OMRON

Environment-resistive Remote Terminal

NXR-S series

Simple Logic Safety I/O Block for CIP Safety

User's Manual

NXR-SXD1204-CST
NXR-SXD1204B-CST

Safety I/O Block



Original instructions

W645-E1-04

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.
- Smartclick is a trademark or registered trademark of OMRON Corporation in Japan and other countries.
- 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 a 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 ODVA and CIP Safety logos 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/ and http://www.fa.omron.co.jp/nx_info_e/.

Introduction

Thank you for purchasing an Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety (hereinafter referred to as Safety I/O Block).
This manual contains information that is necessary to use the Safety I/O Block. Please read this manual and make sure you understand the functionality and performance of the Unit before you attempt to build an IO-Link 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.

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

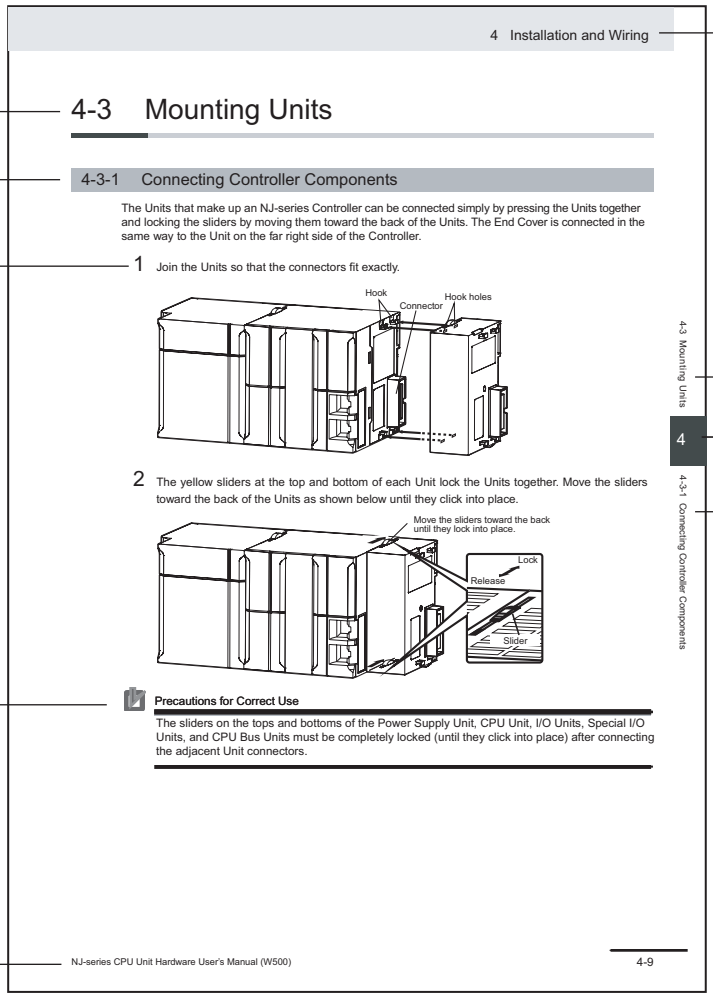
This manual covers the following products.

- Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety
  NXR-SXD1204-CST
  NXR-SXD1204B-CST

Manual Structure

Page Structure

The following page structure is used in this manual.



Level 1 heading
Level 2 heading
Level 3 heading
Gives the current headings.

Page tab
Gives the number of the main section.

A step in a procedure
Indicates a procedure.

Special information
Icons indicate precautions, additional information, or reference information.

Manual name

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

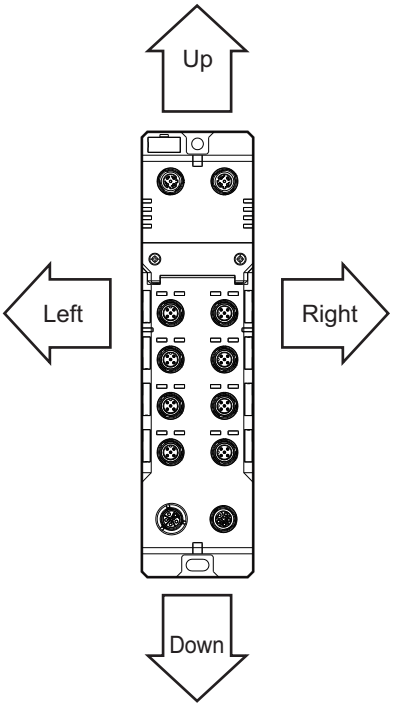
Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality for Controllers with different unit versions and for different versions of the Support Software is given.

Precaution on Terminology

- In this manual, "download" refers to transferring data from the Support Software to a physical device and "upload" refers to transferring data from a physical device to the Support Software.
- In this manual, the directions of the Unit are given as in the following diagram, which shows a front view of the Unit.



Sections in this Manual

1 Features and System Configuration

2 Specifications and Application Procedures

3 Part Names and Functions

4 Designing the Power Supply System

5 Installation and Wiring

6 Operation of the Safety I/O Block

7 Safety I/O Block Settings

8 Functions of Safety I/O Block

9 Safety Response Performance

10 Security Guidelines

11 Troubleshooting

12 Inspection and Maintenance

A Appendices

I Index

CONTENTS

Introduction 1
Intended Audience 1
Applicable Products 1

Manual Structure 2
Page Structure 2
Special Information 3
Precaution on Terminology 3

Sections in this Manual 5

Terms and Conditions Agreement 13
Warranty, Limitations of Liability 13
Application Considerations 14
Disclaimers 14
Statement of security responsibilities for assumed use cases and against threats 15

Safety Precautions 16
Definition of Precautionary Information 16
Symbols 16
Warnings 17
Cautions 23

Precautions for Safe Use 24

Precautions for Correct Use 27

Regulations and Standards 29
Conformance to EU Directives and Regulations 29
Conformance to EN ISO 13849-1 30
Conformance to UL and CSA Standards 30
Conformance to Shipbuilding Standards 31
Conformance to KC Certification 31

Unit Versions 32
Unit Versions 32

Related Manuals 34

Terminology 36

Revision History 38

Section 1 Features and System Configuration

1-1 Overview of Safety I/O Block 1-2

1-2 Features of Safety I/O Block 1-3

1-3 System Configuration 1-4
1-3-1 Safety Control System 1-4
1-3-2 Network Topology 1-13
1-3-3 Cascade Connections 1-14

1-4 Support Software 1-16

Section 2 Specifications and Application Procedures

2-1 Specifications 2-2
2-1-1 General Specifications 2-2
2-1-2 Communications Specifications 2-3
2-1-3 Safety Specifications 2-4
2-1-4 Unit Specifications 2-6

2-2 Usage Procedures 2-9
2-2-1 Step 1. System Design 2-9
2-2-2 Step 2. Software Design 2-9
2-2-3 Step 3. Hardware Design 2-10
2-2-4 Step 4. Calculating and Verifying Safety Response Performance 2-10
2-2-5 Step 5. Software Settings and Programming 2-11
2-2-6 Step 6. Installation and Wiring 2-11
2-2-7 Step 7. Checking Operation 2-12
2-2-8 Step 8. Operation, Maintenance, and Inspection 2-13

Section 3 Part Names and Functions

3-1 Parts and Names 3-2

3-2 Indicators 3-5
3-2-1 Status Indicators 3-5
3-2-2 I/O Indicators 3-8
3-2-3 Unit Identification Indicator 3-9

3-3 Rotary Switches 3-10

3-4 Connectors 3-11
3-4-1 EtherNet/IP Communications Connectors 3-11
3-4-2 Power Supply Connectors 3-11
3-4-3 I/O Connectors 3-12

Section 4 Designing the Power Supply System

4-1 Power Supply Types and Power Supply System 4-2
4-1-1 Power Supply Types and Applications 4-2
4-1-2 Power Supply System 4-2

4-2 Designing the Power Supply System 4-6
4-2-1 Procedure for Designing the Power Supply System 4-6
4-2-2 Design Method for Direct Power Supply 4-6
4-2-3 Design Method for Power Supply System with Through-wiring 4-13

4-3 Selecting Power Supplies and Protective Devices 4-21
4-3-1 Selecting External Power Supplies 4-21
4-3-2 Selecting Protective Devices 4-21

Section 5 Installation and Wiring

5-1 Installing Units 5-2
5-1-1 Installation Precautions 5-2
5-1-2 Installation Orientations 5-2
5-1-3 Installation Method 5-3

5-2 EtherNet/IP Network Wiring 5-5
5-2-1 Installation Precautions 5-5
5-2-2 Connecting Communications Cables 5-6

5-3 Wiring the Power Supply 5-12
5-3-1 Installation Precautions 5-12

5-3-2 Power Supply Cables, Tightening Tools and Tightening Torque to Use....5-12
5-3-3 Connecting Power Supply Cables to External Power Supplies....5-13
5-3-4 Connecting Power Supply Cables....5-14

5-4 Wiring I/O Cables....5-19
5-4-1 Installation Precautions....5-19
5-4-2 Connecting I/O Cables....5-19
5-4-3 Wiring Examples....5-24

5-5 Connected Devices....5-29
5-5-1 Ethernet Cables....5-29
5-5-2 Power Supply Cables....5-31
5-5-3 I/O Cables....5-34
5-5-4 Waterproof Covers for Connectors....5-38

5-6 Options....5-39
5-6-1 Markers....5-39

Section 6 Operation of the Safety I/O Block

6-1 Overview of Operations....6-2

6-2 CIP Safety Communications....6-4

6-3 EtherNet/IP Communications....6-6
6-3-1 Tag Data Link Communications....6-6
6-3-2 Explicit Message Communications....6-6

6-4 Safety Input Functions....6-8
6-4-1 Connectable Devices....6-8
6-4-2 Test Output Function....6-10
6-4-3 Test Pulse Evaluation Function....6-10
6-4-4 Dual Channel Evaluation....6-11
6-4-5 Errors Detectable by the Diagnosis Function of Safety Input Terminals....6-12
6-4-6 Input Filter Function....6-13
6-4-7 Input Error Latch Time....6-15

6-5 Safety Output Functions....6-16
6-5-1 Connectable Devices....6-16
6-5-2 Test Pulse Evaluation Function....6-16
6-5-3 Dual Channel Evaluation....6-17
6-5-4 Errors Detectable by the Diagnosis Function of Safety Output Terminals....6-18
6-5-5 Output Error Latch Time....6-18
6-5-6 EDM Feedback....6-19
6-5-7 Output Delay....6-19

6-6 Logic Function....6-20
6-6-1 Logical Processing....6-20

6-7 Safety Applications....6-23
6-7-1 Purpose of Safety Applications....6-23
6-7-2 Types of Safety Applications....6-23
6-7-3 Fixed Application Details....6-27

6-8 Operating Modes....6-47
6-8-1 Operating Mode Types....6-47
6-8-2 Functions Executable in Each Operating Mode....6-48
6-8-3 Web UI Functions Executable in Each Operating Mode....6-50
6-8-4 Operating Mode Changing and Power-on Mode....6-51

Section 7 Safety I/O Block Settings

7-1 Setting Procedure....7-3
7-1-1 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)....7-3

7-1-2 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI) 7-6
7-1-3 Setting Procedure of Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application 7-9
7-1-4 Setting Procedure of Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User 7-11
7-1-5 Setting Procedure of Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User 7-14

7-2 Overview of the Web UI 7-17
7-2-1 Various Specifications of the Web UI 7-17
7-2-2 Operation Authorities of the Web UI 7-17
7-2-3 Screen Configuration of Web UI 7-17
7-2-4 Main Menu List 7-18
7-2-5 Web UI Startup Procedure 7-21
7-2-6 Login 7-22
7-2-7 Logout 7-24
7-2-8 Precautions for Initial Login 7-24

7-3 CIP Safety Communications Settings 7-27
7-3-1 Connection Settings for CIP Safety Communications 7-27
7-3-2 Exporting and Importing the Settings of the Safety I/O Block 7-36

7-4 EtherNet/IP Communications Settings 7-38
7-4-1 Setting Tag Data Link Communications 7-38
7-4-2 LLDP Function 7-42

7-5 Safety Input Functions Settings 7-44
7-5-1 Setting Procedure for Safety Input Functions 7-44
7-5-2 Setting Procedure for Standard Output Functions 7-47

7-6 Setting Safety Output Functions 7-50
7-6-1 Safety Output Function Setting Procedure 7-50

7-7 Logic Function Settings 7-53
7-7-1 Logic Setting Procedure 7-53
7-7-2 Displaying the Parameter List 7-58
7-7-3 Examples of Abnormal Operations of Input Devices That Should Be Considered 7-59

7-8 Setting the Safety Signatures 7-63

7-9 Create the safety application file 7-65
7-9-1 Registration of Safety I/O Block 7-65
7-9-2 Safety Application Settings 7-66
7-9-3 Safety I/O Functions Settings 7-68
7-9-4 Logic Function Settings 7-68
7-9-5 Exporting a Safety Application File 7-68

7-10 Setting IP Addresses 7-71
7-10-1 IP Address Configuration 7-71
7-10-2 Selecting the Method to Set the IP Address Using the Rotary Switches 7-73
7-10-3 Setting by Sysmac Studio 7-74
7-10-4 Setting by Web UI 7-76

7-11 TUNID Settings 7-78
7-11-1 Purpose of TUNID 7-78
7-11-2 TUNID Setting Procedure 7-78

7-12 Selecting the Safety Application 7-83

7-13 Restart 7-84
7-13-1 Purpose of Restart 7-84
7-13-2 Procedure for Using Restart 7-84

7-14 Configuration 7-87
7-14-1 Configuring the Safety Controller 7-87
7-14-2 Configuration of Safety I/O Block 7-87

7-15 Setting the Automatic Clock Adjustment 7-91
7-15-1 Purpose of Automatic Clock Adjustment 7-91
7-15-2 Procedure for Using the Automatic Clock Adjustment 7-91

7-15-3 Details on Automatic Clock Adjustment 7-94
7-16 Changing the Operating Mode 7-95
7-16-1 Procedure for Using Change Operating Mode 7-95
7-17 Configuration Lock 7-99
7-17-1 Purpose of Configuration Lock 7-99
7-17-2 Procedure for Using the Configuration Lock 7-99
7-17-3 Details on Configuration Lock 7-103
7-18 Setting the Safety Password 7-104
7-18-1 Purpose of Safety Password 7-104
7-18-2 Procedure for Using Safety Password Setting 7-104
7-18-3 Details on Safety Password 7-106
7-19 Backup 7-108
7-19-1 Purpose of Backup 7-108
7-19-2 Procedure for Using Backup 7-108
7-19-3 Details on Backup 7-111

