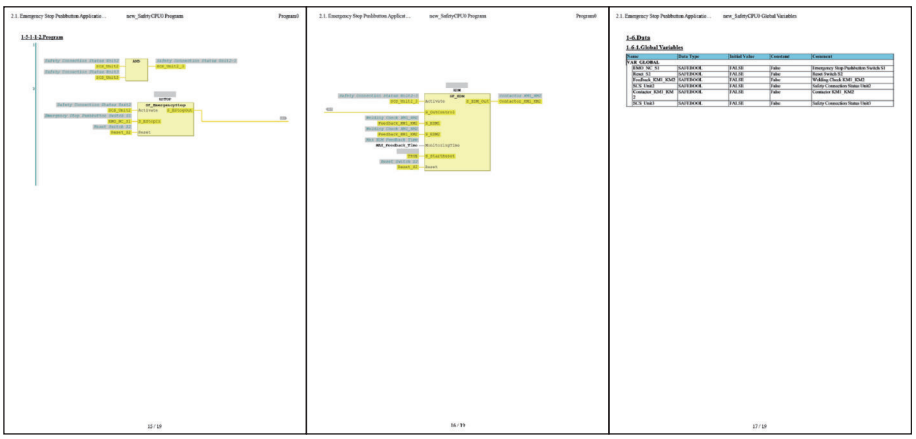
Wiring Diagrams

The wiring diagrams that are set on the Parameters Tab Page are printed.



Program

The programs are printed.

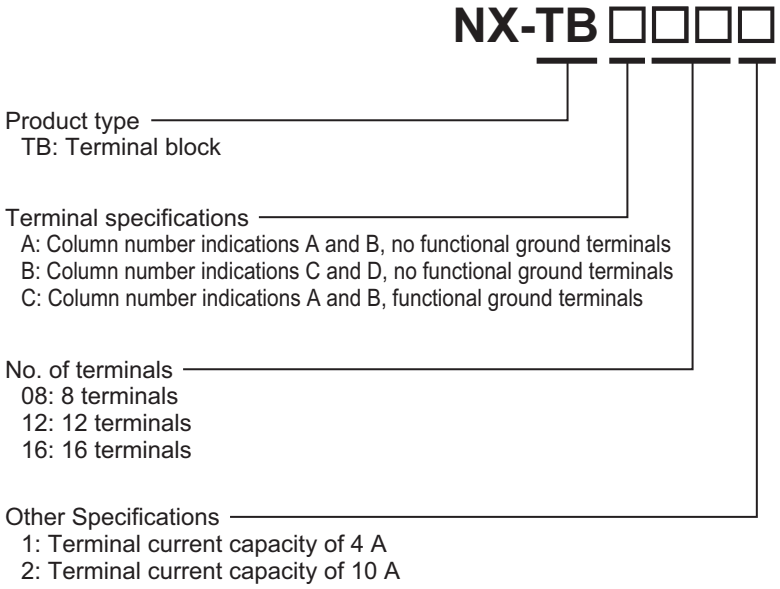


A-11 List of Screwless Clamping Terminal Block Models

This section explains how to read the screwless clamping terminal block model numbers and shows the model number table.

A-11-1 Model Notation

The screwless clamping terminal block models are assigned based on the following rules.



A-11-2 List of Terminal Block Models

The following table shows a list of screwless clamping terminal blocks.

Terminal block model	Number of terminals	Ground terminal mark	Terminal current capacity
NX-TBA081	8	Not provided	4 A
NX-TBA121	12		
NX-TBA161	16		
NX-TBB121	12		
NX-TBB161	16		
NX-TBA082	8		10 A
NX-TBA122	12		
NX-TBA162	16		
NX-TBB082	8		
NX-TBB122	12		
NX-TBB162	16		
NX-TBC082	8	Provided	
NX-TBC162	16		

Note When you purchase a terminal block, purchase an NX-TB□□□2.

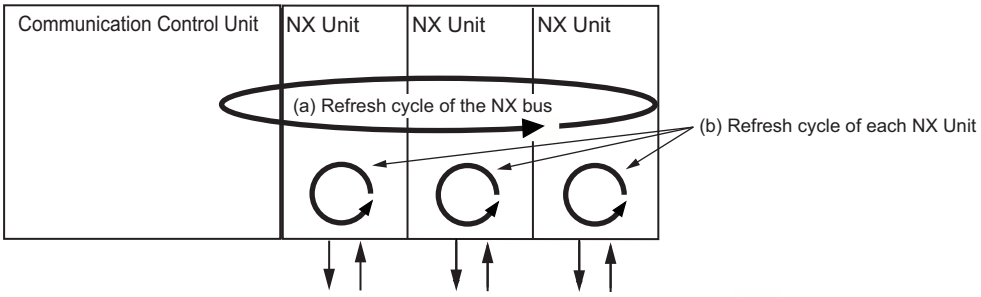
A-12 I/O Refreshing between NX Units

A-12-1 I/O Refreshing from the Communication Control Unit to NX Units

The Communication Control Unit cyclically performs I/O refreshing with the NX Units.

The following two cycles affect operation of the I/O refreshing between the Communication Control Unit and the NX Units.

a. Refresh cycle of the NX bus
b. Refresh cycle of each NX Unit



The refresh cycle of each NX Unit in item (b) depends on the I/O refreshing method which is given below.

A-12-2 Methods of I/O Refreshing between the Communication Control Unit and NX Units

This section describes I/O refreshing methods between Communication Control Unit and NX Unit. Refer to the manuals for each NX Unit for information on the I/O refreshing methods that you can use for the NX Unit.

Types of I/O Refreshing Methods

The I/O refreshing methods that you can use between the Communication Control Unit and the NX Units are shown below.

I/O refreshing method*1	Outline of operation
Free-Run refreshing	With this I/O refreshing method, the refresh cycle of the NX bus and the I/O refresh cycles of the NX Units are asynchronous.
Synchronous I/O refreshing	With this I/O refreshing method, the timing to read inputs or to refresh outputs is synchronized on a fixed interval between more than one NX Unit connected to the Communication Control Unit.

*1. Task period prioritized refreshing and time stamp cannot be used for the Communication Control Unit.

Since the Communication Control Unit can execute all the above I/O refreshing methods at the same time, you can use NX Units with different I/O refreshing methods together.

Setting the I/O Refreshing Methods

For the Communication Control Unit, no setting operation is required, and the method is determined according to the following table.

NX Unit that support only Free-Run refreshing	NX Unit that support both Free-Run refreshing and synchronous I/O refreshing
Free-Run refreshing	Synchronous I/O refreshing

Selecting NX Units

The I/O refreshing methods that you can use depend on the model of the NX Unit. After you decide on which I/O refreshing method to use, select the NX Units.

Free-Run Refreshing

With this I/O refreshing method, the refresh cycle of the NX bus and the I/O refresh cycles of the NX Units are asynchronous.
NX Units read inputs and refresh outputs at the time of I/O refreshing.
This method is used when it is not necessary to be aware of factors such as the I/O timing jitter and the concurrency of the timing to read inputs and refresh outputs between the NX Units.

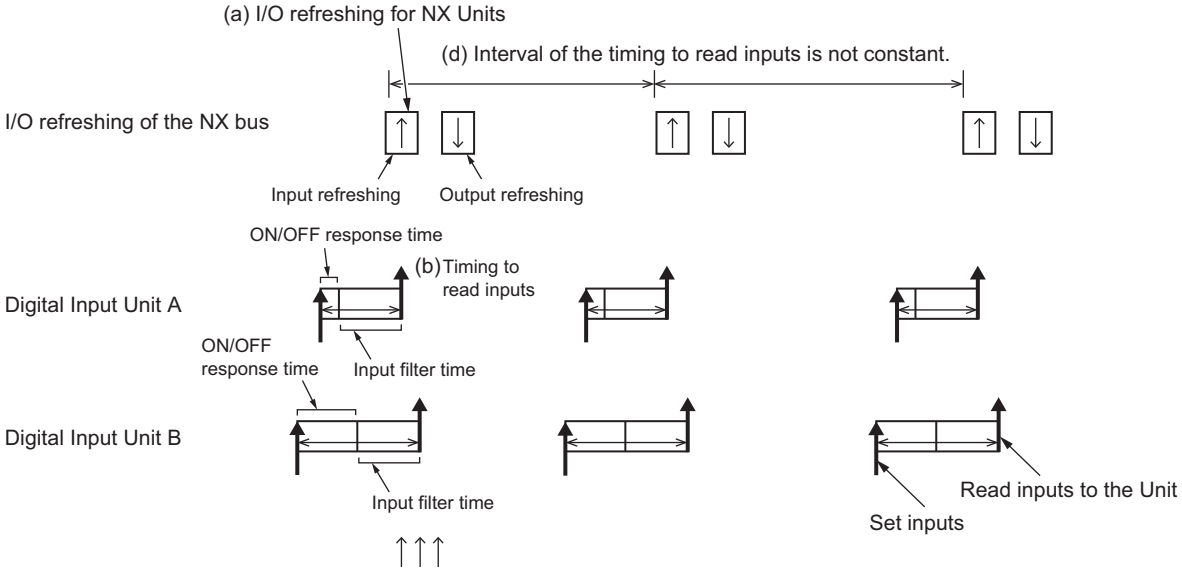
This section explains operations when NX Units are connected to a CPU Unit or Communications Coupler Unit.
Refer to the user's manual for the Communication Control Unit for operations when NX Units are connected to a Communication Control Unit.