Section 8 Functions of Safety I/O Block

8-1 List of Functions 8-3
8-2 Clear All Memory Function 8-4
8-2-1 Purpose of Clear All Memory Function 8-4
8-2-2 Procedure for Using the Clear All Memory Function 8-4
8-2-3 Details on Clear All Memory Function 8-7
8-3 HTTPS Communications Function 8-8
8-3-1 Purpose of HTTPS Communications Function 8-8
8-3-2 Procedure for Using the HTTPS Communications Function 8-8
8-3-3 Details on HTTPS Communications Function 8-9
8-4 Device Level Ring (DLR) Function 8-10
8-4-1 Purpose of DLR Function 8-10
8-4-2 Procedure for Using the DLR Function 8-10
8-4-3 Details on DLR Function 8-10
8-5 Power OFF Function for Through-wiring Output 8-11
8-5-1 Purpose of Power OFF Function for Through-wiring Output 8-11
8-5-2 Procedure for Using the Power OFF Function for Through-wiring Output 8-11
8-6 I/O Wiring Checking Function 8-13
8-6-1 Purpose of I/O Wiring Checking Function 8-13
8-6-2 Operation of the I/O Wiring Checking Function 8-13
8-6-3 I/O Configuration Settings for I/O Wiring Checking Function 8-13
8-6-4 Procedure for Using I/O Wiring Checking Function 8-14
8-7 Send General CIP Command Function 8-15
8-7-1 Purpose of Send General CIP Command Function 8-15
8-7-2 Procedure for Using Send General CIP Command Function 8-15
8-8 Unit Identification Function 8-16
8-8-1 Purpose of Unit Identification Function 8-16
8-8-2 Procedure for Using the Unit Identification Function 8-16
8-8-3 Details on Unit Identification Function 8-18
8-9 IP Address Indication Function 8-19
8-9-1 Purpose of IP Address Indication Function 8-19
8-9-2 Procedure for Using the IP Address Indication Function 8-19
8-9-3 Details on IP Address Indication Function 8-19
8-10 Power Supply Monitor Function 8-22
8-10-1 Purpose of Power Supply Monitor Function 8-22
8-10-2 Procedure for Using the Power Supply Monitor Function 8-22
8-10-3 Details on Power Supply Monitor Function 8-24
8-11 I/O Monitor Function 8-27

8-11-1 Purpose of I/O Monitor Function 8-27
8-11-2 Procedure for Using the I/O Monitor Function 8-27

8-12 Contact Operation Count Monitor Function 8-29
8-12-1 Purpose of the Contact Operation Count Monitor Function 8-29
8-12-2 Procedure for Use with Safety Input Terminals 8-29
8-12-3 Procedure for Use with Safety Output Terminals 8-29

8-13 Communications Cable Diagnosis Function 8-31
8-13-1 Purpose of Communications Cable Diagnosis Function 8-31
8-13-2 Procedure for Using the Communications Cable Diagnosis Function 8-31
8-13-3 Details on Communications Cable Diagnosis Function 8-33

8-14 Firmware Update Function 8-35
8-14-1 Purpose of Firmware Update Function 8-35
8-14-2 Procedure for Using the Firmware Update Function 8-35
8-14-3 Details on Firmware Update Function 8-36

Section 9 Safety Response Performance

9-1 Safety Response Performance of Safety I/O Block 9-2
9-1-1 Calculating Safety Response Performance 9-2
9-1-2 Verifying Safety Response Performance 9-5

Section 10 Security Guidelines

10-1 Defense in Depth Provided by the Safety I/O Block 10-2
10-1-1 Operating Environment of the Safety I/O Block 10-2
10-1-2 Security Measures for the Technical Layer Using the Safety I/O Block 10-3

10-2 Security Functions of Safety I/O Block to Protect Assets 10-5
10-2-1 Protecting Data on Communication Lines 10-5
10-2-2 Blocking External Attacks on the Safety I/O Block 10-7
10-2-3 Preventing Unauthorized Operations on the Safety I/O Block 10-9
10-2-4 Preventing Tampering of the Assets of the Safety I/O Block 10-10
10-2-5 Protecting Safety Application Files and Backup Files 10-11
10-2-6 Preventing Repudiation 10-12

10-3 Applying Security Patches 10-13
10-3-1 Updating the Safety I/O Block 10-13
10-3-2 Updating the Sysmac Studio 10-13
10-3-3 Updating the OS of Your PC 10-13

10-4 Safely Disposing of Equipment 10-14
10-4-1 Erasing Your Assets in the Safety I/O Block 10-14

Section 11 Troubleshooting

11-1 Checking for Errors 11-2
11-1-1 How an Error Is Notified and What Information to Check 11-2
11-1-2 How to Check for Errors 11-2
11-1-3 Operating Status Monitor Function 11-3

11-2 Checking for Errors and Troubleshooting with the Event 11-6
11-2-1 Event Log Function 11-6
11-2-2 Checking Events Using Sysmac Studio 11-6
11-2-3 Checking Events Using the Web UI 11-9
11-2-4 Event Details and Troubleshooting 11-12

Section 12 Inspection and Maintenance

12-1 Cleaning and Inspection 12-2
12-1-1 Cleaning 12-2
12-1-2 Inspection Procedure 12-2

12-2 Replacing Units 12-4
12-2-1 Unit Replacement Precautions 12-4
12-2-2 Unit Replacement Using the Backup Function 12-4
12-2-3 Unit Replacement Without Using the Backup Function 12-5

Appendices

A-1 Dimensions A-2

A-2 Safety I/O Assembly Data A-4
A-2-1 Safety Input Assembly Data A-4
A-2-2 Safety Output Assembly Data A-6
A-2-3 Configuration Assembly Data A-7

A-3 I/O Assembly Ports and Corresponding Safety I/O Assembly Data Elements A-14

A-4 Supported CIP Objects A-16
A-4-1 Identity Object (Class ID: 01 Hex) A-17
A-4-2 Assembly Object (Class ID: 04 Hex) A-19
A-4-3 Unit Manager Object (Class ID: 380 Hex) A-22
A-4-4 Event History Log Object (Class ID: 34B Hex) A-27
A-4-5 Error Event Object (Class ID: 34C Hex) A-30
A-4-6 Safety Discrete Input Point (SDIP) Object (Class ID: 3D Hex) A-33
A-4-7 Safety Discrete Output Point (SDOP) Object (Class ID: 3B Hex) A-35
A-4-8 Device Level Ring (DLR) Object (Class ID: 47 Hex) A-37
A-4-9 QoS Object (Class ID: 48 Hex) A-39
A-4-10 TCP/IP Interface Object (Class ID: F5 Hex) A-41
A-4-11 Ethernet Link Object (Class ID: F6 Hex) A-45
A-4-12 LLDP Management Object (Class ID: 109 Hex) A-51
A-4-13 LLDP Data Table Object (Class ID: 10A Hex) A-53
A-4-14 Logic Process Object (Class ID: 309 Hex) A-58

A-5 Declaration of Conformity A-60

Index

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.

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 Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety.
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

⚠ WARNING

During Power Supply

Do not touch the terminal section while power is ON.
Electric shock may occur.



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.



Fail-safe Measures

Provide safety measures in external circuits to ensure safety in the system if an abnormality occurs due to malfunction of the CPU Unit, other Units, or Slaves 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 CPU Unit turns OFF all outputs from Basic Output Units in the following cases. The Remote I/O Slaves operate according to the settings in the Slaves.

- If a power supply error occurs.
- If the power supply connection becomes faulty.
- If a CPU watchdog timer error or CPU reset occurs.
- If a Controller error of the major fault level occurs.
- While the CPU Unit is on standby until RUN mode is entered after the power is turned ON.

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



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.



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.



Power Supply Design

Follow the instructions in this manual to correctly perform power supply design and wiring. Inputting voltages or currents that are outside of the specified ranges, as well as incorrect wiring, may cause failure or fire.



CIP Safety Communications

Before installing the Safety I/O Block in a device or equipment or connecting it to the network, execute memory all clear to delete any setting data previously saved to the Safety I/O Block.
There is a risk of death due to personal injury in the worst case.



Before connecting the Safety I/O Block to the network, set the appropriate IP address and communications speed settings.
There is a risk of death due to personal injury in the worst case.



Confirm that the calculated reaction times meet the required specifications for all safety chains.
There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



If Open Type is set to “Open Only,” verify that the originator and target are configured correctly before use.
There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



When debugging the Safety I/O Block, verify that the Unit and connected external devices operate correctly in accordance with the operation programmed on the originator device.
There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



Before you start the system, perform user testing to check that the configuration data and operations of all devices are correct.
There is a risk of death due to personal injury in the worst case.



When safety devices with different SIL will coexist within a safety network, thoroughly evaluate the impact that this will have and confirm that the required safety level for the entire system can be ensured.
There is a risk of death due to personal injury in the worst case.



The SNN assigned to each safety network or safety subnet must be configured to be unique across the entire system.
There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



Check that the configuration data for the Safety I/O Block is downloaded correctly based on the information displayed in the Web UI.
There is a risk of death due to personal injury in the worst case.



When configuring using Type1 Safety Open, be sure to check that the ownership (CFUNID) assignment is configured correctly as part of the final verification process.
There is a risk of death due to personal injury in the worst case.



Be sure to download the connection data set for the originator and/or the configuration data of the target to the target, and perform testing and verification.
Check the SCID on the target only after testing and verification is completed.
There is a risk of death due to personal injury in the worst case.



Be sure to compare the SCID and configuration data transferred to the Safety I/O Block with the SCID and configuration data displayed and checked in the configuration tool at the time of configuration.
There is a risk of death due to personal injury in the worst case.



When replacing the Safety I/O Block, you must verify that the replacement device is correctly configured, and after the replacement, the user must personally verify the device's operation.
There is a risk of death due to personal injury in the worst case.



Be sure to fully test the operation of the corresponding device before locking the Safety I/O Block.
There is a risk of death due to personal injury in the worst case.



Grounding

Never ground the 24-V side. There is a risk that the safety functions may be lost due to shorting of the safety outputs.
There is a risk of death due to personal injury in the worst case.



Building the System

When building the system, observe the following warnings to ensure the integrity of the safety-related components.
There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



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 measures

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/TS 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 provided in Instruction Manual and User's 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



When Using the Safety I/O Block

Indicators are not reliable indications and are not guaranteed to provide accurate information. Use them only for general diagnostics during trial operation or troubleshooting. Do not use indicators as indications during operation.

There is a risk of death due to personal injury in the worst case.



Do not use non-safety signals, including explicit messages and exposed variables, as safety signals.

There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



Do not use the test outputs of the Unit as safety outputs.

There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



When using an intranet environment through a global address, connecting to an unauthorized terminal such as a SCADA or 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 yourself.



All safety devices and components that are connected to a 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.



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.



When a Unit is replaced, confirm that the model of the Unit, the Unit and connector mounting positions, and the Unit configuration and its operation are correct.



The power OFF function for through-wiring output is a non-safety function. Do not use it as a safety output. There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



When using a safety application function of the Unit, check that the rotary switch settings are correct and always confirm operation on the actual equipment before you operate the equipment.
There is a risk that the safety functions may be lost, which could lead to death due to personal injury in the worst case.



Always confirm safety at the destination before you transfer the Unit configuration information, parameters, set values, or other data from the Sysmac Studio or other Support Software. The devices or machines may operate unexpectedly, regardless of the operating mode of the Controller.



To prevent the configuration from being changed unintentionally, lock the configuration upon completion of safety validation.



When building a safety chain with single-channel outputs, only up to Safety Category 2/PLc can be achieved. If single-channel inputs and outputs are used, the requirements for the system must be met, including the safety category, PL constraints, and error detection. Build the system in accordance with these requirements and constraints.



When executing the following functions, always check that the area around the system is safe.

- Changing the operating mode of the corresponding Unit
- Setting/resetting of safety I/O contacts
- Forced refreshing of safety I/O contacts
- Changing present values of safety I/O data

The outputs may operate and may cause serious injury.



When restoring a Unit, check that the safety signatures of the restored programs are correct. Serious injury may possibly occur due to loss of required safety functions.



Lock the configuration upon completion of safety validation. If you change the rotary switches for the safety application and restart the power supply while the configuration is unlocked, the system will restart with a different safety configuration. Serious injury may possibly occur due to loss of required safety functions.



Before and during operation

There is a risk of death due to personal injury in the worst case.
Please conduct a risk assessment of the entire system yourself. Through risk assessment, ensure that the automatic operation state transitions after power-on do not result in dangerous conditions.
If the power-on mode is set to Executing, this product will automatically enter the operating state (Executing) after power-on or after configuration via Type1 Safety Open. The conditions under which the power-on mode becomes Executing are as follows:



- When using a fixed application.
- When designing the logic for an add-on application or user-defined application, if the power-on mode is set to Executing.

There is a risk of death due to personal injury in the worst case.
User-defined applications and add-on applications should be designed, tested, and verified in accordance with the Safety Integrity Level (SIL) requirements of your equipment.
Use Sysmac Studio to create an application file. Instructions on how to use Sysmac Studio can be found in this manual and*Sysmac Studio Version 1 Operation Manual (Cat. No. W504)*.



There is a risk of death due to personal injury in the worst case.
Please ensure that this product operates continuously for at least 8 hours.
This product may take up to 8 hours for some hardware self-diagnoses. If continuous operation lasts less than 8 hours, diagnostics for specific functions or areas may not be performed, potentially preventing the detection of faults occurring in those areas.



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 a SCADA or an unauthorized terminal such as an 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

Getting an IP Address

If you get an IP address from a DHCP server, make sure that the DHCP server is set as follows. Otherwise, the control system may operate unexpectedly.
- IP address allocation method: Static allocation
- Lease period: Infinite



During Power Supply and when Power Supply Is OFF

Do not touch the equipment during power supply and immediately after the power is turned OFF. Doing so may result in a burn.



Precautions for Safe Use

Transporting

- When transporting any Unit, use the special packing box for it.
  Also, do not subject the Unit to excessive vibration or shock during transportation.
- Do not drop any Unit or subject it to abnormal vibration or shock.
  There is a risk of Unit failure or malfunction.