● Description of Operation

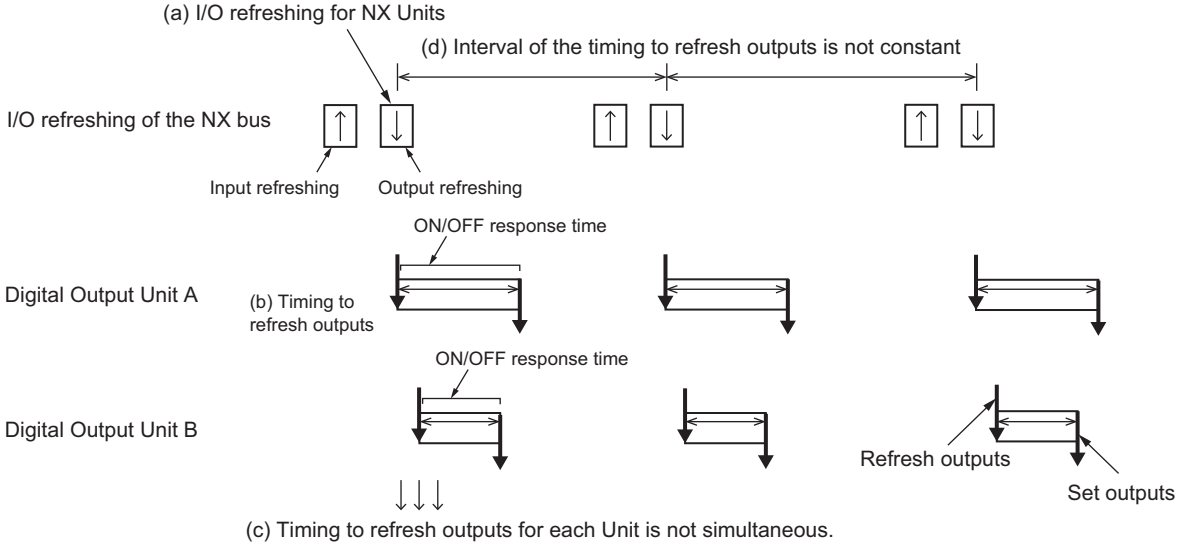
The following describes the operation of Free-Run refreshing between the Communication Control Unit and the NX Units.

- The Communication Control Unit performs I/O refreshing for NX Units. (Refer to (a) in the figure below.)
- The NX Units read inputs or refresh outputs at the time of I/O refreshing. (Refer to (b) in the figure below.)
- The Communication Control Unit can read the most recent input value at the time of I/O refreshing and the NX Units can control the most recent output value at the time of I/O refreshing. However, timing to read inputs or timing to refresh outputs for each NX Unit does not occur at the same time. (Refer to (c) in the figure below.)
- The interval of I/O refreshing varies with the processing conditions of the Communication Control Unit. Therefore, the interval of the timing to read inputs or to refresh outputs for the NX Units is not always the same. (Refer to (d) in the figure below.)
- In order to read input values correctly, you must set the inputs before the total of the ON/OFF response time and the input filter time from the timing to read inputs for each NX Unit.
- The ON/OFF response time is needed from the timing to refresh outputs until setting the output status of external terminals on the NX Units.

Inputs



Outputs



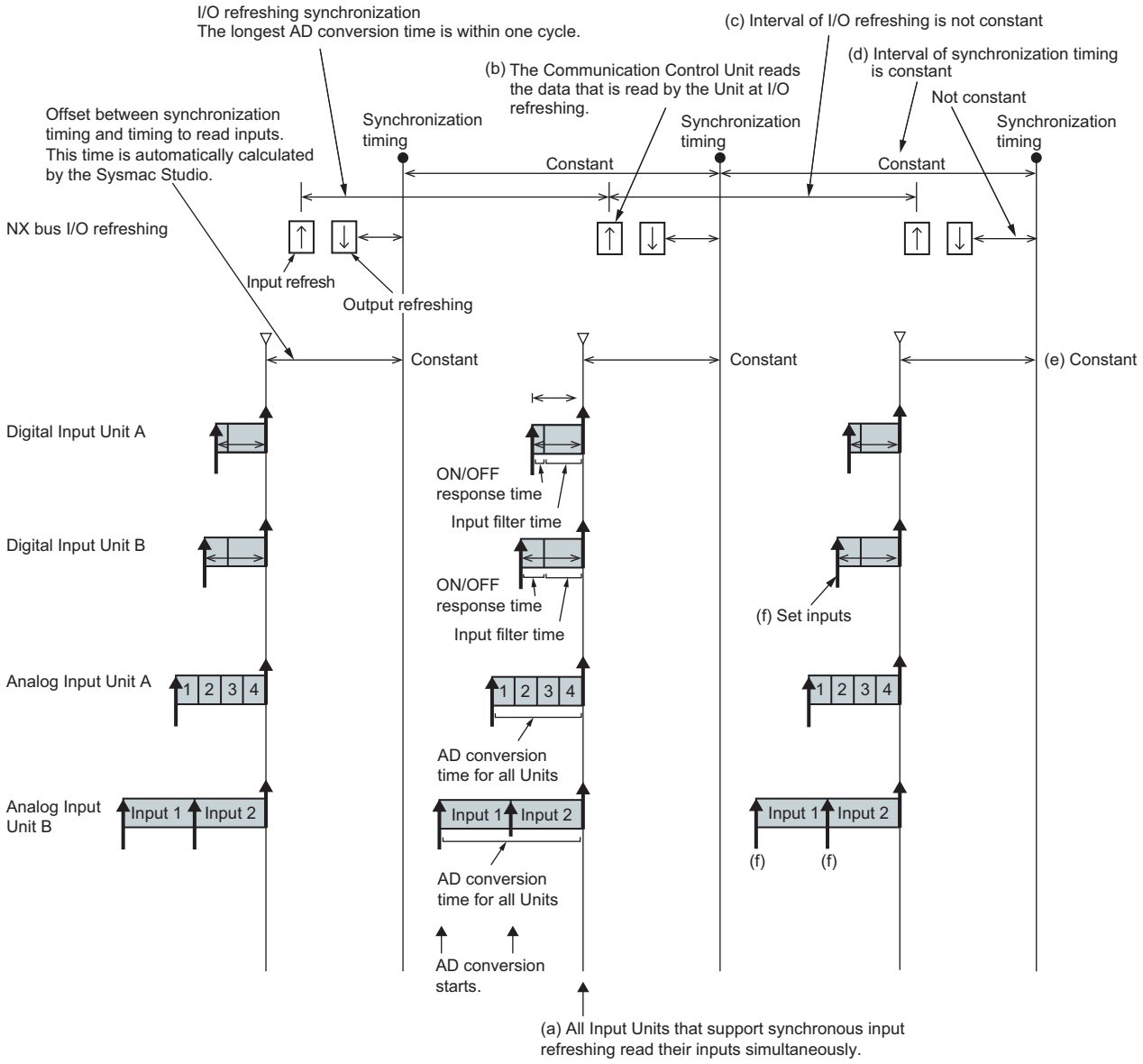
Synchronous Input Refreshing

With this I/O refreshing method, the timing to read inputs is synchronized on a fixed interval between more than one NX Unit connected to the Communication Control Unit.
This method is used when the problem such as input timing jitter or offset of timing to read inputs between more than one NX Unit happens.

● Description of Operation

The following describes the operation of synchronous input refreshing between the Communication Control Unit and the NX Units.

- All Digital Input Units and Analog Input Units that are connected to the Communication Control Unit and operate with synchronous input refreshing read their inputs at the same time at a fixed interval based on the synchronization timing. (Refer to (a) in the figure below.)
- The Communication Control Unit reads the input values, which are read by the Unit at the timing of reading inputs, at immediate I/O refreshing. (Refer to (b) in the figure below.)
- The interval of I/O refreshing varies with the processing conditions of the Communication Control Unit. (Refer to (c) in the figure below.) The timing to read inputs will be at a fixed interval. (Refer to (d) and (e) in the figure below.)
- The timing of reading inputs, the synchronization timing, and the maximum NX bus I/O refresh cycle are automatically calculated by the Sysmac Studio according to the input refresh cycles of the NX Units on the Communication Control Unit when a Unit configuration in the Communication Control Unit is created and set up.
- In order to read input values correctly, you must determine the inputs before the total of ON/OFF response time and input filter time from the timing to read inputs for each NX Unit. (Refer to (f) in the figure below.)



Synchronous Output Refreshing

With this refreshing method, the timing to refresh outputs is synchronized on a fixed interval between more than one NX Unit connected to the Communication Control Unit.

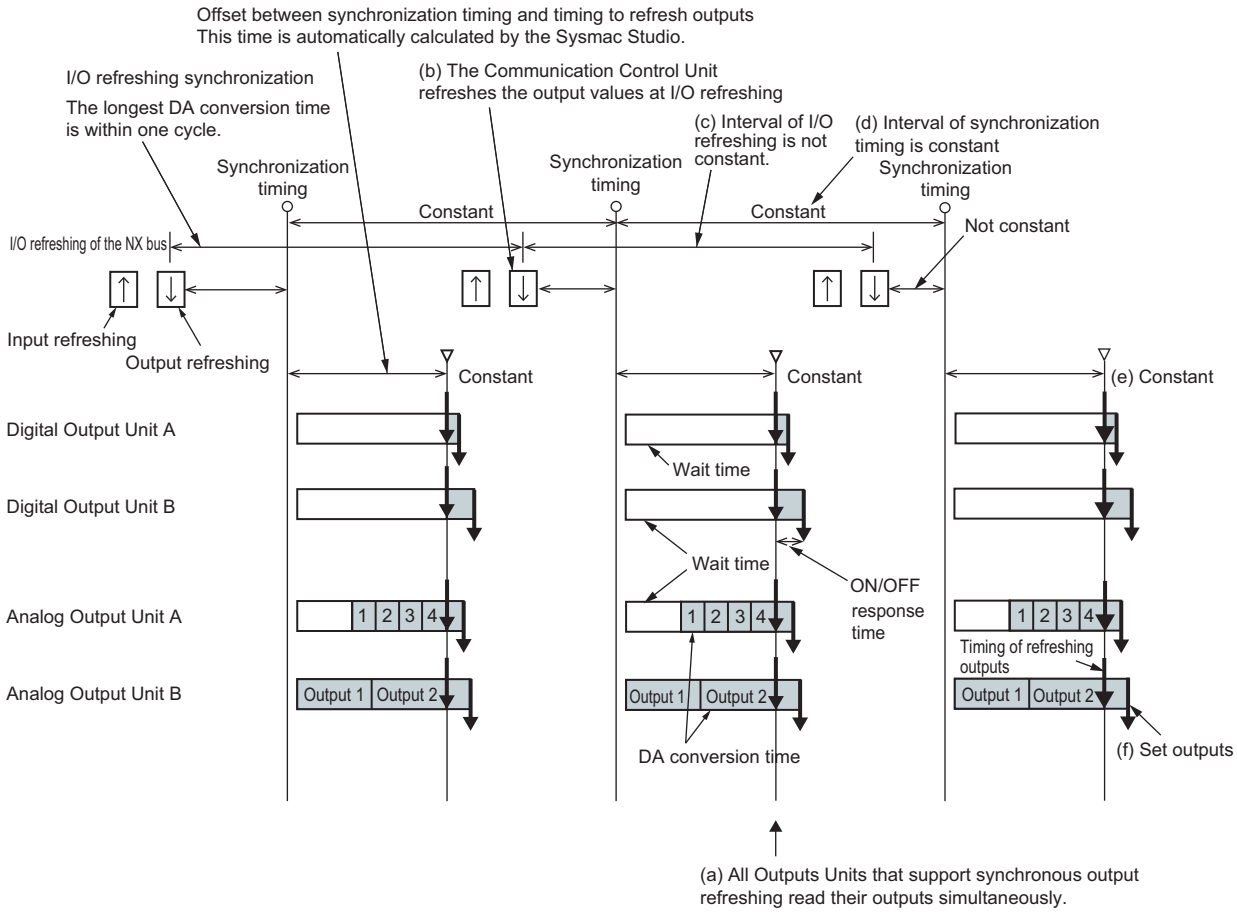
This method is used when the problem such as input timing jitter or offset of timing to refresh outputs between more than one NX Unit happens.

● Description of Operation

The following describes the operation of synchronous output refreshing between the Communication Control Unit and the NX Units.

- All Digital Output Units and Analog Output Units that are connected to the Communication Control Unit and operate with synchronous output refreshing refresh their outputs at the same time at a fixed interval based on the synchronization timing. (Refer to (a) in the figure below.)
- The Communication Control Unit refreshes the output values at I/O refreshing. (Refer to (b) in the figure below.)

- The interval of I/O refreshing varies with the processing conditions of the Communication Control Unit. (Refer to (c) in the figure below.) The timing of refreshing outputs will be at a fixed interval. (Refer to (d) and (e) in the figure below.)
- The timing of refreshing outputs, the synchronization timing, and the maximum NX bus I/O refresh cycle are automatically calculated by the Sysmac Studio according to the output refresh cycles of the NX Units on the Communication Control Unit when a Unit configuration in the Communication Control Unit is created and set up.
- The ON/OFF response time is needed from the timing to refresh outputs until setting the output status of external terminals on the NX Units. (Refer to (f) in the figure below.)



A-12-3 I/O Response Time for Communications between NX Units

This section describes the input response time and the output response time for communications between NX Units.

For calculations of the response time specific to each NX Unit, refer to the user's manuals for individual NX Units or the *NX-series Data Reference Manual* (Cat. No. W525).

Input Response Times

The input response time gives the time required from when an external signal is input to the NX Unit until it is processed by the Safety CPU Unit.

The maximum input response time is calculated as follows:

Formula: Maximum input response time = Tnx-InProc x 2 + Tnx-Indelay + 3.75 ms + Safety task period

The elements in the formulas are as follows:

- Safety task period: Setting of the safety task period in the Safety CPU Unit
- Tnx-InProc: Input data processing time of the NX Unit
- Tnx-Indelay: Output delay time of the NX Unit

Output Response Times

The output response time is the time from data processing on the Safety CPU Unit until the results are externally output from an NX Unit.
The maximum output response time is calculated as follows:

Formula: Maximum output response time = Tnx-OutProc x 2 + Tnx-Outdelay + 3.75 ms + Safety task period

The elements in the formulas are as follows:

- Safety task period: Setting of the safety task period in the Safety CPU Unit
- Tnx-OutProc: Output data processing time of the NX Unit
- Tnx-Outdelay: Output delay time of the NX Unit



Additional Information

To calculate the I/O response times between a Safety I/O Unit and standard I/O Unit, add the input response time or output response time to the FSoE watchdog timer value of the Safety I/O Unit.

A-13 Units That Support Communications between NX Units

Refer to *A-20 Version Information* on page A-115.

A-14 Checking the Signature Code on the Seven-segment Indicator

Use the following procedure to display a signature code on the seven-segment indicator on the front panel of the Safety CPU Unit.

1 Press the service switch on the front panel of the Safety CPU Unit.
If you hold down the service switch, the display of the seven-segment indicator will change as shown below.