Installation

- Before touching the product, be sure to first touch a grounded metal object in order to discharge any static build-up.
- Make sure that all of the mounting screws and switch cover screws of the product are tightened to the torque specified in this manual.

Mounting

- Make sure that the terminal blocks, communications cables, and other items with locking devices are properly locked into place.

Wiring

- Use cables, connectors, and waterproof covers that are specified in this manual.
- Make sure that all cable connector screws and waterproof cover screws are tightened to the torque specified in this manual.
- Double-check all switches and other settings and double-check all wiring 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.
- Do not pull on the cables or bend the cables beyond their natural limit.
- Do not place heavy objects or step on top of the cables.
- If the Unit is used in more than one system, be sure to keep a clearance of at least 5 mm between cables to prevent unstable operation due to interference. Do not bundle the cables together.
- Observe the following precautions when wiring the communications cables.
  a) Keep the communications cables away from power lines and high-voltage lines.
  b) Always lay communications cables inside ducts.
  c) Use the recommended communications cables that are specified in this manual.
  d) Connect both ends of communications cable shielded wires to the connector hoods.

Power Supply Design

- Use the power supply voltage that is specified in this manual.

- The maximum power supply current is 9 A, which is the sum of the Unit/input power supply current and the output power supply current. Do not use the Unit beyond the maximum power supply current. Otherwise, an excess current flows through the power supply cable, and it may cause fire.
- Inrush current may flow in the Unit/input power supply and output power supply in the following cases.
  a) When power is turned ON.
  b) When the power supply to connected external devices is started.
  c) When connected external devices are turned ON and OFF.

  In addition, overcurrent may flow until the protection is activated when there is a short-circuit in I/O cables. Consider these currents and select power supplies with sufficient extra capacity. The inrush current may prevent the power supply from operating correctly, or cause the power supply to turn OFF.

EtherNet/IP Communications

- Make sure that the communications distance, number of nodes connected, and method of connection for EtherNet/IP are within specifications.
- EtherNet/IP communications are not always established immediately after the power supply is turned ON. Use the CPU Unit system-defined variables or status in the user program to confirm that communications are established before attempting control operations.

Actual Operation

- Check the user program, data, and parameter settings for proper execution before you use them for actual operation.
- 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.

Turning OFF the Power Supply

- Turn OFF the external power supply to the Units and the power supply to the devices that communicate with the Unit before you wire the communications cables.
- Always turn OFF the external power supply to the Units before attempting any of the following.
  a) Assembling Units including the connected devices
  b) Setting the rotary switches
  c) Connecting or wiring cables
  d) Attaching or removing terminal blocks or connectors

Operation

- Confirm that the controlled system will not be adversely affected before you perform any of the following operations.
  a) Changing the operating mode of the CPU Unit (including changing the Startup Mode setting)

b) Changing the user program or settings

c) Changing set values or present values

d) Forced refreshing

- The CPU Unit refreshes I/O even when the operation is stopped (i.e., even in *PROGRAM* mode). Therefore, sufficiently confirm the safety before performing any of the following operations to change the data of output memory allocated to this product or the data of any memory allocated to Special I/O Units or CPU Bus Units. The load connected to this product or the Special I/O Units or CPU Bus Units may perform unexpected operation.

a) Transferring I/O memory data to the CPU Unit with a Programming Device (PC tool).

b) Changing present values in memory with a Programming Device.

c) Force-setting or force-resetting bits with a Programming Device.

d) Transferring I/O memory files from a memory card or EM file memory to the CPU Unit.

e) Transferring I/O memory from a host computer or from another PLC on a network.

Maintenance

- Do not use paint thinner when cleaning. Use commercially available alcohol.
- Do not use high-pressure cleaning.

Disposal

- Disposal of the product may be subject to regulations set by local authorities. Dispose of the product according to local ordinances as they apply.
- To prevent information leakage, delete all of the user data before disposal.

Precautions for Correct Use

Storage, Mounting, and Wiring

- Do not operate or store the Unit in the following locations. Doing so may result in operation stopping or a 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 acid, oil, or chemicals
  g) Locations where vibration or shock is directly transmitted to the Unit
  h) Locations close to power lines
- Take sufficient shielding measures when installing the Unit in the following locations.
  a) Locations subject to static electricity or other forms of noise
  b) Locations subject to strong electric fields or magnetic fields
  c) Locations where there is a risk of exposure to radiation
  d) Locations close to power supply lines
- Perform wiring correctly according to instructions in this manual.
- When you attach the switch cover, make sure that the packing is not twisted. Also confirm that there is no foreign matter adhering to the case and packing.
- Do not use the Unit continuously submerged in water.

Power Supply Design

Always use separate power supplies for the Unit/input power supply and the output power supply. If you supply power from the same power supply, load variations in output devices may cause malfunctions.

EtherNet/IP Communications

Do not disconnect the EtherNet/IP communications cables during operation. The outputs will become unstable.

Executing a Communication Cable Diagnosis

The communications are interrupted for the port with communications cable diagnosis running, and all connections (tag data links) and message communications via the port are stopped temporarily. Confirm that the system will not be adversely affected before you execute communications cable diagnosis.

Security Measures

For security purposes, we recommend that you set safety passwords for the Unit and project files. Keep the safety passwords under strict control to prevent them from being leaked. In particular, when transmitting safety password data over the Internet, implement measures such as using public key encryption to prevent interception.

Regulations and Standards

The NXR-S-seriesSafety I/O Block is certified for the following standards.

Certification body	Standards
TÜV Rheinland	• EN 61508 parts 1-3 • EN ISO 13849-1 • EN ISO 13849-2 • EN IEC 61131-2 • IEC 61326-3-1 • EN 60529 • EN 61131-6
UL	• NRAQ/NRAQ7 • UL 61010-1 and UL 61010-2-201 • CSA C22.2 No. 61010-1 and CSA C22.2 No. 61010-2-201 • FSPC (IEC 61508 parts 1-3 and ISO 13849-1)
ODVA	• CIP Safety on EtherNet/IP • EtherNet/IP

The NXR-S-seriesSafety I/O Block allows you to build a safety control system that meets the following standards.

- Requirements for SIL 3 (Safety Integrity Level 3) in IEC 61508 (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 Safety I/O Block is also registered for RCM, UKCA, and KC compliance.

Conformance to EU Directives and Regulations

Applicable Directives and Regulations

- EMC Directives 2014/30/EU
- Machinery Directive 2006/42/EC (Valid until 19.01.2027)
- Machinery Regulation (EU)2023/1230 (Valid from 20.01.2027)

Concepts

● EMC Directives 2014/30/EU

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 2006/42/EC, Machinery Regulation (EU)2023/1230

The Machinery Directive and the Machinery Regulation demand that the safety components that are used to provide safety for the relevant machinery are used according to the required levels of safety.
The applicable standard is EN ISO 13849-1.

● Conformance to EU Directives

The NXR-S-series complies with EU Directives. To ensure that the machine or device in which the product is used complies with EU Directives, the following precautions must be observed.

- You must use SELV power supplies for the DC power supplies that are connected as the Unit/input power supplies and output power supplies for the NXR-S-series.
  We recommend that you use the OMRON S8VK-S-series Power Supplies. EMC standard compliance was confirmed for the recommended Power Supplies.
- NXR-S-series products 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 NXR-S-series products are used complies with EU Directives.
- You must use power supplies with an output hold time of 10 ms or longer for the DC power supplies that are connected as the Unit/input power supplies and output power supplies for the NXR-S-series.
- 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 EU Directives was confirmed using power supply cables and I/O cables with a cable length of 30 m or shorter.

Conformance to EN ISO 13849-1

EN ISO 13849-1 requires that process controls be in place for the creation of safety-related software when building a safety control system. The process controls must ensure that the software is easy to read, understand, test, and maintain to avoid system failures during each phase (i.e., general software design, safety circuit system design, and software upgrades) of the software design lifecycle.
This means that process controls must also be in place for the design and development of safety software, such as for equipment and devices.
It is the customer's responsibility to conform with all 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_jp.html.

Conformance to UL and CSA Standards

Some NXR-S-series products comply with UL and CSA standards.

If you use a product that complies with UL or CSA standards and must apply those standards to your machinery or devices, refer to the *Instruction Sheet* that is provided with the product. The *Instruction Sheet* provides the application conditions for complying with the standards.

Conformance to Shipbuilding Standards

This product does not comply with any shipbuilding standards.

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.

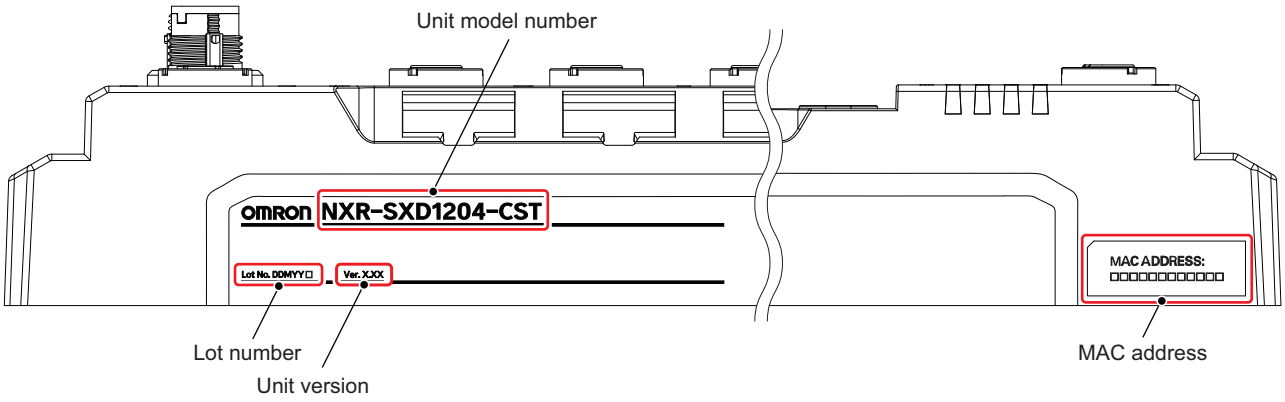
Unit Versions

Unit Versions

Unit versions are the revision numbers for the respective Units of the NXR-S-series. Even if Units are the same model, there will be some differences in functionality when the Unit version differs.

Notation of Unit Versions on Products

The *unit version* is given with the Unit specifications on the side of the Unit.



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	Gives 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)
MAC address	Shows the MAC addresses of the EtherNet/IP ports on the Unit.

Display in the Web UI

You can also use the production information display function of the Web UI to check the Unit version. The following are “Product Information Display Function” and “Product Information Screen” of the Web UI.

● Details on Production Information Display Function

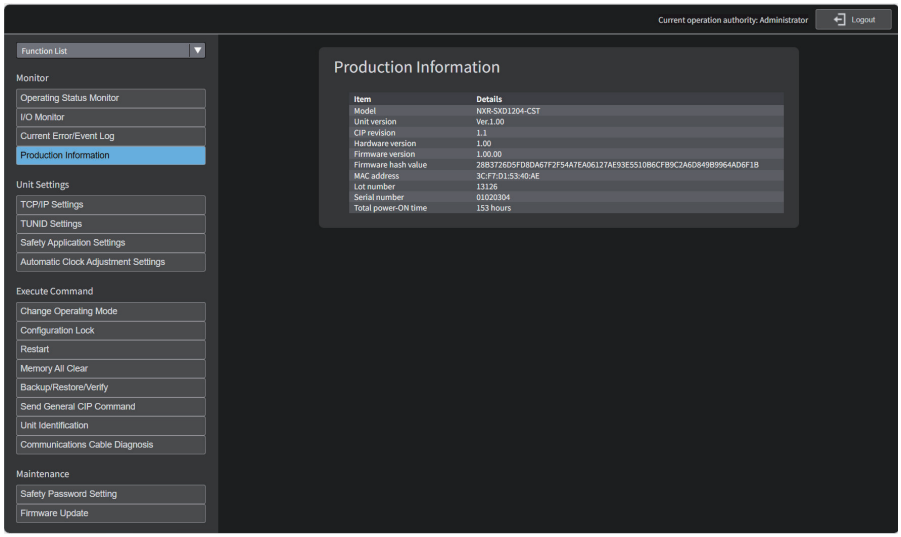
The production information display function displays the following information for the Safety I/O Block.

- Model
- Unit version
- CIP revision
- Hardware version

- Firmware version
- Firmware hash value
- MAC address
- Lot number
- Serial number
- Total power-ON time

Production Information Screen

The Production Information screen displays the Unit version and other production information for the corresponding Unit.



Related Manuals

The following table shows related manuals. Use these manuals for reference.

Manual name	Cat. No.	Model	Application	Description
Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety User's Manual (this manual)	W645	NXR-SXD1204-CST NXR-SXD1204B-CST	Learning how to use the Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety.	Describes the hardware, setup methods, and functions of the Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety.
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.
NX-series Safety Control Unit User's Manual	Z930	NX-SL□□□□ NX-SI□□□□ NX-SO□□□□	Learning how to use NX-series Safety Control Units.	Describes the hardware, setup methods, and functions of the NX-series Safety Control Units.
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.
NJ/NX-series CPU Unit Built-in EtherNet/IP™ Port User's Manual	W506	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Using the built-in EtherNet/IP port on an NJ/NX-series CPU Unit.	Information on the built-in EtherNet/IP port is provided. Information is provided on the basic setup, tag data links, and other features.
NY-series IPC Machine Controller Industrial Panel PC / Industrial Box PC Built-in EtherNet/IP™ Port User's Manual	W563	NY532-□□□□ NY512-□□□□	Using the built-in EtherNet/IP port in an NY-series Industrial PC.	Information on the built-in EtherNet/IP port is provided. Information is provided on the basic setup, tag data links, and other features.

Manual name	Cat. No.	Model	Application	Description
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.
Security Guideline for Factory Automation System	P162	-	Leaning concepts of security related to entire FA system.	Describes OMRON's security initiatives for its FA products and the security measures we would like customers to implement when using the FA products.
NJ/NX Controller Security Guideline	P166	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Learning about security measures using NJ/NX-series CPU Units.	Describes the security measures you can implement using NJ/NX-series CPU Units.
Environment-resistive IP67 Power Supply User's Manual	T245	S8NR-S□□□24	Learning how to use the Environment-resistive IP67 Power Supply.	Describes the functions, performance, and operating procedures of the Environment-resistive IP67 Power Supply.