After 1 second "Si." → After 3 seconds "Lo." → After 5 seconds "--"

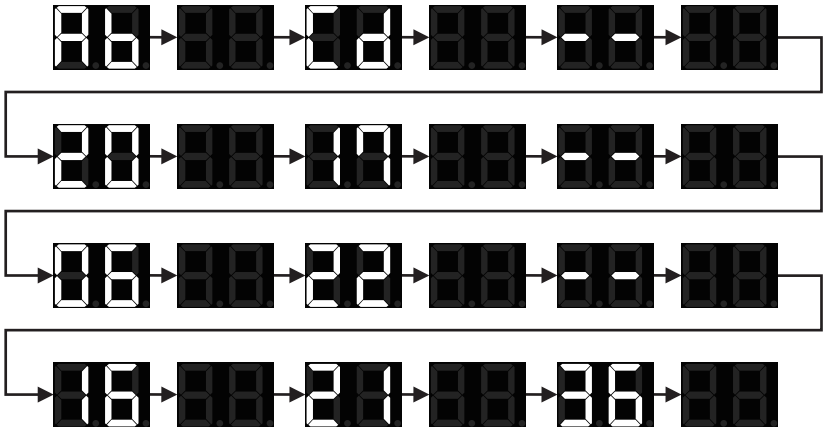


Release the service switch while the indicator shows "Si".
If you release the service switch while "--" is displayed, the function does not execute and the original state is restored.

2 The signature code appears.
The indicator displays all nine bytes starting from the creation date (UTC) and then the signature code one byte at a time.

(Signature display start symbol --> Signature code (High) --> Signature code (Low) --> Separator (--) --> Year (High) --> Year (Low) --> Separator (--) --> Month --> Day --> Separator (--) --> Hour --> Minute --> Second)

Example: The signature code is ABCD, and the date is 16:21:36 of June 22, 2017 (UTC)



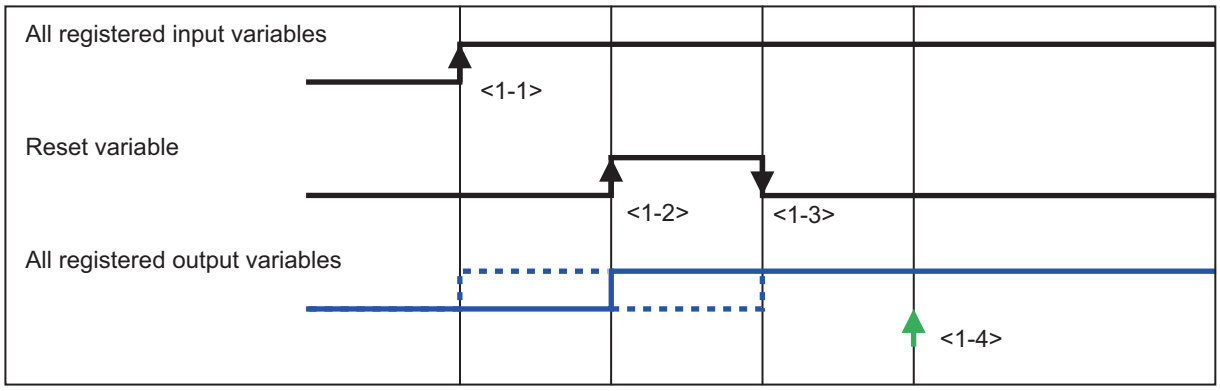
When the signature code is undefined, "--" appears.

A-15 Execution Scenarios for the Simple Automatic Test

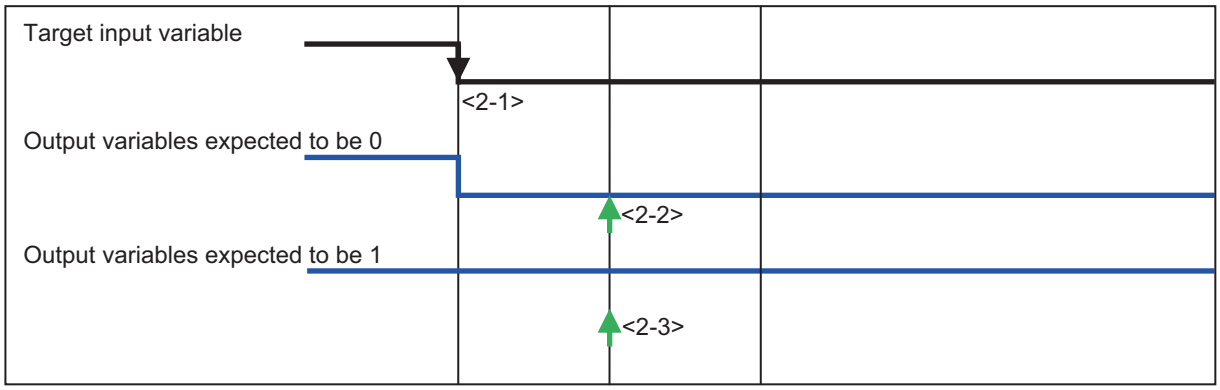
The operations given in the following table are executed in order for the Simple Automatic Test.

No.	Test phase	Executed processes	Confirmations	Displayed errors
1	Initialize	Set all the registered input variables to TRUE. <1-1> Set the reset variable to TRUE. <1-2> Set the reset variable to FALSE. <1-3>	Examine all the registered output variables are TRUE. <1-4>	<Error> "Cannot Execute" <Remarks> "The following output variables are FALSE after the reset."
2	Shutoff Test	The input variables are set to FALSE. <2-1>	Examine the output variables expected to be 0 in the expected value setting table are FALSE. <2-2>	<Error> "Failed" <Remarks> "The following output variables do not match with the expected values."
			Examine the output variables expected to be 1 in the expected value setting table are TRUE. <2-3>	<Error> "Failed" <Remarks> "The following output variables do not match with the expected values."
3	Restore Test <Reset Type: Auto>	Set the input variable to TRUE. <3-1>	Examine all the registered output variables are TRUE. <3-2>	<Error> "Failed" <Remarks> "The following output variables do not return."
4	Restore Test <Reset Type: Manual>	Set the input variable to TRUE. <4-1> Set the reset variable to TRUE. <4-2> Set the reset variable to FALSE. <4-3>	Examine the output variables expected to be 0 in the expected value setting table are FALSE. <4-4>	<Error> "Failed" <Remarks> "The following output variables do return."
			Examine all the registered output variables are TRUE. <4-5>	<Error> "Failed" <Remarks> "The following output variables are FALSE after the reset."

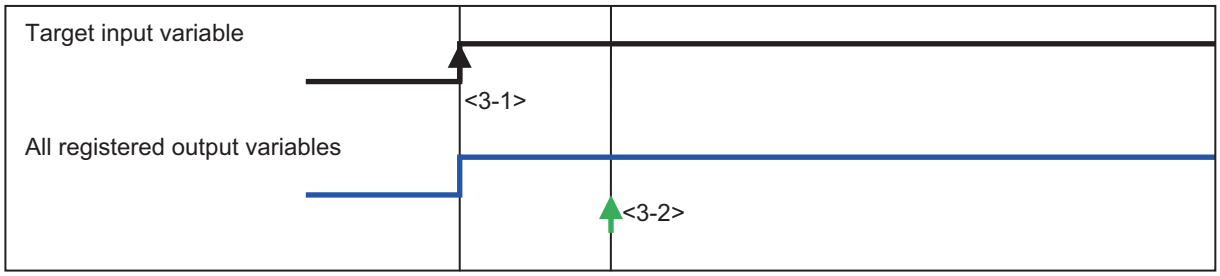
1. Initialization



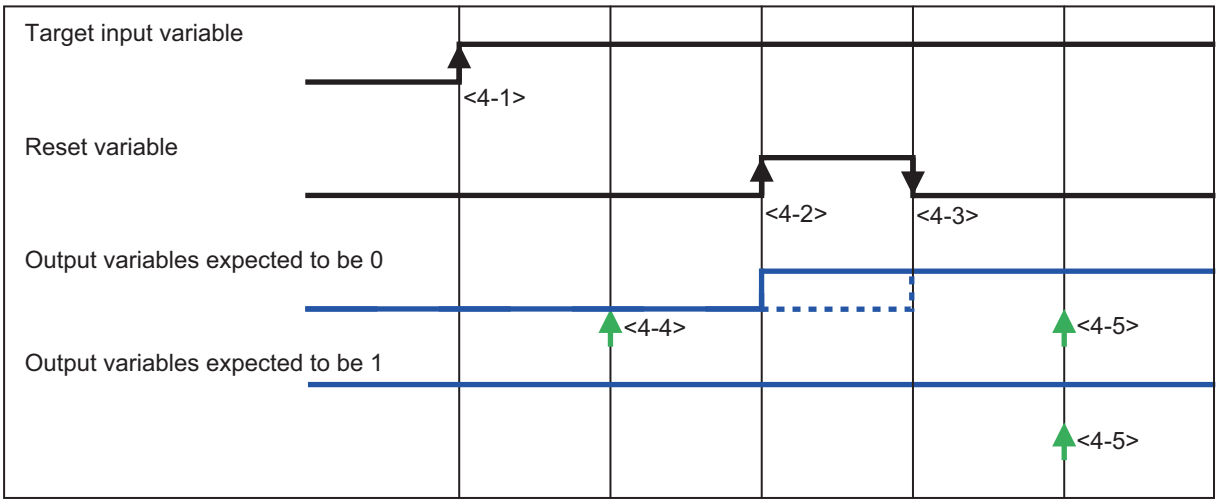
2. Shutoff Test



3. Restore Test (Reset Type: Auto)



4. Restore Test (Reset Type: Manual)


Target input variable
<4-1>
Reset variable
<4-2>
<4-3>
Output variables expected to be 0
<4-4>
<4-5>
Output variables expected to be 1
<4-5>

A-16 Differences in Checking Operation between the Simulator and Safety CPU Unit

This section describes the differences in the program debugging functions that you can perform on the Sysmac Studio between online debugging on a Safety CPU Unit and offline debugging with the Simulator.

Debugging function	Safety CPU Unit	Simulator	Reference
Monitoring	Supported.	Supported.	*9-6-3 Monitoring Variables in the FBD Editor* on page 9-23 *9-6-4 Monitoring Variables in a Watch Tab Page* on page 9-24
Monitoring in a Watch Tab Page	Supported.	Supported.	*9-6-5 Controlling BOOL Variables, Changing Present Values, and Using Forced Refreshing* on page 9-26
Controlling BOOL variables	Supported.	Supported.	
Forced refreshing inputs	Supported.	Supported.	
Changing present values of data	Supported.	Supported.	
Monitoring Controller status	Supported.	Supported.	*9-15 Monitoring Controller Status* on page 9-70
Clear All Memory	Supported.	Not supported.	*9-16-2 Clear All Memory Operation* on page 9-72
Changing the operating mode	Supported.	Not supported.	*9-3 Operating Modes of the Safety CPU Unit* on page 9-8
Troubleshooting	Supported.	Not supported.	*Section 15 Troubleshooting* on page 15-1
Monitoring error information	Supported.	Not supported.	
Displaying error logs	Supported.	Not supported.	

A-17 I/O Data Enable Flag for CIP Safety Connections

You can use the I/O data enable flag for CIP Safety connections in the safety program.

ON and OFF Conditions of the I/O Data Enable Flag for CIP Safety Connections

You can use the I/O data enable flag for CIP Safety connections in the safety program.

Connection type	Data Direction	ON (data enabling) conditions	OFF (data disabling) conditions
Originator Connection	IN (Target Device →Safety CPU Unit)	Safety connection open and valid data*1 received	Disconnection or invalid data*1 received
	OUT (Safety CPU Unit→ Target Device)	Safety connection open and data being transmitted	Disconnection
Target Connection (Single-cast)	OUT (Originator Device → Safety CPU Unit)	Safety connection open and valid data*2 received	Disconnection or invalid data*2 received
	IN (Safety CPU Unit → Originator Device)	Safety connection open and data being transmitted	Disconnection
Target Connection (Multi-cast)	IN (Safety CPU Unit → Originator Device)	At least one connection open and data being transmitted	All connections disconnected

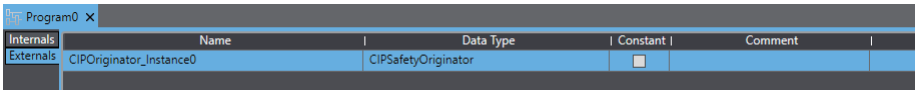
*1. Whether the data is enabled or disabled depends on the target device. When the target device is NX-SL5500 or NX-SL5700, the data is always enabled.

*2. Whether the data is enabled or disabled depends on the originator device. When the originator device is NX-SL5500 or NX-SL5700, the data is always enabled.

Using the I/O Data Enable Flag for CIP Safety Connections

The following describes the procedure to use the I/O data enable flag for CIP Safety connections.

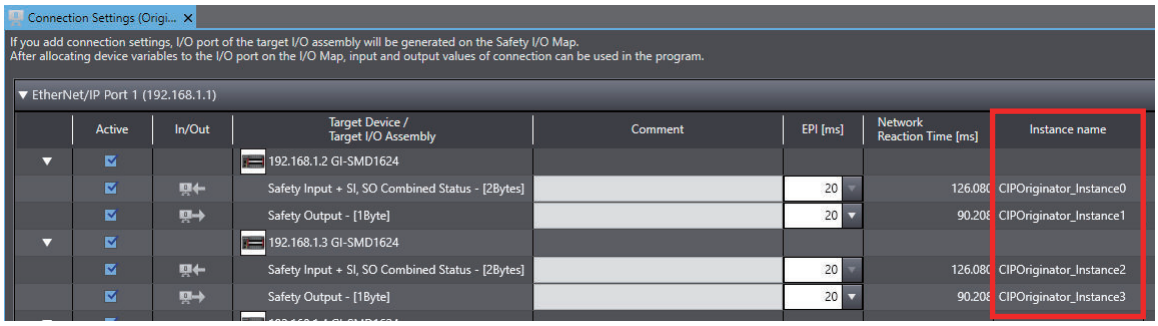
1 Register CIP Safety connection instance variables as the external variables of the program POU.



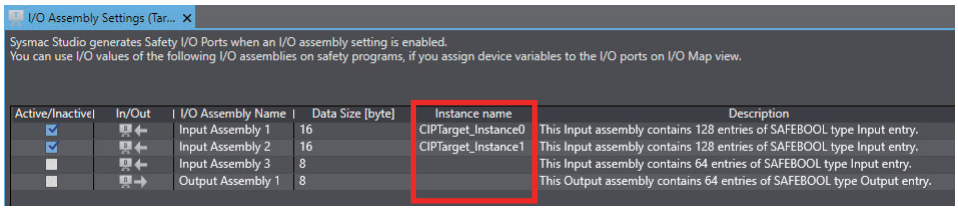
The following list shows a combination of the instance variable name and data type.

Instance variable name	Data type
"CIPOriginator_Instance" + number	CIPSafetyOriginator
"CIPTarget_Instance" + number	CIPSafetyTarget

The instance variable name of the originator can be verified on the **Connection Settings (Originator)** screen.



The target instance variable name can be verified on the **I/O Assembly Settings (Target)** screen.



2 Use "InstanceVariableName.S_RunIdleFlag" in the program POU.

Precautions for Correct Use

The I/O data enable flag for CIP Safety connections (S_RunIdleFlag) is supported by the NX-SL5500/NX-SL5700 unit version 1.4 or higher. Do not use this feature with the unit version 1.3 or lower.

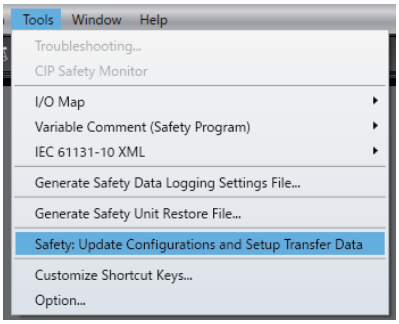
A-18 Safety: Update Configurations and Setup Transfer Data

If a standard controller and a Safety CPU Unit are transferred by using different projects, the following error may occur.

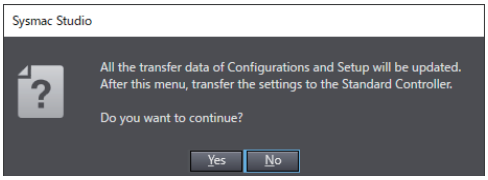
Event name	Event Code
NX Bus Communications Settings and Safety Application Data Mismatch	10520000 hex

If you cannot resolve the above error after you implement the normal correction, use the following procedure.

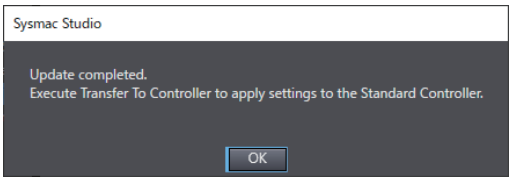
1 From the main menu, select **Tools** – **Safety: Update Configurations and Setup Transfer Data**.



The following confirmation dialog is displayed.



2 Click the **Yes** button.
When you complete Safety: Update Configurations and Setup Transfer Data, the following message appears.