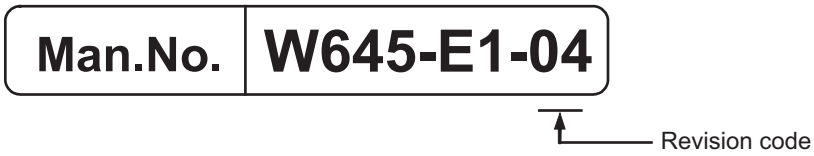
Terminology

Term	Description
CIP Safety originator	A role in CIP Safety communications. A CIP Safety originator manages a CIP Safety connection for a CIP Safety target. A CIP Safety originator exists in a connection unit, and not in a device unit.
CIP Safety connection	A safety I/O connection where the protocol for safety process data communications is CIP Safety. Depending on the role in communications, there are CIP Safety originator connections and CIP Safety target connections.
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. A CIP Safety target exists in a connection unit, and not in a device unit.
Device Level Ring (DLR)	A data-link layer protocol that provides single-fault tolerance defined by EtherNet/IP standards.
TUNID	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. A TUNID is a value totaling 10 bytes, consisting of a 6-byte Safety Network Number (SNN) and a 4-byte Node ID.
Assembly	A collection of the data held internally in a device. The data is gathered into one place for access from outside.
Add-on application	A safety application with logic assigned to a rotary switch number using the Web UI for this Unit.
Safety application	A safety application is an application for implementing safety control. In this manual, only a safety application that operates inside this Unit is referred to as a “safety application.” Four types of safety applications are discussed in this manual: fixed applications, add-on applications, user-defined applications, and remote I/O mode applications.
Simple logic mode	A mode to operate using the simple logical processing functions.
Simple logic mode application	An application that is used in simple logic mode. The I/O configuration settings and logic settings are defined. There are three types: fixed applications, add-on applications, and user-defined applications.
Fixed application	A safety application that is pre-installed in this Unit.
Connection	A logical communications path for performing communications between devices.
Configuration	The settings configured for the devices and network.
Single channel	One input or output is used as a point without redundancy.
Standard	*Standard* is the term used in this manual for devices, functions, and data that are used for general control purposes to differentiate from those that are designed with special safety measures for use in safety control.
Standard control	A type of control that uses devices, functions, and data that are designed for general control purposes. The term used to differentiate from a safety control.
Safety CPU Unit	A CPU Unit that is used for safety controls. A type of NX Unit.
Safety I/O Block	An I/O block that is used for safety controls.
Safety function	A function that is executed by the safety control system to achieve a safe state for a machine hazard.
Safety control	A type of control that uses devices, functions, and data which are designed with special safety measures.
Safety Control Unit	The generic term for an NX Unit that is used in safety controls.
Safety output device	An output device that is designed with special safety measures for use in safety controls. The generic term for devices such as safety relays.
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.
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.

Term	Description
Safety input device	An input device that is designed with special safety measures for use in safety controls. The generic term for devices such as emergency stop switches and safety door switches.
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 Network Controller	The generic term for building-block safety controllers that have a Safety Control Unit mounted to the NX-series Communication Control Unit.
Safety Network Number (SNN)	A number assigned to a safety network so that it can be uniquely identified for CIP Safety communications.
Safety programs	User programs for safety controllers. This term is used to differentiate from the user program of the standard controller.
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 switch, interruption of a light curtain, opening of a safety door, etc.) or device failure.
Safety validation	A check to confirm that the safety controls meet the required specifications of a safety system in safety validation testing. It may also be used to refer to the action of appending that confirmation information to the safety application data.
Communication Control Unit	The generic term for the interface units for the Safety CPU Unit and CIP Safety on EtherNet/IP device to have CIP Safety communications on a network.
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.
Dual channel	Two inputs or outputs are used as a pair of points for redundancy.
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.
Operating mode	Each status of operation of the Unit. The available functions differ depending on the operating mode.
Node ID	An ID assigned to each of the 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.
User-defined application	A safety application with logic to download to the Unit using the configuration in Type1 Safety Open. User-defined applications are created by users in Sysmac Studio.
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.
Remote I/O mode	A mode to operate as simple remote I/O without using the simple logical processing functions.
Remote I/O mode application	An application that is used in remote I/O mode. Only the I/O configuration settings are defined, and the logic is not included. The settings are configured for the Unit using Type1 Safety Open or the Web UI.
Ring supervisor	The ring supervisor is responsible for verifying the integrity of the ring. It reconfigures the ring to recover from faults and collects diagnostic information for the ring.

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	July 2026	Original production
02	July 2026	Made changes accompanying the addition of the power supply cables.
03	September 2026	• Made changes accompanying the addition of the IP65 protective structure specifications. • Made changes accompanying the application to the Mechinery Regulation.
04	October 2026	• Made changes accompanying the update of the Declaration of Conformity. • Corrected mistakes.

1

Features and System Configuration

This chapter describes the features and system configuration of the Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety.

1-1 Overview of Safety I/O Block 1-2

1-2 Features of Safety I/O Block 1-3

1-3 System Configuration 1-4

1-3-1 Safety Control System 1-4

1-3-2 Network Topology 1-13

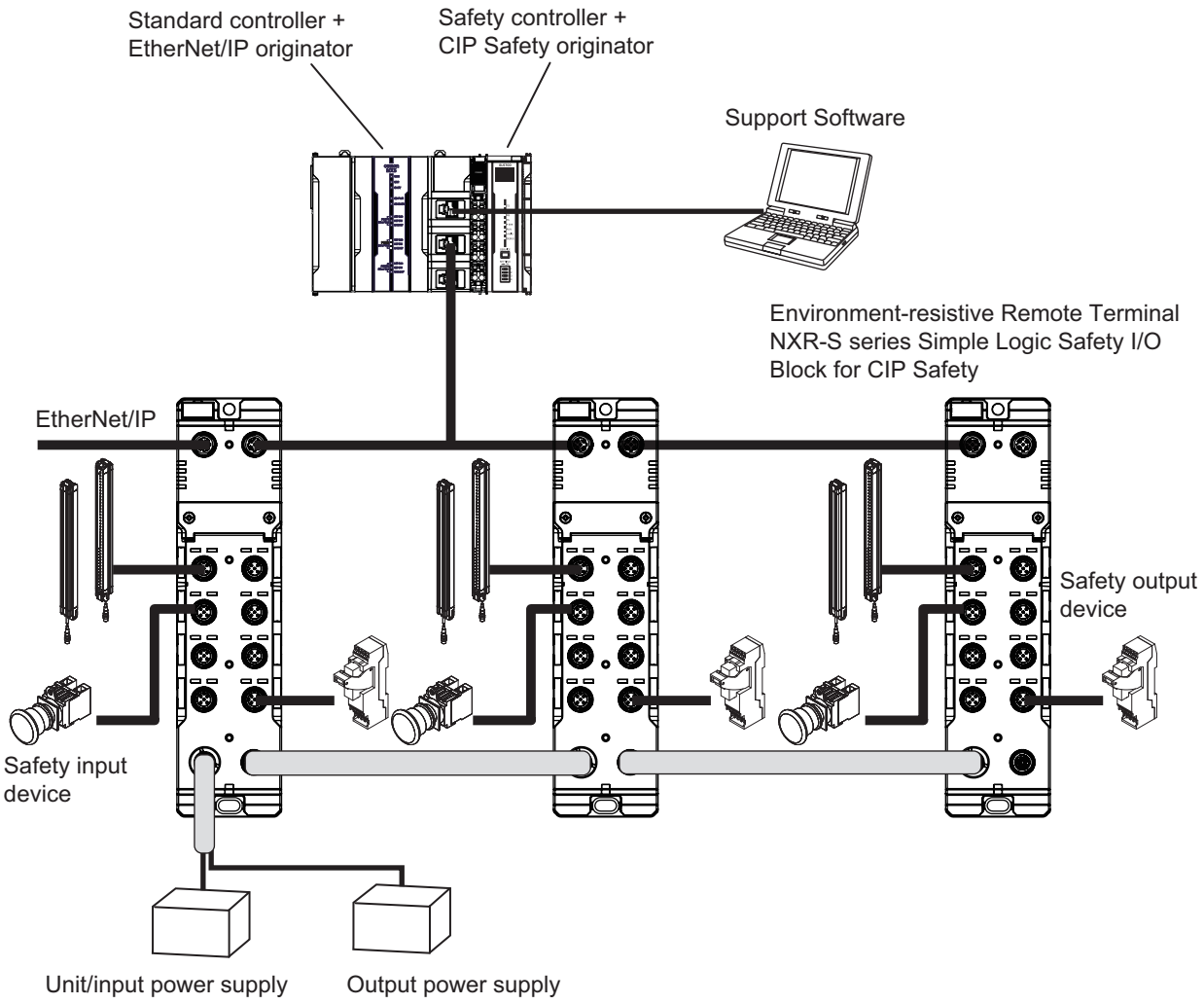
1-3-3 Cascade Connections 1-14

1-4 Support Software 1-16

1-1 Overview of Safety I/O Block

The Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety is a safety I/O device that has a CIP Safety target function as well as high ingress protection equivalent to IP65/IP67. In addition, it can control safety output devices by using a simple logic function.
The following functions are supported as basic functions.

- Performing safety communications with a CIP Safety originator as a CIP Safety target.
- Exchanging data with an EtherNet/IP originator as an EtherNet/IP target.
- Performing I/O processing with emergency stop switches, safety light curtains, and other safety devices.



1-2 Features of Safety I/O Block

This section describes the features of the Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety.

Simple Logic Function

The Safety I/O Block has a logic function to control safety output devices.
Therefore, simple control is achieved without any programming, and high-speed response safety control is possible using the Safety I/O Block alone.

Ingress Protection Equivalent to IP65/IP67

The Safety I/O Block has high ingress protection equivalent to IP65/IP67. Therefore, it can be installed outside the control panel even in an environment where it will be subject to water exposure or high dust levels.

Simple Wiring of Various Cables

Since the Safety I/O Block has connector connections for all ports, including for the power supply cable and communications cables, wiring is easier than for terminal block connections. Furthermore, all ports are equipped with Smartclick connectors, enabling easy one-touch connections.

Simple Unit Replacement

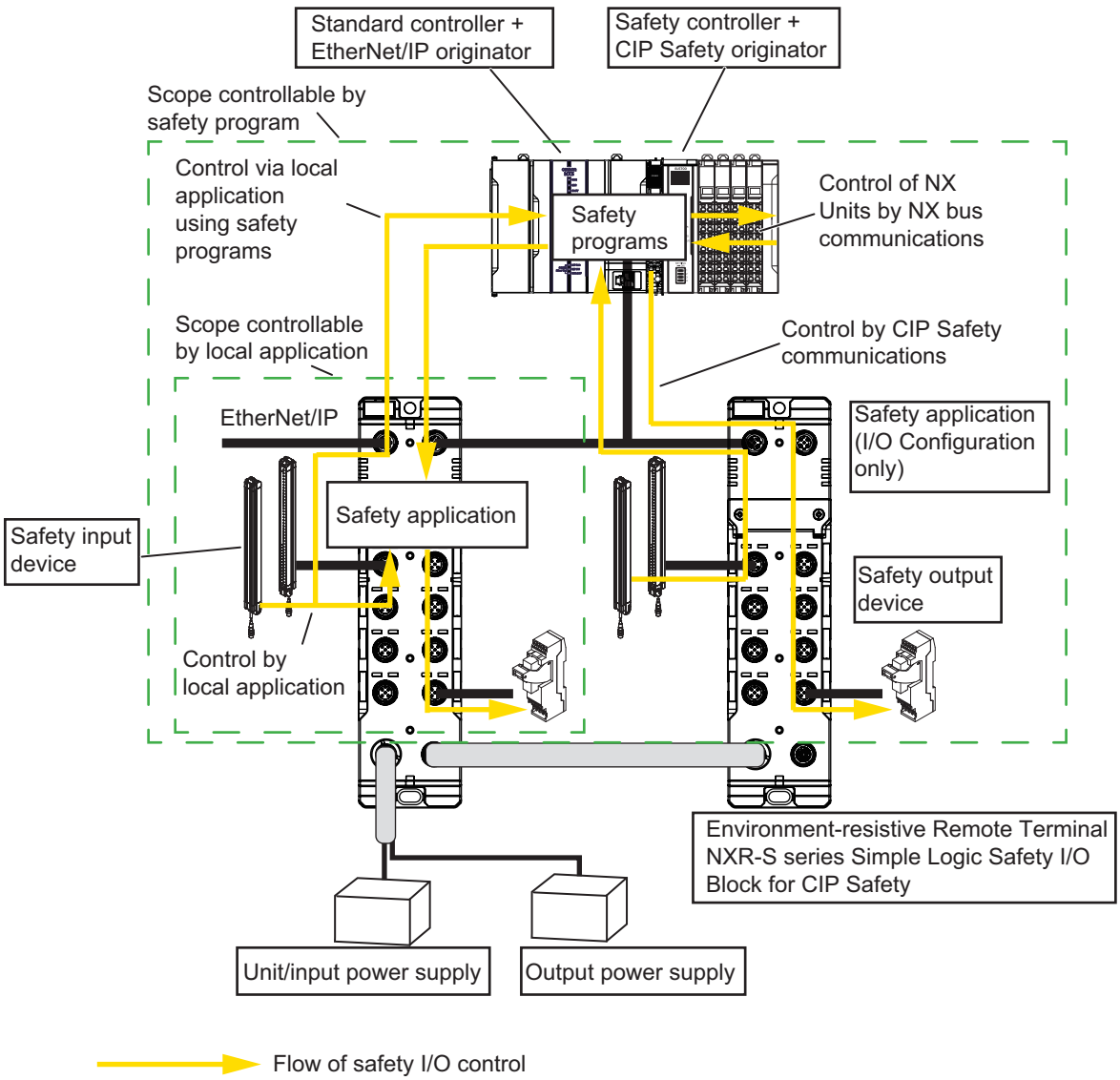
The Safety I/O Block includes a Web UI.
By using the Web UI, you can perform the backup, restoration, and other work necessary for I/O monitoring, troubleshooting, and restoration of the Safety I/O Block without using dedicated support software.

1-3 System Configuration

The system configuration when using the Safety I/O Block is called the safety control system.
This section describes the network topology when connecting the safety control system and Safety I/O Block to the same EtherNet/IP network as well as the cascade connections to connect the safety input ports and safety output ports of the Safety I/O Block.