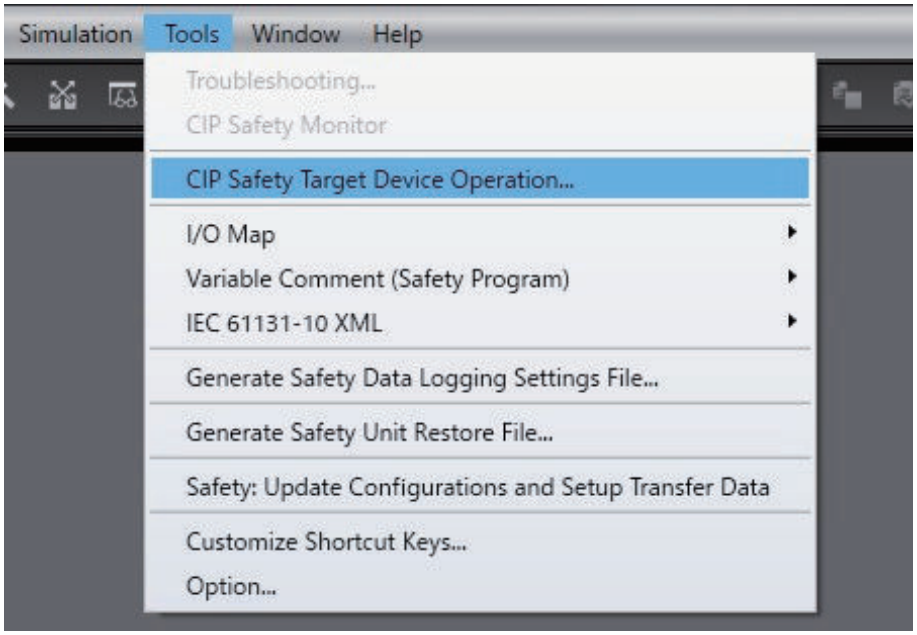


3 Click the **OK** button.
Execute **Transfer to Controller** of the standard controller after the update is completed.

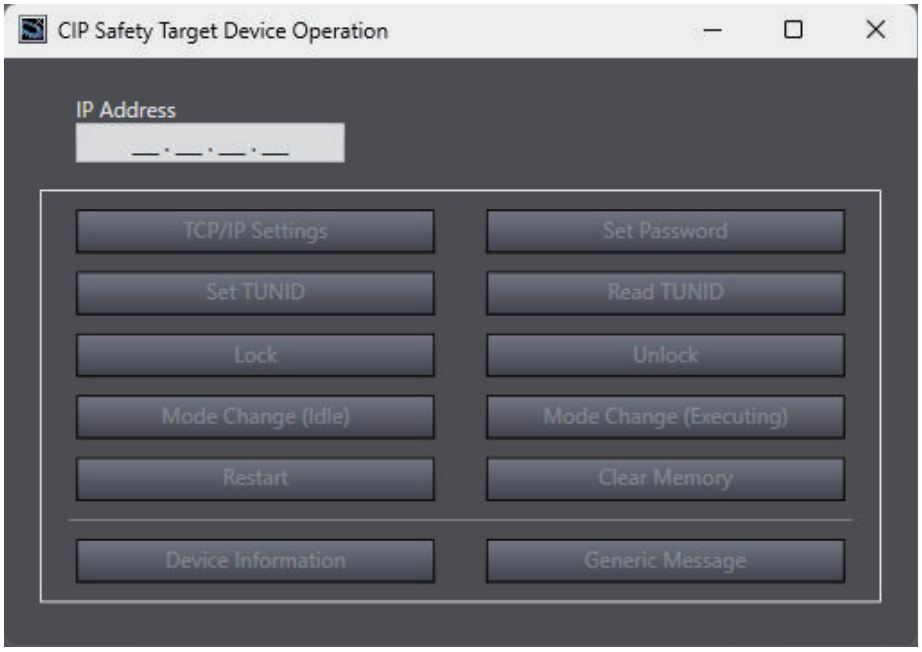
A-19 CIP Safety Target Device Operation

You can send CIP messages directly to a CIP Safety target device from the computer to perform the memory clear, TUNID setting, and other operations.
To directly operate the target device without using the Safety CPU Unit, perform the following procedure.

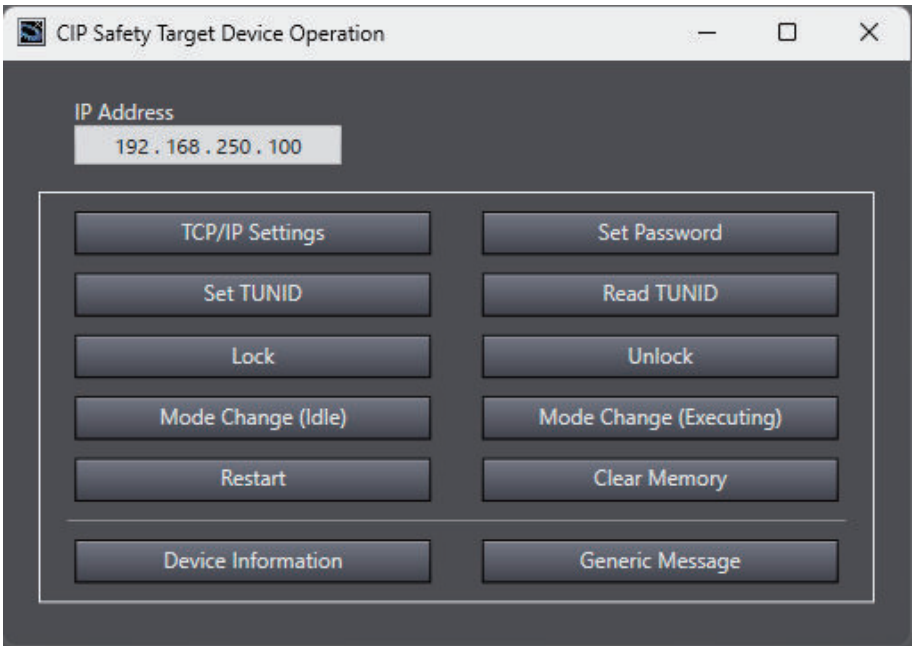
1 From the Controller Menu, select**Tools**–**CIP Safety Target Device Operation**.



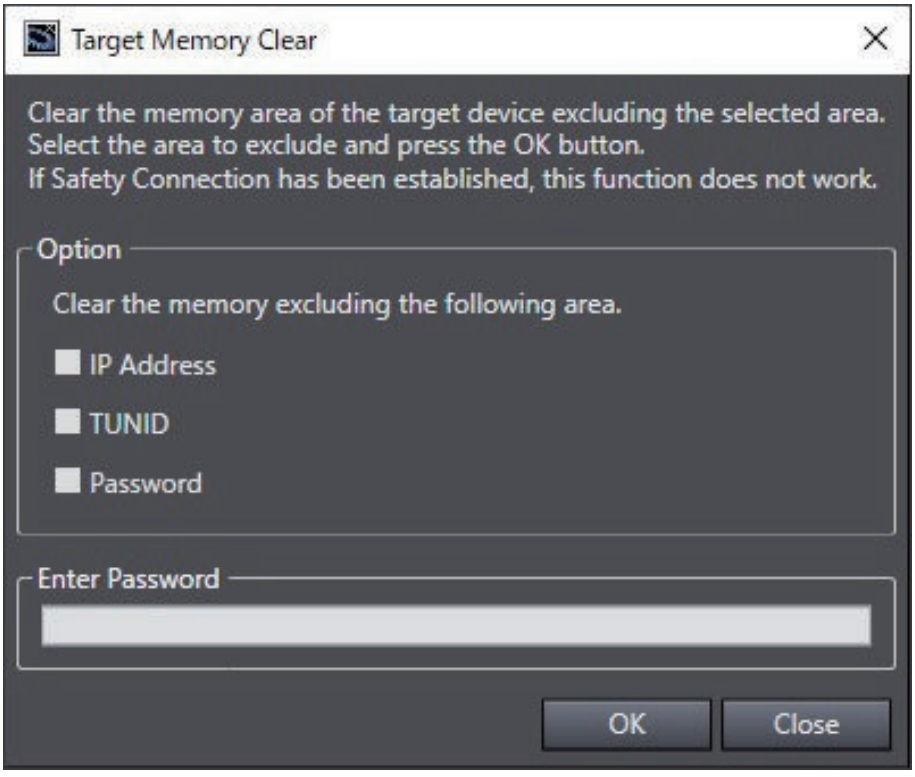
The CIP Safety Target Device Operation window is displayed.



2 Enter the IP address of the target device, and click a desired operation button.



Example: When the**Clear Memory**button is pressed
The following Target Memory Clear window is displayed.



3 Operate the device as instructed on the displayed window.
The operation buttons and the contents to be executed are as follows.

Button name	Description
TCP/IP Settings	Sets such as the IP address of the target device.
Set Password	Sets the password of the target device.
Set TUNID	Sets TUNID of the target device.
Read TUNID	Reads TUNID of the target device.
Lock	Locks the configuration for the target device.

Button name	Description
Unlock	Unlocks the configuration for the target device.
Mode Change (Idle)	Change the target device's mode to Idle.
Mode Change (Executing)	Change the target device's mode to Executing.
Restart	Restarts the target device.
Clear Memory	Clears the settings of the target device.
Device Information	Reads the device information of the target device.
Generic Message	Sends desired CIP messages to the target device.



Precautions for Correct Use

- This function depends on the operation specifications of the target device. Some operations are not supported depending on the device functions.
- If you set TUNID to the target device, make sure that the correct TUNID is set to the intended device under your responsibility. Also, ensure that all TUNIDs are unique across the system.

A-20 Version Information

This section describes the compatibility between unit versions of the Safety Control Units and the version of the Sysmac Studio, as well as the functions supported by the Sysmac Studio.

A-20-1 Relationship between the Unit Versions and Sysmac Studio Versions

This section describes the possible combinations of versions of Safety Control Units, Communication Control Units, and Sysmac Studio.

The following table gives the first unit version of the Communication Control Unit and the lowest versions of the Sysmac Studio that can be used together.

Model	:	This is the model number of the NX Unit.
Unit version	:	This is the unit version of the NX Unit.
Communication Control Unit	:	This is the unit version of the Communication Control Unit that supports the Safety CPU Unit.
Sysmac Studio	:	These are the versions of Sysmac Studio that support the Communication Control Unit and the Safety CPU Unit.

Safety Control Unit

NX Unit		Corresponding unit version/version	
Model	**Unit version**	**Communication Control Unit NX-CSG□□□**	**Sysmac Studio**
NX-SL5500	Version 1.3	Version 1.01	Version 1.24*1
	Version 1.4		Version 1.40*1
NX-SL5700	Version 1.2	Version 1.00 only	Version 1.24*1
	Version 1.3	Version 1.01	
	Version 1.4		Version 1.40*1
NX-SIH400	Version 1.0	Version 1.00	Version 1.24*2
	Version. 1.1		
NX-SID800	Version 1.0		
NX-SOD400			
NX-SOH200			

*1. The data types in the following table are supported for communications between NX Units.

Supported data types
BOOL
BYTE
INT
WORD
DINT

*2. Communications between NX Units are not supported.

Digital I/O Units

NX Unit		Corresponding unit version/version	
Model	Unit version	Communication Control Unit NX-CSG□□□	Sysmac Studio
NX-ID3317	Version 1.0	Version 1.00	Version 1.24*1
NX-ID3343	Version 1.0	Version 1.00	Version 1.24*1
NX-ID3417	Version 1.0	Version 1.00	Version 1.24*1
NX-ID3443	Version 1.0	Version 1.00	Version 1.24*1
NX-ID4342	Version 1.0	Version 1.00	Version 1.24*1
NX-ID4442	Version 1.0	Version 1.00	Version 1.24*1
NX-ID5142-1	Version 1.0	Version 1.00	Version 1.24*1
NX-ID5142-5	Version 1.0	Version 1.00	Version 1.24*1
NX-ID5342	Version 1.0	Version 1.00	Version 1.24*1
NX-ID5442	Version 1.0	Version 1.00	Version 1.24*1
NX-ID6142-5	Version 1.0	Version 1.00	Version 1.24*1
NX-ID6142-6	Version 1.0	Version 1.00	Version 1.24*1
NX-IA3117	Version 1.0	Version 1.00	Version 1.24*1
NX-OD3121	Version 1.0	Version 1.00	Version 1.24*1
NX-OD3153	Version 1.0	Version 1.00	Version 1.24*1
NX-OD3256	Version 1.0	Version 1.00	Version 1.24*1
NX-OD3257	Version 1.0	Version 1.00	Version 1.24*1
NX-OD3268	Version 1.0	Version 1.00	Version 1.24*1
NX-OD4121	Version 1.0	Version 1.00	Version 1.24*1
NX-OD4256	Version 1.0	Version 1.00	Version 1.24*1
NX-OD5121	Version 1.0	Version 1.00	Version 1.24*1
NX-OD5121-1	Version 1.0	Version 1.00	Version 1.24*1
NX-OD5121-5	Version 1.0	Version 1.00	Version 1.24*1
NX-OD5256	Version 1.0	Version 1.00	Version 1.24*1
NX-OD5256-1	Version 1.0	Version 1.00	Version 1.24*1
NX-OD5256-5	Version 1.0	Version 1.00	Version 1.24*1
NX-OD6121-5	Version 1.0	Version 1.00	Version 1.24*1
NX-OD6121-6	Version 1.0	Version 1.00	Version 1.24*1
NX-OD6256-5	Version 1.0	Version 1.00	Version 1.24*1
NX-OC2633	Version 1.0	Version 1.00	Version 1.24*1
NX-OC2733	Version 1.0	Version 1.00	Version 1.24*1
NX-OC4633	Version 1.0	Version 1.00	Version 1.24*1
NX-MD6121-5	Version 1.0	Version 1.00	Version 1.24*1
NX-MD6121-6	Version 1.0	Version 1.00	Version 1.24*1
NX-MD6256-5	Version 1.0	Version 1.00	Version 1.24*1

*1. The data types in the following table are supported for communications between NX Units.

Supported data types
BOOL
BYTE
INT
WORD
DINT

Analog I/O Units

NX Unit		Corresponding unit version/version	
Model	Unit version	Communication Control Unit NX-CSG□□□	Sysmac Studio
NX-AD2203	Version 1.0	Version 1.00	Version 1.24*1
NX-AD2204	Version 1.0	Version 1.00	Version 1.24*1
NX-AD2208	Version 1.0	Version 1.00	Version 1.24*1
NX-AD2603	Version 1.0	Version 1.00	Version 1.24*1
NX-AD2604	Version 1.0	Version 1.00	Version 1.24*1
NX-AD2608	Version 1.0	Version 1.00	Version 1.24*1
NX-AD3203	Version 1.0	Version 1.00	Version 1.24*1
NX-AD3204	Version 1.0	Version 1.00	Version 1.24*1
NX-AD3208	Version 1.0	Version 1.00	Version 1.24*1
NX-AD3603	Version 1.0	Version 1.00	Version 1.24*1
NX-AD3604	Version 1.0	Version 1.00	Version 1.24*1
NX-AD3608	Version 1.0	Version 1.00	Version 1.24*1
NX-AD4203	Version 1.0	Version 1.00	Version 1.24*1
NX-AD4204	Version 1.0	Version 1.00	Version 1.24*1
NX-AD4208	Version 1.0	Version 1.00	Version 1.24*1
NX-AD4603	Version 1.0	Version 1.00	Version 1.24*1
NX-AD4604	Version 1.0	Version 1.00	Version 1.24*1
NX-AD4608	Version 1.0	Version 1.00	Version 1.24*1
NX-DA2203	Version 1.0	Version 1.00	Version 1.24*1
NX-DA2205	Version 1.0	Version 1.00	Version 1.24*1
NX-DA2603	Version 1.0	Version 1.00	Version 1.24*1
NX-DA2605	Version 1.0	Version 1.00	Version 1.24*1
NX-DA3203	Version 1.0	Version 1.00	Version 1.24*1
NX-DA3205	Version 1.0	Version 1.00	Version 1.24*1
NX-DA3603	Version 1.0	Version 1.00	Version 1.24*1
NX-DA3605	Version 1.0	Version 1.00	Version 1.24*1

*1. The data types in the following table are supported for communications between NX Units.