1-3-1 Safety Control System

The following figure shows a safety control system using the Safety I/O Block.



The following table describes each configuration device.

Configuration device	Description
Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety NXR-SXD□□□□-CST	This product A device to exchange safety data with the CIP Safety originator. It outputs the data received from the CIP Safety originator to the safety output device, and transmits the input signals from the safety input device to the CIP Safety originator. In addition, it can also directly control safety output devices by using simple logic functions.
Standard controller + EtherNet/IP originator	Performs standard control of the Safety I/O Block. In addition, this device performs EtherNet/IP communications, and is used to monitor the operating status of the Safety I/O Block. OMRON products include the NX502 CPU Unit and NX102 CPU Unit. Furthermore, the NX-CSG320 is available as an OMRON EtherNet/IP originator.
Safety controller + CIP Safety originator	Performs CIP Safety communications with the Safety I/O Block, and controls the safety functions with safety programs. OMRON products include the NX-SL5□□□.
Safety program	A user program for safety control that is operated with a safety controller. It controls the entire safety control system through NX bus communications, CIP Safety communications, and other communications.
Local application	An application that is run on a remote device instead of the safety controller. With this product, it is referred to as a safety application and is implemented using safety I/O diagnostic functions and logic functions. The safety applications of the Safety I/O Block are categorized into two types: applications that contain only I/O configuration settings and applications that contain both logic settings and I/O configuration settings. Safety applications that have only I/O configuration settings are for using the Safety I/O Block as simple remote I/O, and safety control is implemented by a safety program of the safety controller. Conversely, safety applications that have both logic settings and I/O configuration settings are suitable for applications that require high-speed responses because local control is possible in the Safety I/O Block without going through a safety controller. In addition, control is also possible with a combination of the safety output data transmitted from the safety controller and the logic settings of the safety application.
Unit/input power supply	A power supply used for operation of the Safety I/O Block and for interfacing with safety input devices. Supply power by connecting an external power supply to the power supply connector (input).
Output power supply	A power supply used for interfacing with safety output devices. Supply power by connecting an external power supply to the power supply connector (input).
Safety input device	An input device that is designed with special safety measures for use in safety controls. The generic term for devices such as emergency stop switches and safety door switches.
Safety output device	An output device that is designed with special safety measures for use in safety controls. The generic term for devices such as safety relays.

When broken down into types, there are the following four types of safety control system depending on the applications and programs used. Select based on the features.

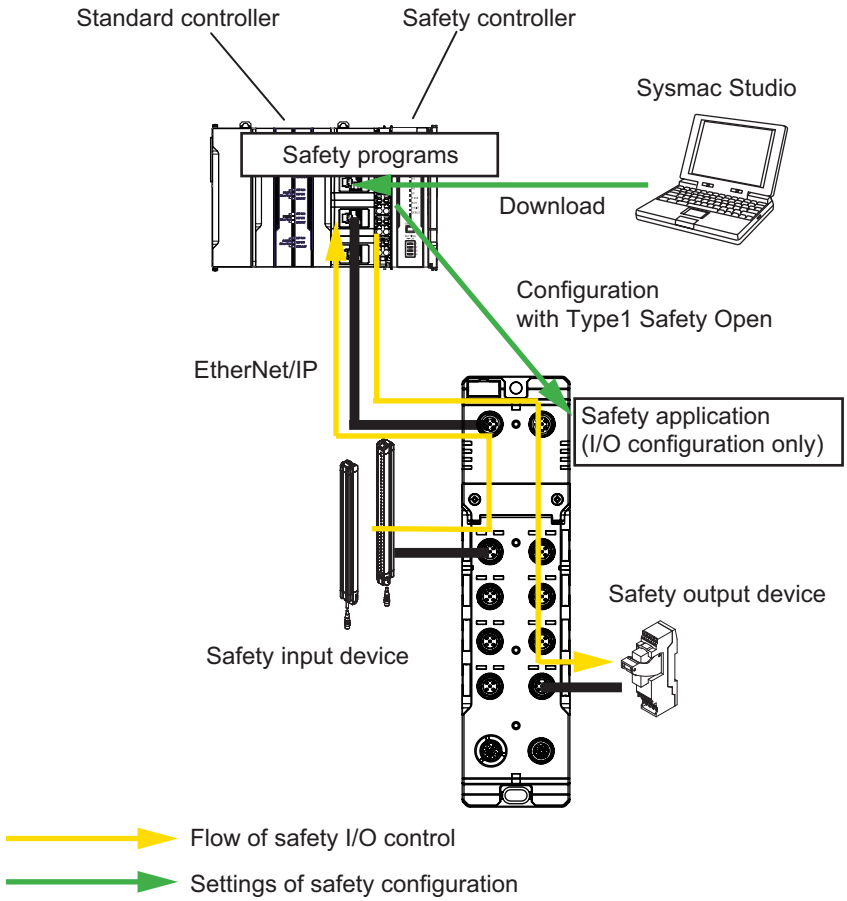
Safety control system configuration	Safety application to use	Features	Method to set and change safety application	Selection criteria
Configuration for the safety controller to perform control	Remote I/O mode application	• The safety controller controls safety output devices via a network. • A complicated, large-scale system can be built using network communications. • The response time may become long.	• A safety application with only I/O configuration settings is designed, and downloaded to the safety controller. In this case, the safety controller configures the Safety I/O Block based on the downloaded safety application (configuration using Type 1 Safety Open). • Alternatively, a safety application with only I/O configuration settings designed by a user is downloaded to the Safety I/O Block (configuration using the Web UI).	• Wish to build a complicated, large-scale system that is difficult to implement with the logic function of the Safety I/O Block. • A safety program is used with a safety controller.
Configuration for the Safety I/O Block to perform control using a preset safety application	Fixed application	• The Safety I/O Block controls the safety output device. • A system for small-scale control by simple logic. • High-speed responses are possible.	• A safety application (fixed application) preset in the Safety I/O Block is used.	• There are applications that can be used as-is among the fixed applications.

Safety control system configuration	Safety application to use	Features	Method to set and change safety application	Selection criteria
Configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user	User-defined application	• The Safety I/O Block controls the safety output device. • Since the user designs the logic, control with greater flexibility than a preset safety application is possible. Systems such as the following can be built. a) Control using a combination of control performed via a network using a safety program and high-response control performed locally using a safety application. b) Local control using a safety application design by a user. c) Control with the Safety I/O Block connected in cascade to expand the number of control points.	• A safety application containing logic settings and I/O configuration settings (user-defined application) is designed, and downloaded to the safety controller. • The safety controller configures the Safety I/O Block based on the downloaded safety application (configuration using Type 1 Safety Open).	• This is an application that can be implemented with the logic function of the Safety I/O Block for simple processing. • There are no applications that can be used as-is among the fixed applications. • Wish to manage a safety application on the safety controller side to perform the same processing on multiple Safety I/O Block units.
Configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user	Add-on application		• A safety application (add-on application) containing logic settings and I/O configuration settings is designed, and downloaded to the Safety I/O Block (configuration using the Web UI). • Up to five types of add-on application can be saved to the Safety I/O Block, and the safety application is selected from them.	• This is an application that can be implemented with the logic function of the Safety I/O Block for simple processing. • There are no applications that can be used as-is among the fixed applications. • Wish to manage a safety application on the Safety I/O Block side to use a single Safety I/O Block alone.

A configuration example and operation details for each of the safety control systems are shown below.

Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)

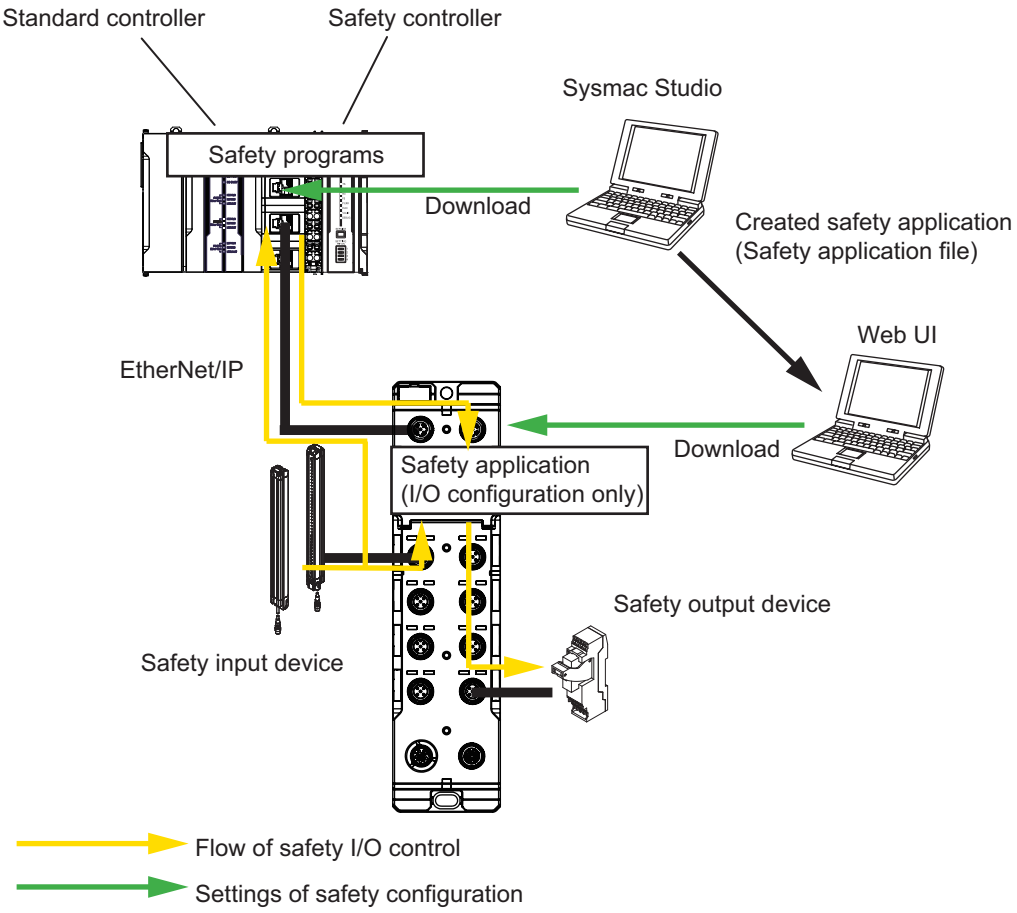
The following shows a figure of the configuration for the safety controller to perform control (configuration using Type 1 Safety Open).



- Control is performed with the safety program of the safety controller.
- A safety application with only I/O configuration settings is used for the Safety I/O Block. The logic functions are not used.
- The safety application resides together with the safety program in the safety controller, and is sent to the Safety I/O Block when a connection is opened.
- Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to *0*.

Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI)

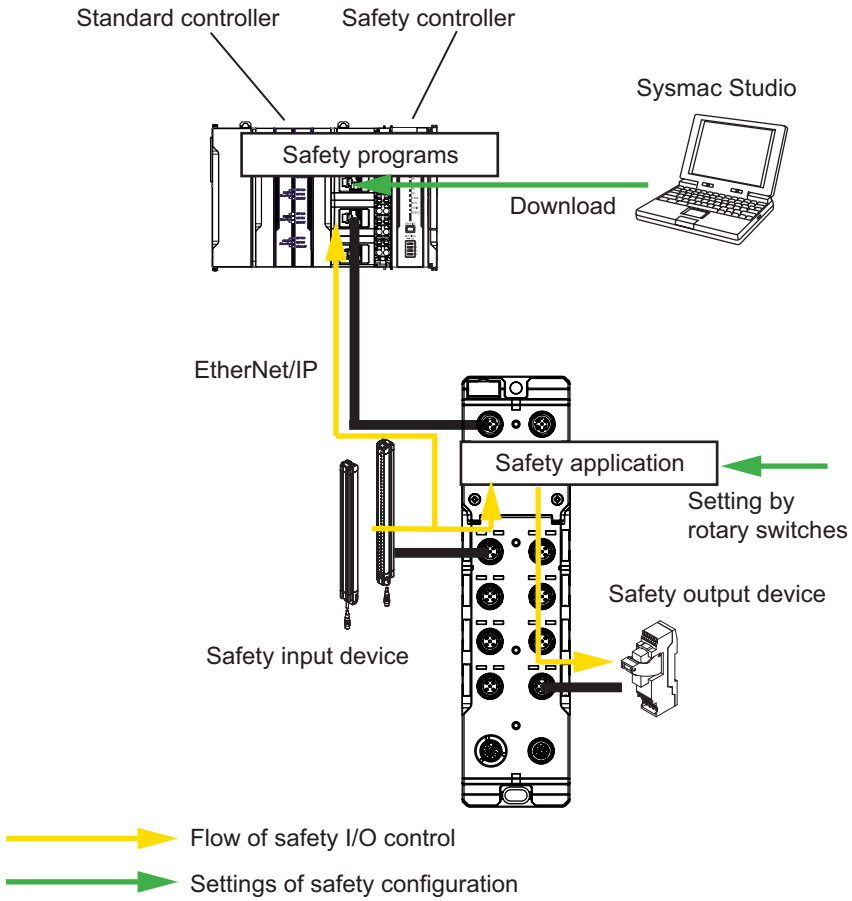
The following shows a figure of the configuration for the safety controller to perform control (configuration using the Web UI).



- Control is performed with the safety program of the safety controller.
- The safety controller opens a Type 2a Safety Open connection to the Safety I/O Block.
- A safety application with only I/O configuration settings is used for the Safety I/O Block. The logic functions are not used.
- The safety program resides in the safety controller. The safety application is created in Sysmac Studio, and the Web UI is used to download it to the Safety I/O Block.
- Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to *0*.

Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application

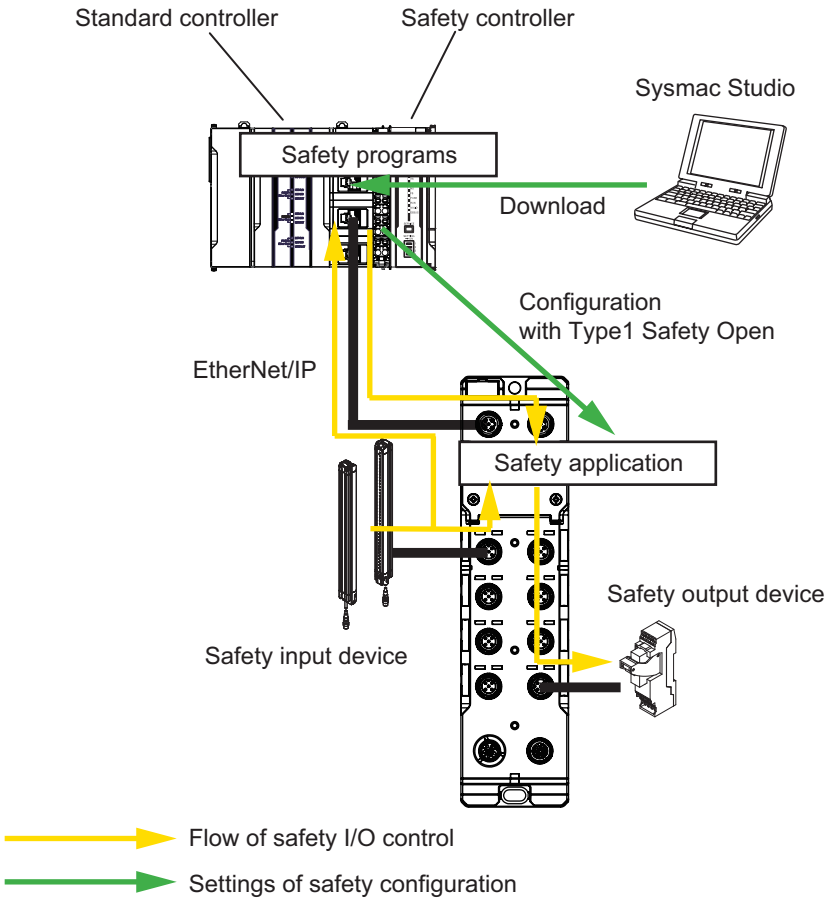
The following shows a figure of a configuration for the Safety I/O Block to perform control using a preset safety application.



- Use a safety application preset in the Safety I/O Block. A safety application contains logic settings and I/O configuration settings.
- Monitoring of the I/O data of the Safety I/O Block is also possible using a safety program of the safety controller.
- The safety application resides in the Safety I/O Block.
- Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to number *1-3* of the safety application (fixed application) to be used.

Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User

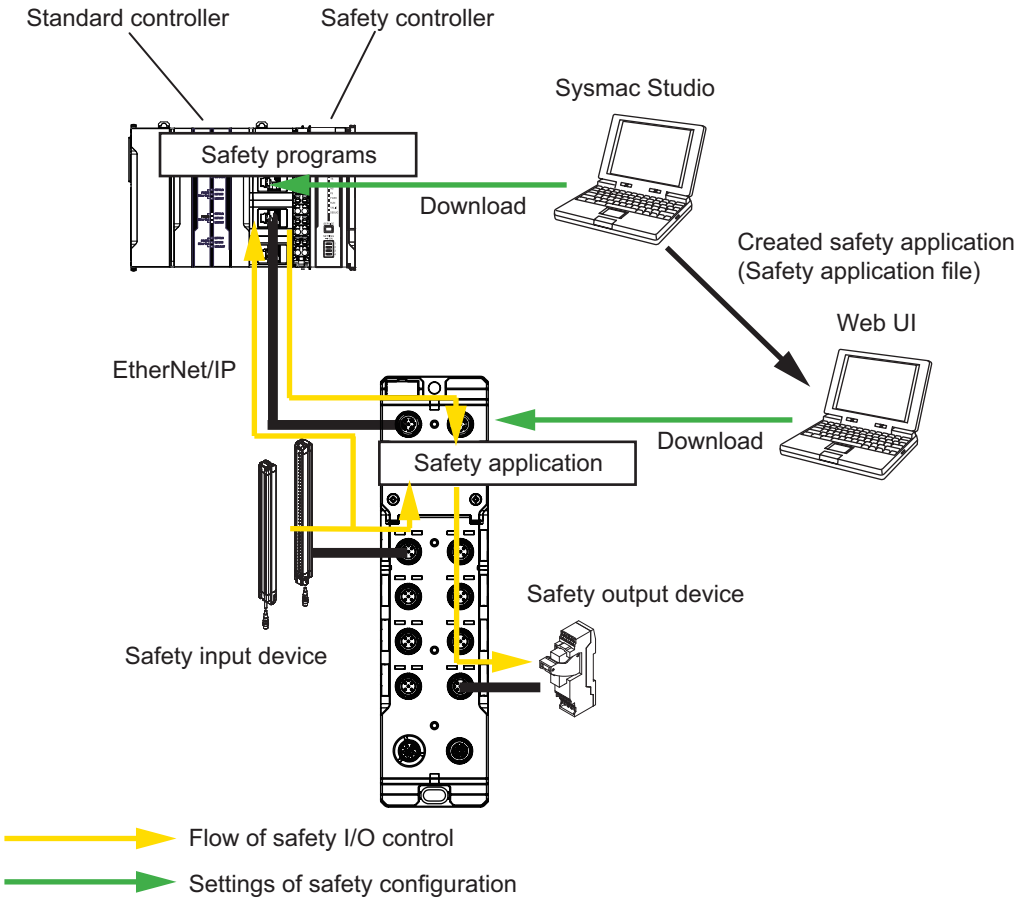
The following figure shows a configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user.



- The safety application of the Safety I/O Block is used to perform control. A safety application contains logic settings and I/O configuration settings.
- Control is also possible in combination with the safety program of the safety controller.
- The safety application resides together with the safety program in the safety controller, and is sent to the Safety I/O Block when a connection is opened.
- Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to *F* (user-defined application).

Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User

The following figure shows a configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user.



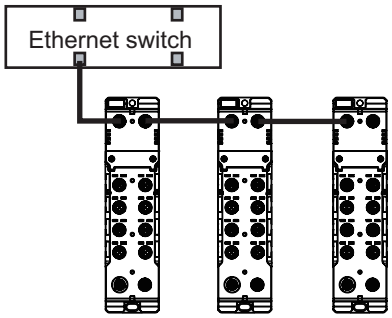
- The safety controller opens a Type 2a Safety Open connection to the Safety I/O Block.
- The safety application of the Safety I/O Block is used to perform control. A safety application contains logic settings and I/O configuration settings.
- Control is also possible in combination with the safety program of the safety controller.
- The safety program resides in the safety controller. The safety application is created in Sysmac Studio, and the Web UI is used to download it to the Safety I/O Block.
- Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to number *9-D* of the safety application (add-on application) to be used.

1-3-2 Network Topology

With the Safety I/O Block, you can configure various topologies, including line, star, tree, and ring topologies of the EtherNet/IP network, as the Unit has two communications ports.

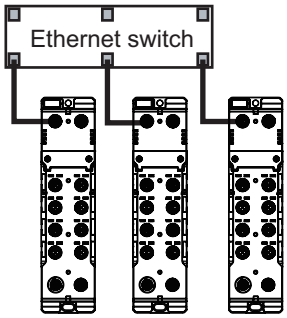
● Line

A line topology consists of more than one Safety I/O Block connected to each other.



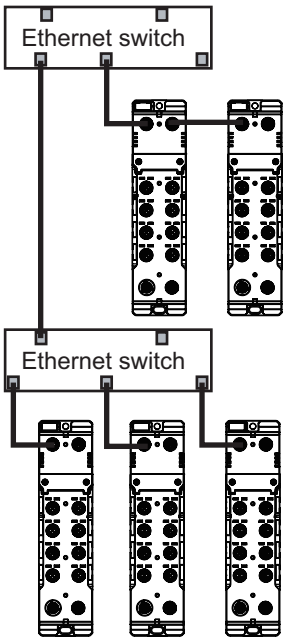
● Star

A start topology consists of more than one Safety I/O Block connected to an Ethernet switch.



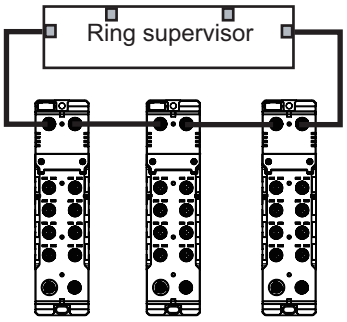
● Tree

A tree topology consists of a combination of star and line topologies.



- **Ring**

  A ring topology consists of a combination of a ring supervisor and the Safety I/O Block. A ring topology has the feature of being able to maintain normal communications even when there is a communications cable break in one place as it uses the Device Level Ring (DLR) function. Refer to *8-4 Device Level Ring (DLR) Function* on page 8-10 for details on the DLR function.



1-3-3 Cascade Connections

In the case of the NXR-SXD1204-CST, the safety input ports and safety output ports of multiple Units can be connected in cascade.
This configuration has the following advantages.

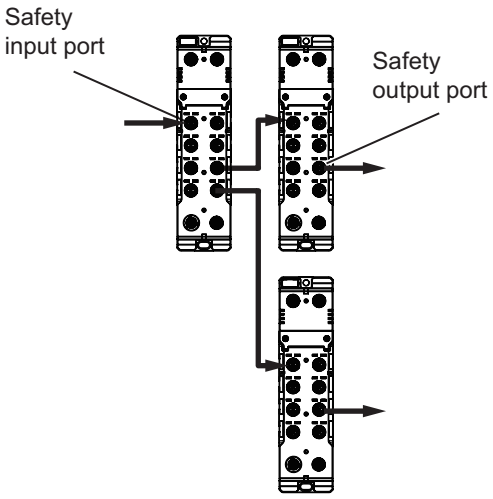
- Complicated logic can be implemented because the communications time of the CIP Safety communications has no impact.
- The number of safety input terminals and safety output terminals can be increased.

Use dual channel for the I/O configuration settings of the safety intput function and the safety output function.

Precautions for Correct Use

When using a cascade connection, check the safety response performance. Refer to *Section 9 Safety Response Performance* on page 9-1 for details on the safety response performance.

A one-stage cascade connection is supported, and up to three Units can be connected as shown in the figure below.
With a cascade connection, CIP Safety communications with the CIP Safety originator can be performed by all Units.



1-4 Support Software

The following table shows the support software that you can use with the Safety I/O Block.

Setting target	Model	Support software
Safety I/O Block	• NXR-SXD1204-CST • NXR-SXD1204B-CST	• Sysmac Studio version 1.67 or higher

Precautions for Correct Use

Setting using Sysmac Studio is performed via the NJ/NX-series CPU Unit, NY-series Industrial Panel PC/Industrial Box PC, or Communication Control Unit NX-CSG320. Use a direct Ethernet connection or an Ethernet hub connection as the connection method.

2

Specifications and Application Procedures

This chapter describes the specifications and application procedures for the Safety I/O Block.

2-1 Specifications 2-2
2-1-1 General Specifications 2-2
2-1-2 Communications Specifications 2-3
2-1-3 Safety Specifications 2-4
2-1-4 Unit Specifications 2-6

2-2 Usage Procedures 2-9
2-2-1 Step 1. System Design 2-9
2-2-2 Step 2. Software Design 2-9
2-2-3 Step 3. Hardware Design 2-10
2-2-4 Step 4. Calculating and Verifying Safety Response Performance 2-10
2-2-5 Step 5. Software Settings and Programming 2-11
2-2-6 Step 6. Installation and Wiring 2-11
2-2-7 Step 7. Checking Operation 2-12
2-2-8 Step 8. Operation, Maintenance, and Inspection 2-13

2-1 Specifications

This section describes the following specifications of the Safety I/O Block.

- General specifications
- Communications specifications
- Unit specifications
- Safety specifications

2-1-1 General Specifications

The general specifications of the Safety I/O Block are as follows.

Item		Specifications
Degree of protection		IP65 and IP67
Operating environment	**Ambient operating temperature**	-10 to 55°C
	Ambient operating humidity	25% to 85% (with no condensation)
	Atmosphere	Must be free from corrosive gases.
	Storage temperature	-25 to 65°C
	Storage humidity	25% to 85% (with no condensation)
	Altitude	2,000 m max.
	Pollution degree	3 or less: Conforms to IEC 61010-2-201
	Noise immunity	Conforms to IEC 61131-2 (Zone B) and EN 61131-2 (Zone B) Conforms to IEC 61326-3-1 and EN 61326-3-1
	Overvoltage category	Category II: Conforms to 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, and 10 m/s^2 100 min each in X, Y, and Z directions Other 10 to 60 Hz with amplitude of 0.35 mm, 60 to 150 Hz, and 50 m/s^2 80 min each in X, Y, and Z directions
	Shock resistance	Conforms to IEC 60068-2-27 150 m/s^2, 3 times each in 6 directions along X, Y, and Z axes
	Dielectric strength	600 VAC (between isolated circuits)
	Insulation resistance	20 MΩ min. (between isolated circuits)

Item		Specifications
Conformance to standards	**TÜV Rheinland**	• EN 61508 parts 1-3 • EN ISO 13849-1 • EN ISO 13849-2 • EN IEC 61131-2 • IEC 61326-3-1 • EN 60529 • EN 61131-6
	UL	• NRAQ/NRAQ7 • UL 61010-1 and UL 61010-2-201 • CSA C22.2 No. 61010-1 and CSA C22.2 No. 61010-2-201 • FSPC (IEC 61508 parts 1-3 and ISO 13849-1)
	ODVA	• CIP Safety on EtherNet/IP • EtherNet/IP
	Other	• EU: EN61131-2, RCM • UKCA • KC: KC Registration • Machinery Directive • Machinery Regulation

Note Refer to the OMRON website (www.ia.omron.com) or ask your OMRON representative for the most recent applicable standards.

2-1-2 Communications Specifications

The communications specifications of the Safety I/O Block are as follows.

Item		Specifications
Physical specifications	**Port**	Layer-2 switch port
	Physical layer	10BASE-T/100BASE-TX Auto negotiation or fixed settings
	Media access method	CSMA/CD
	Modulation	Baseband
	Topology	Line, star, tree, ring
	Baud rate	100 Mbps (100BASE-TX)
	Transmission media	Category 5 or higher twisted-pair cable (Recommended cable: double-shielded cable with aluminum tape and braiding)
	Transmission distance	100 m or less (Distance between nodes and between hub and node)
	Number of Units connectable per line	50

Item		Specifications
CIP Safety	**CIP Safety target**	Possible
	Maximum number of connections	5 (Input 2/Output 3) Input connections can share the same data with up to 8 CIP Safety originators by using Multicast communication.
	Packet interval	5 - 500 ms
	Maximum data size	Input: 9 bytes Output: 3 bytes
EtherNet/IP communications	**EtherNet/IP target**	Possible (Exclusive Owner, Input Only, Listen Only)
	Maximum number of connections	2 (Input 2/Output 0) Input connections can share the same data with EtherNet/IP originators by using multicast communication.
	Packet interval	5 - 10,000 ms
	Maximum data size	Input: 9 bytes
	DLR	Ring nodes supported
	EtherNet/IP conformance test	Conforms to CT21
CIP message communications	**Protocol**	Class3/UCMM
	Maximum number of connections (Class 3)	5
	Data size	504 bytes
HTTPS communications	**TLS version**	TLS 1.2 is supported. TLS 1.0, TLS 1.1, and SSL are not supported.
	Authentication method	Server authentication (X.509) and session authentication by safety password

The following table shows the port number to use, whether a communications path encryption function is available, whether enabled or disabled by default, and whether switchable between enable and disable for each external interface.