Supported data types
BOOL
BYTE

Supported data types
INT
WORD
DINT

Temperature Input Units

NX Unit		Corresponding unit version/version	
Model	Unit version	Communication Control Unit NX-CSG□□□	Sysmac Studio
NX-TS2101	Version 1.0	Version 1.00	Version 1.24*1
NX-TS2101	Version.1.1	Version 1.00	Version 1.24*1
NX-TS2102	Version.1.1	Version 1.00	Version 1.24*1
NX-TS2104	Version.1.1	Version 1.00	Version 1.24*1
NX-TS2201	Version 1.0	Version 1.00	Version 1.24*1
NX-TS2201	Version.1.1	Version 1.00	Version 1.24*1
NX-TS2202	Version.1.1	Version 1.00	Version 1.24*1
NX-TS2204	Version.1.1	Version 1.00	Version 1.24*1
NX-TS3101	Version 1.0	Version 1.00	Version 1.24*1
NX-TS3101	Version.1.1	Version 1.00	Version 1.24*1
NX-TS3102	Version.1.1	Version 1.00	Version 1.24*1
NX-TS3104	Version.1.1	Version 1.00	Version 1.24*1
NX-TS3201	Version 1.0	Version 1.00	Version 1.24*1
NX-TS3201	Version.1.1	Version 1.00	Version 1.24*1
NX-TS3202	Version.1.1	Version 1.00	Version 1.24*1
NX-TS3204	Version.1.1	Version 1.00	Version 1.24*1

*1. The data types in the following table are supported for communications between NX Units.

Supported data types
BOOL
BYTE
INT
WORD
DINT

System Unit

NX Unit		Corresponding unit version/version	
Model	Unit version	Communication Control Unit NX-CSG□□□	Sysmac Studio
NX-PD1000	Version 1.0	Version 1.00	Version 1.24*1
NX-PF0630	Version 1.0	Version 1.00	Version 1.24*1
NX-PF0730	Version 1.0	Version 1.00	Version 1.24*1

NX Unit		Corresponding unit version/version	
Model	Unit version	Communication Control Unit NX-CSG□□□	Sysmac Studio
NX-PC0010	Version 1.0	Version 1.00	Version 1.24*1
NX-PC0020	Version 1.0	Version 1.00	Version 1.24*1
NX-PC0030	Version 1.0	Version 1.00	Version 1.24*1
NX-TBX01	Version 1.0	Version 1.00	Version 1.24*1

*1. Communications between NX Units are not supported.

I

Index

Index

A

Additional I/O Power Supply Unit..... 4-5
Additional NX Unit Power Supply Unit.....4-4
Adjusting the communications load..... 11-2
Adjusting the device bandwidth usage..... 11-5
angle for insertion.....5-51, 5-53
Applicable Wire.....5-46
Assumed cause..... 15-50
Attached information.....15-50

B

Backing up data.....13-2
Block.....4-21
Built-in EtherNet/IP Port (PORT1) 3-11
Built-in EtherNet/IP Port (PORT2) 3-11

C

Calculating the Effective Value..... 4-19
Checking Bandwidth Usage for Tag Data Links.....11-3
Checking for errors.....15-6, 15-15, 15-31
checking the current IP address.....7-17
Checking the Device Bandwidth Usage of the CIP Safety Routing.....11-4
CIDR.....7-11
CIP communications errors..... 15-19
Coding Pin.....5-56
commercially available markers..... 5-20
Communication Control Unit operating status..... 15-3
Communications port errors..... 15-19
connection status codes and troubleshooting..... 15-249
Connection Tab Page..... 15-245
Controller errors.....15-8
Controller Event Times..... 15-7
Controller events..... 15-6
Controller events sources.....15-7
Controller information..... 15-8
Controller Log Tab Page.....15-246
Controller status..... 6-9
Correction..... 15-50
CPU Unit Error..... 15-4, 15-25
crimping tool..... 5-47

D

Daisy chain.....5-69
Daisy Chain..... 5-67
Detection timing.....15-50
Device Monitor.....15-241
DIN Track.....5-9, 5-11
DIN Track contact plate..... 3-11, 5-35
DIN Track Insulation Spacer.....5-38
DIN Track mounting hook.....3-10
DIP Switch 3-11

E

Earthing Methods..... 5-67
End Cover 3-11, 5-17
End Plate.....5-9, 5-10, 5-18
Equipotential bonding system..... 5-67, 5-68
Error Status variable.....15-16, 15-31
Ethernet connectors..... 5-44
Ethernet Information Tab Page.....15-248
Ethernet switches
  connection methods.....5-44
  functions.....5-39
  installation precautions..... 5-43
  selection precautions..... 5-40
event code..... 15-14
Event code.....15-50
event log..... 15-6
Event name..... 15-50
events..... 15-6
Extended Status Code..... A-80

F

Ferrule..... 5-46
Functional Grounding..... 5-71

G

General Status Codes.....A-78
Ground terminal.....5-47, 5-48
Grounding.....5-35, 5-67

H

Hardware Initialization Error..... 15-25

I

I/O power supply..... 4-3, 4-22
I/O Power Supply Connection Unit.....4-7
ID information indication 3-11, 3-21
identifying and resetting errors..... 15-25
incorrect attachment prevention hole..... 5-58
indicators..... 15-15
Information level..... 15-8
inrush current.....4-22
Installation Dimensions.....5-28
Installation Height..... 5-31
Installation in Cabinets or Control Panels.....5-5
Installation Locations for Protective Devices..... 4-24
Installation Method in Control Panels..... 5-7
IP address allocation..... 7-9
IP address configuration.....7-9
IP address setting.....7-13
IP Address Switch 1 (x16, x1).....3-11
IP Address Switch 2 (x16, x1).....3-11

L

LED....15-2
Level....15-50
levels....15-8
Log category....15-50
Lot number....44, 3-21

M

MAC addresses....44, 3-21
major fault level....15-8, 15-13
Maximum I/O Power Supply Current....4-14
minor fault level....15-8
multicast and unicast communications....6-8

N

NX bus connector....3-10
NX Unit Power Supply Capacity....4-10

O

Observation level....15-8
Online....15-31
Operation Status Indicators....3-11
Operation until Operation Ready Status....5-2
Other Troubles and Corrections....15-167
Overcurrent....4-23

P

Packet Interval (RPI)....6-8
partial fault level....15-8
Periodic Inspection Item....16-2
Power Supply Error....15-4, 15-24
power supply-related Unit....4-3
Preventing Incorrect Attachment....5-56
Prevention....15-50
Production Information....46
Protective device....4-23

R

Recovery....15-50
Relationship between the Number of Packets Used per Second and Packet Intervals....11-5
Required Power Supply Capacity of the I/O Power Supply....4-22
Required Power Supply Capacity of the Unit Power Supply....4-20
Requirements for Power Supplies....4-20, 4-22
resetting errors....15-17
Restoring data....13-2
Restrictions on Inrush Current....4-19

S

safety data types....8-15
safety input functions....6-28
  dual channel evaluation....6-30
    dual channel....6-30, 6-42
    single channel....6-30, 6-42
  input filters....6-36
  test pulse....6-29
safety output functions....6-41
  dual channel evaluation....6-42
  test pulse evaluation....6-42
safety program....8-3
SD Memory Card....5-21
SD Memory Card connector....3-10
SD Memory Card cover....3-11
SD Memory Card power supply switch....3-10
Securing Wires....5-48
security errors....15-240
Selecting Protective Device....4-23
Solid Wire....5-47
source details....15-7
Source details....15-50
sources....15-19
special marker printer....5-20
standard data types....8-15
Star earthing....5-67, 5-68
starting and stopping tag data links....6-8
Status 1 Tab Page....15-241
Status 2 Tab Page....15-244
subnet mask....7-10
supply from external source....4-12
supply from the NX bus....4-12
synchronization timing....A-99, A-100
Sysmac Studio....3-61
System Initialization Error....15-4, 15-25
system-defined variables....15-16, 15-31

T

tag data links
  data areas....6-5
  introduction....6-4
  settings....7-17
tag sets....6-5
Tag Status Tab Page....15-247
tags....6-5
TCP application errors....15-19
The voltage drop in the I/O power supply....4-13, 4-17
timing to read inputs....A-97
timing to refresh outputs....A-97
Troubleshooter....15-16
troubleshooting....15-15
Troubleshooting Functions....15-25
Twisted Wire....5-47
twisted-pair cable
  installation precautions....5-41

U

Unit hookup guide....3-11
Unit power supply....4-2, 4-20
Unit Version....44, 3-21

V

Verifying data.....13-2

W

Wiring Ducts..... 5-7
Wiring Terminal.....5-46
Wiring the Unit Power Supply.....5-33

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN **Contact : www.ia.omron.com**

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

©OMRON Corporation 2018-2026 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. Z395-E1-21 1026