External interface		Port number	Communications path encryption	Enabled/disabled by default	Whether enable/disable switchable
Ethernet port	**CIP Safety**	UDP/2222	No	Enabled	Not possible
	HTTPS	TCP/443	Yes	Enabled	Not possible
	SNTP	UDP/123	No	Disabled	Possible by Sysmac Studio, Web UI, and CIP message
	DHCP	UDP/68	No	Disabled	Possible by Sysmac Studio, Web UI, and CIP message
	EtherNet/IP	UDP/2222	No	Enabled	Not possible
	CIP messages	TCP/44818, UDP/44818	No	Enabled	Not possible
Rotary switch		Not applicable	Not applicable	Enabled	Not possible

2-1-3 Safety Specifications

The safety specifications of the Safety I/O Block are as follows:

Item	Specifications			
	Safety input		Safety output	
	Dual channel	Single channel	Dual channel	Single channel
PL	Up to PL e	Up to PL d*1	Up to PL e	Up to PL c*2
Category	Up to Cat.4	Up to Cat.2*1	Up to Cat.4	Up to Cat.2*2
$MTTF_D$	1428 years	100 years	1431 years	100 years
Mission Time	20 years	20 years	20 years	20 years
DCavg	98.61%	98.60%	98.60%	98.60%
SIL	Up to SIL 3	Up to SIL 2	Up to SIL 3	Up to SIL 1
PFH	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h

***1.** To achieve Cat.2/PLd with a single-channel safety input, ensure the safety control system incorporates a safety output function that meets the following requirements.

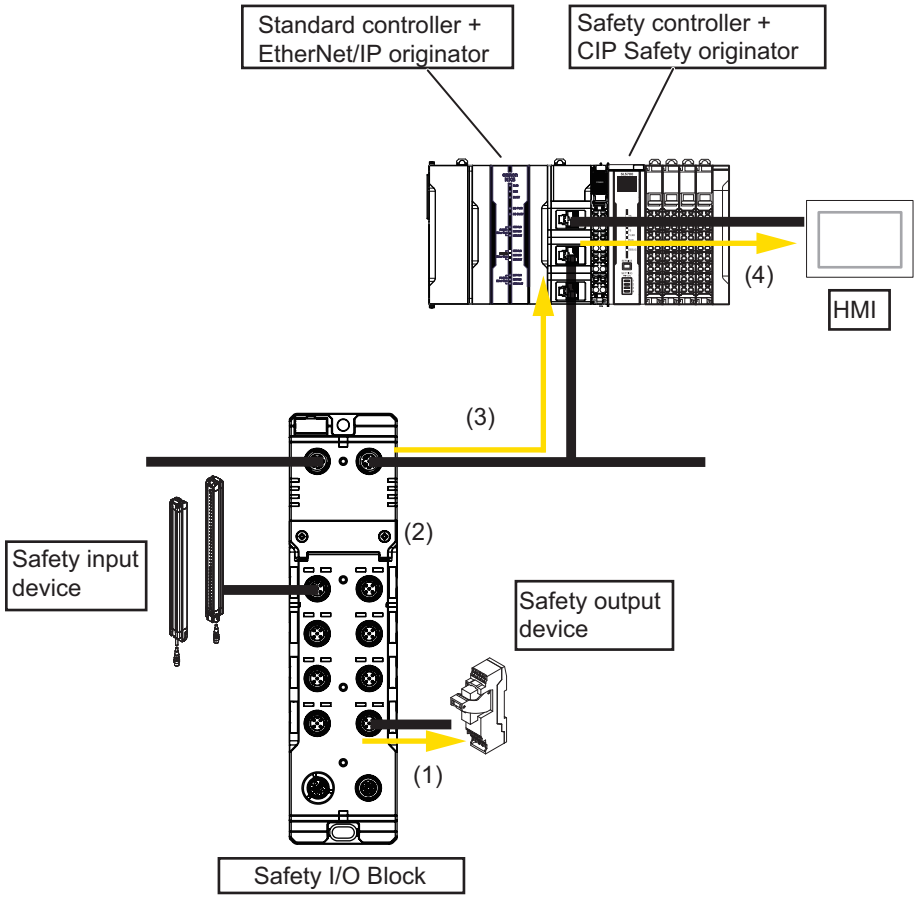
- When a failure occurs, the safety control system can transition to a safe state.
- When a failure occurs, the safety control system can maintain a safe state until the cause of the failure is cleared.

***2.** To achieve Cat.2/PLc with a single-channel safety output, detect failures of the safety output as a safety control system by using CIP Safety communications or EtherNet/IP communications to monitor the output terminal of the Safety I/O Block.
When a failure of a safety output is detected, notify the user of the error occurrence by indicator light, HMI, or other means.
The target of output terminal status monitoring must be one of the following four bit types of the input assembly.

Assembly	Monitoring target bit	Bit name
Safety Input 1	Output terminal status (aggregate)	Combined Safety Output Status
Safety Input 2	Output terminal status (aggregate)	Combined Safety Output Status
Safety Input 3	Output terminal status (aggregate)	Combined Safety Output Status
	Output terminal status (individual)	Safety Output0 Status to Safety Output3 Status

The procedure from an error occurring with a safety output terminal to notifying the user of the error occurrence is as follows.

1. An error occurs with a safety output terminal.
2. The Safety I/O Block detects the error of the safety output terminal and sets the safety output terminal where the error occurred to Inactive. In addition, it sets the bit of the target output terminal status to FALSE.
3. The safety controller or standard controller detects that the output terminal status of the Safety I/O Block has become FALSE.
4. The safety controller or standard controller notifies the user of the error occurrence by indicator light, HMI, or other means.



In addition, when the safety control system is switched to a safe status, shut off the power of the safety output device using a circuit breaker other than Safety I/O Block, based on the information given. The time until the power of the safety output device is shut off should be calculated as the sum of (the time until theSafety I/O Block indicates the occurrence of an error: 265 ms), (network reaction time) and (the response time of the shutoff device other than Safety I/O Block).
If the monitoring target bit is output terminal status (aggregate), the user must shut off the power of all safety output devices controlled by the Safety I/O Block. If the monitoring target bit is output terminal status (individual), the user must shut off the power of the safety output device where the error occurred.

2-1-4 Unit Specifications

The specifications of the Safety I/O Block Unit are as follows.

Item	Specifications	
	NXR-SXD1204-CST	NXR-SXD1204B-CST
Unit name	Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety	
Dimensions	60 (W) × 240 (H) × 34.2 (D) [mm] (60 (W) × 240 (H) × 46.65 (D) [mm] when the connectors are included)	
Mounting method	Mounting with M5 screws	
Mounting strength	100 N	
Mounting orientation and restrictions	Mounting orientation: 6 possible orientations Restrictions: No restrictions	
Available connectors	• EtherNet/IP communications connectors: M12 (D-coding, female) • Power supply connectors: M12 (L-coding, female), M12 (L-coding, male) • I/O connectors: M12 (A-coding, female)	

Item		Specifications	
		NXR-SXD1204-CST	NXR-SXD1204B-CST
Connector strength		30 N Applicable to all connectors	
Screw tightening torque		• EtherNet/IP communication connector and I/O connector (M12 screw): 0.5 to 0.6N·m*1 • Power supply connector (M12 screw): 0.39 to 0.49N·m*1 • Unit mounting (M5 screw): 1.47 to 1.96 N·m • Rotary switch cover (M3 screw): 0.4 to 0.6 N·m	
Weight		710 g	700 g
Unit/input power supply voltage		24 VDC (19.2 to 28.8 VDC)	
Output power supply voltage		24 VDC (19.2 to 28.8 VDC)	
Isolation method		Digital isolator isolation	
Isolation inside the Unit		Isolate between the Unit/input power supply and output power supply	
Insulation resistance		20 MΩ min. between isolated circuits (at 100 VDC)	
Maximum power supply current		9 A	
Current consumption		• Unit/Input power supply: 220mA • Output power supply: 40mA	
Number of safety I/O terminals	**Number of safety input terminals**	12	
	Number of test output terminals	12	
	Number of safety output terminals	4	
Number of I/O ports	**Safety input ports**	5-pin × 6 ports	5-pin × 4 ports
	Safety output ports	4-pin × 2 ports	0
	Safety I/O ports	0	8-pin × 2 ports
Number of terminals per I/O port	**Safety input ports**	• Safety inputs: 2 • Test outputs: 2 • Unit/input power supply: 1	
	Safety output ports	• Safety outputs: 2 • Output power supplies: 2	-
	Safety I/O ports	-	• Safety inputs: 2 • Test outputs: 2 • Safety outputs: 2 • Unit/input power supply: 1 • Output power supply: 1
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		0.7 A/point	
Test output ON residual voltage		1.2 V max. (Unit/input power supply + and each output terminal)	
Test output leakage current		0.1 mA max.	
Safety output internal I/O common		PNP (sourcing outputs)	
Safety output maximum load current		2.0 A/point and 9.0 A/Unit	0.7 A/point and 9.0 A/Unit

Item		Specifications	
		NXR-SXD1204-CST	NXR-SXD1204B-CST
Safety output ON residual voltage		1.2 V max. (between output power supply + and each output terminal)	
Safety output OFF residual voltage		2 V max. (between output power supply - and each output terminal)	
Safety application functions	**Without logic**	Remote I/O mode application	
	With logic	Fixed applications, user-defined applications, and add-on applications	

***1.** These values are for screw-type connectors. With Smartclick connectors, torque management is not required. Insert the connectors all the way in and then turn the approximately 1/8 of a turn.

2-2 Usage Procedures

This section describes the usage procedures of the Safety I/O Block.

2-2-1 Step 1. System Design

Step	Description	Reference
Step 1-1 Determining Safety Measures by Performing Risk Assessment	• Identify potential danger factors and perform risk assessment. • Study and decide measures to reduce risks.	-
Step 1-2 Selecting Safety Devices	Decide whether to use the Safety I/O Block. Furthermore, decide the model to use.	*2-1 Specifications* on page 2-2
Step 1-3 Selecting Network Devices	Confirm the communications topology and other specifications, and decide the Ethernet network configuration.	*1-3 System Configuration* on page 1-4
	Select Ethernet switches, twisted-pair cables, and communications connectors suitable for the specifications of the Safety I/O Block.	*5-5 Connected Devices* on page 5-29
Step 1-4 Designing the Interface between the Safety Controller and the Safety I/O Block	Design the interface between the safety controller and the Safety I/O Block.	*7-3 CIP Safety Communications Settings* on page 7-27
Step 1-5 Designing the Interface between the Standard Controller and the Safety I/O Block	Design the interface between the standard controller and the Safety I/O Block.	*7-4 EtherNet/IP Communications Settings* on page 7-38
Step 1-6 Designing Device Security	Configure the security settings of the equipment and facilities according to the security guidelines.	*Section 10 Security Guidelines* on page 10-1

2-2-2 Step 2. Software Design

Step	Description	Reference
Step 2-1 Designing I/O Devices and Processing	Design the following items for the Safety I/O Block. • Safety I/O devices to connect • Standard I/O devices to connect	*Section 6 Operation of the Safety I/O Block* on page 6-1

Step	Description	Reference
Step 2-2 Designing Program	**When configuration for a safety controller to perform control** Design the safety program for the safety controller	*NX-series Safety Control Unit/ Communication Control Unit User's Manual (Cat. No. Z395)*
	When configuration for the Safety I/O Block to perform control using a preset safety application • Use a fixed application as the safety application. • Determine the application to use from among the fixed applications.	*Fixed Applications* on page 6-24
	When configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user • Use a user-defined application as the safety application. • Design the logic of the user-defined application.	*User-defined Applications* on page 6-25
	When configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user • Use an add-on application designed by a user as the safety application. • Design the logic of the add-on application.	*Add-on Applications* on page 6-26

2-2-3 Step 3. Hardware Design

Step	Description	Reference
Step 3. Determining Wiring for Communications, Power Supply, and External I/O Devices	Determine the method to supply power to the Safety I/O Block.	*Section 4 Designing the Power Supply System* on page 4-1
	• Select a communications cable suitable for the specifications of the Safety I/O Block. • Calculate the power supply voltage and maximum current that will be supplied to the Safety I/O Block, and then select a power supply cable. • Select the I/O cables to connect between safety I/O devices.	*5-5 Connected Devices* on page 5-29

2-2-4 Step 4. Calculating and Verifying Safety Response Performance

Step	Description	Reference
Step 4-1 Calculating Safety Communications Performance	Verify the EPI, communications load, and safety task period of the safety controller based on the CIP Safety connection and tag data link connection determined in Step 1-4 and Step 1-5.	*Section 9 Safety Response Performance* on page 9-1 *Calculating Safety Reaction Times* in *NX-series Safety Control Unit/Communication Control Unit User's Manual (Cat. No. Z395)*



Step	Description	Reference
Step 4-2 Calculating Safety Reaction Times	Calculate the safety reaction times based on the I/O response times of the safety I/O devices and Safety I/O Block, and on the response times of the CIP Safety connection.	*Section 6 Operation of the Safety I/O Block* on page 6-1 *Section 9 Safety Response Performance* on page 9-1
⇩		
Step 4-3 Calculating Safety Distance and Verifying Fulfillment of Required Specifications	Calculate the safety distances using 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.	-

2-2-5 Step 5. Software Settings and Programming

Step	Description	Reference
Step 5-1 Creation of the Safety Network Controller System	Deploy the Safety I/O Block.	*CPU Rack Configurations and Setup* in the *NX-series Safety Control Unit/Communication Control Unit User's Manual (Cat. No. Z395)*
⇩		
Step 5-2 Communication Settings, Programming, and Assignment of Connected Devices to the Safety I/O Terminals	**When configuration for a safety controller to perform control** Refer to the reference on the right.	*7-1-1 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)* on page 7-3
	When configuration for the Safety I/O Block to perform control using a preset safety application Refer to the reference on the right.	*7-1-3 Setting Procedure of Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application* on page 7-9
	When configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user Refer to the reference on the right.	*7-1-4 Setting Procedure of Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 7-11
	When configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user Refer to the reference on the right.	*7-1-5 Setting Procedure of Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 7-14

2-2-6 Step 6. Installation and Wiring

Step	Description	Reference
Step 6-1 Installation	Secure the Safety I/O Block with screws using the mounting holes.	*5-1 Installing Units* on page 5-2

Step	Description	Reference
	Select the method to set the IP address using the rotary switches.	*7-10 Setting IP Addresses* on page 7-71
	Select the safety application using the rotary switches.	*3-3 Rotary Switches* on page 3-10
⇩		
Step 6-2 Wiring the Power Supply and I/O	Connect the power supply and I/O cables to the Safety I/O Block.	*5-3 Wiring the Power Supply* on page 5-12 *5-4 Wiring I/O Cables* on page 5-19
	Perform the wiring check of the I/O cables.	*8-6 I/O Wiring Checking Function* on page 8-13
⇩		
Step 6-3 Connecting the Ethernet Cables	Connect the communications cables to the Safety I/O Block.	*5-2 EtherNet/IP Network Wiring* on page 5-5
	Perform the wiring check of the communications cables.	*8-13 Communications Cable Diagnosis Function* on page 8-31

2-2-7 Step 7. Checking Operation

Step	Description	Reference
Step 7. Checking Operation	**When configuration for a safety controller to perform control** Refer to the reference on the right.	*7-1-1 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)* on page 7-3
	When configuration for the Safety I/O Block to perform control using a preset safety application Refer to the reference on the right.	*7-1-3 Setting Procedure of Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application* on page 7-9
	When configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user Refer to the reference on the right.	*7-1-4 Setting Procedure of Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 7-11
	When configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user Refer to the reference on the right.	*7-1-5 Setting Procedure of Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 7-14

2-2-8 Step 8. Operation, Maintenance, and Inspection

Step	Description	Reference
Step 8-1 Operation	Check that the operating mode transitions to *Executing* by setting the power-on mode or changing the operating mode.	*7-16 Changing the Operating Mode* on page 7-95
⇩		
Step 8-2 Troubleshooting Errors If They Occur	If an error occurs, use the indicator display and monitor function to check the error and determine the cause, and then remove the error.	*Section 11 Troubleshooting* on page 11-1
	Execute the power monitor function of the Safety I/O Block.	*8-10 Power Supply Monitor Function* on page 8-22
	Execute the Unit identification function of the Safety I/O Block.	*8-8 Unit Identification Function* on page 8-16
	Execute the IP address display function of the Safety I/O Block.	*8-9 IP Address Indication Function* on page 8-19
	Execute the communications cable diagnosis function of the Safety I/O Block.	*8-13 Communications Cable Diagnosis Function* on page 8-31
⇩		
Step 8-3 Inspection and Replacement	If the Safety I/O Block failed, replace it.	*Section 12 Inspection and Maintenance* on page 12-1
	If the Safety I/O Block was replaced, update the firmware.	*8-14 Firmware Update Function* on page 8-35

3

Part Names and Functions

This chapter provides the names and functions of the parts of the Safety I/O Block.

3-1 Parts and Names 3-2

3-2 Indicators 3-5

3-2-1 Status Indicators 3-5
3-2-2 I/O Indicators 3-8
3-2-3 Unit Identification Indicator 3-9

3-3 Rotary Switches 3-10

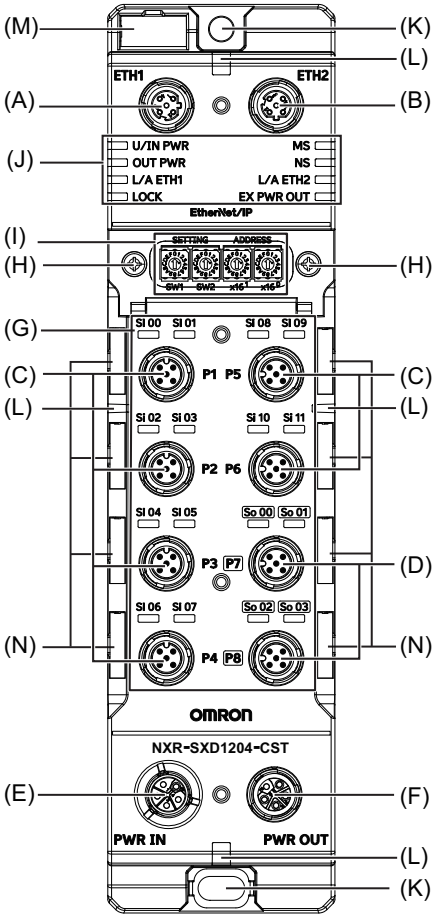
3-4 Connectors 3-11

3-4-1 EtherNet/IP Communications Connectors 3-11
3-4-2 Power Supply Connectors 3-11
3-4-3 I/O Connectors 3-12

3-1 Parts and Names

This section gives the names of the parts of the Safety I/O Block.

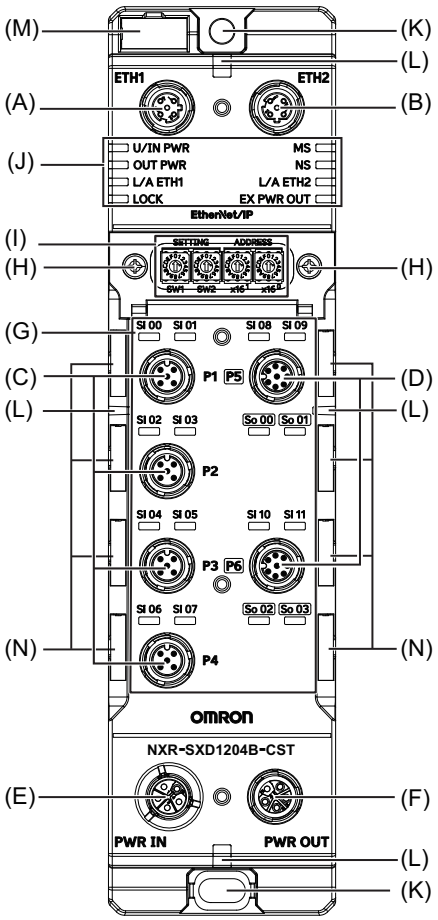
● NXR-SXD1204-CST



Letter	Name	Function
(A)	EtherNet/IP communications connector 1	The connector for EtherNet/IP port 1. The connector is an M12 connector (D-coding, female, Smartclick support). Connect a communications cable.
(B)	EtherNet/IP communications connector 2	The connector for EtherNet/IP port 2. The connector is an M12 connector (D-coding, female, Smartclick support). Connect a communications cable.
(C)	I/O connectors (for safety input ports)	These connectors are for connecting safety input devices. Affix removable makers to the sides of the I/O connectors. The connectors are M12 connectors (A-coding, female, 5-pin, Smartclick support). Connect I/O cables (5-wire).
(D)	I/O connectors (for safety output ports)	These connectors are for connecting safety output devices. Affix removable makers to the sides of the I/O connectors. The connectors are M12 connectors (A-coding, female, 5-pin, Smartclick support). Connect I/O cables (5-wire).

Letter	Name	Function
(E)	Power supply connector (input)	This connector is for supplying Unit/input power and output power. The connector is an M12 connector (L-coding, male, Smartclick support). Connect the power supply cable for connecting to an external power supply.
(F)	Power supply connector (output)	This connector is for supplying Unit/input power and output power from the local node to another node. Use this connector when the power supply method is power supply with through-wiring. The connector is an M12 connector (L-coding, female, Smartclick support).
(G)	I/O indicators	These indicators indicate the status of the safety input or safety output for the terminal of each port.
(H)	Cover mounting holes	These screw holes are for mounting the rotary switch cover. They are provided in two locations. The figure above shows the holes when the cover is mounted with screws.
(I)	Rotary switches	These switches are for selecting the safety application and setting the IP address.
(J)	Status indicators	These indicators indicate the current operating status of the Safety I/O Block.
(K)	Unit mounting holes	These holes are for mounting the Unit. They are provided in two locations. Mount the Unit with M5 screws.
(L)	Unit identification indicator	This indicator provides notification by illuminating when using the Unit identification function.
(M)	Unit identification marker	This marker is for identifying the Safety I/O Block. It is white.
(N)	I/O identification marker	This marker is for identifying the I/O terminal. It is white.

● NXR-SXD1204B-CST



Letter	Name	Function
(A)	EtherNet/IP communications connector 1	The connector for EtherNet/IP port 1. The connector is an M12 connector (D-coding, female, Smartclick support). Connect a communications cable.
(B)	EtherNet/IP communications connector 2	The connector for EtherNet/IP port 2. The connector is an M12 connector (D-coding, female, Smartclick support). Connect a communications cable.
(C)	I/O connectors (for safety input ports)	These connectors are for connecting safety input devices. Affix removable makers to the sides of the I/O connectors. The connectors are M12 connectors (A-coding, female, 5-pin, Smartclick support). Connect I/O cables (5-wire).
(D)	I/O connectors (for safety I/O ports)	These connectors are for connecting safety input devices and safety output devices. Affix removable makers to the sides of the I/O connectors. The connectors are M12 connectors (A-coding, female, 8-pin, Smartclick support). Connect I/O cables (8-wire).
(E)	Power supply connector (input)	This connector is for supplying Unit/input power and output power. The connector is an M12 connector (L-coding, male, Smartclick support). Connect the power supply cable for connecting to an external power supply.
(F)	Power supply connector (output)	This connector is for supplying Unit/input power and output power from the local node to another node. Use this connector when the power supply method is power supply with through-wiring. The connector is an M12 connector (L-coding, female, Smartclick support).
(G)	I/O indicators	These indicators indicate the status of the safety input or safety output for the terminal of each port.
(H)	Cover mounting holes	These screw holes are for mounting the rotary switch cover. They are provided in two locations. The figure above shows the holes when the cover is mounted with screws.
(I)	Rotary switches	These switches are for selecting the safety application and setting the IP address.
(J)	Status indicators	These indicators indicate the current operating status of the Safety I/O Block.
(K)	Unit mounting holes	These holes are for mounting the Unit. They are provided in two locations. Mount the Unit with M5 screws.
(L)	Unit identification indicator	This indicator provides notification by illuminating when using the Unit identification function.
(M)	Unit identification marker	This marker is for identifying the Safety I/O Block. It is white.
(N)	I/O identification marker	This marker is for identifying the I/O terminal. It is white.

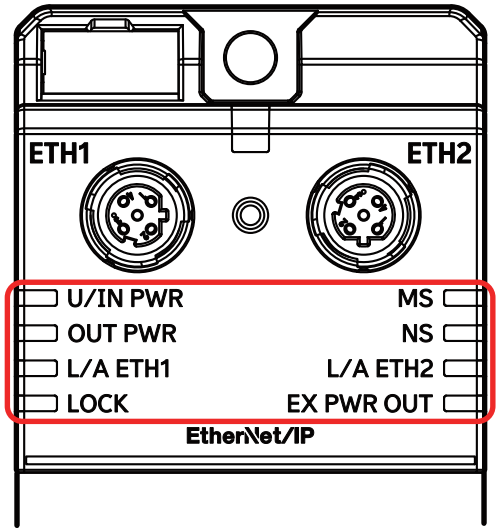
3-2 Indicators

The Safety I/O Block has the following indicators. This section describes them.

- Status Indicators
- I/O indicators
- Unit identification indicator

3-2-1 Status Indicators

These indicators indicate the current operating status of the Safety I/O Block.



U/IN PWR Indicator

This indicator shows the status of the Unit/input power supply.

Color	Status		Description
Green		Lit	The Unit/input power is supplied.
–		Not lit	The Unit/input power is not supplied.

OUT PWR Indicator

This indicator shows the status of the output power supply.

Color	Status		Description
Green		Lit	The output power is supplied.
–		Not lit	The output power is not supplied.

MS Indicator

This is the module status indicator. It shows the operating status of the Unit.

Color	Status		Description
Green		Lit	Normal operating status (Executing)
		Flashing	Normal operation standby status (Idle)
Red		Lit	Critical error occurred (Critical Fault)
		Flashing	Operation stopped error (Abort) *1
Green/Red		Flashing	Initializing (Self-Testing), TUNID setting wait state (Waiting for TUNID), or configuration wait state (Configuring)
–		Not lit	IP address indication function executing (IP Address Display), I/O wiring check function executing (I/O Wiring Checking), or power supply is OFF

***1.** Refer to *11-2 Checking for Errors and Troubleshooting with the Event* on page 11-6 for details on errors.

NS Indicator

This is the network status indicator. It shows the communications status of the Safety I/O Block.

Color	Status		Description
Green		Lit	Connection established for one of CIP Safety, EtherNet/IP, and CIP message communications.
		Flashing	Connection not established for any of CIP Safety, EtherNet/IP, and CIP message communications.
Red		Lit	A critical fault that affects the network occurred. Example: IP address is duplicated.
		Flashing	A timeout error occurred with one of the connections in CIP Safety and EtherNet/IP communications.*1
–		Not lit	The IP address is not set or the power supply is OFF.

***1.** Refer to *11-2 Checking for Errors and Troubleshooting with the Event* on page 11-6 for details on errors.

L/A ETH1 Indicator

This is the Link/Activity indicator for EtherNet/IP port 1. It shows the linked status and communications status of EtherNet/IP port 1.

Color	Status		Description
Green		Lit	Link established
		Flashing	Link established and communications are active
–		Not lit	No link established

L/A ETH2 Indicator

The Link/Activity indicator for EtherNet/IP port 2. This indicator shows the linked status and communications status of EtherNet/IP port 2.

Color	Status		Description
Green		Lit	Link established
		Flashing	Link established and communications are active
–		Not lit	No link established

LOCK Indicator

This indicator shows the user authentication status for setting data of the Safety I/O Block. The user is recommended to set the configuration locked state for use after the application operation check.

Color	Status		Description
Yellow		Lit	Configuration locked
		Flashing	Configuration unlocked and can be locked
–		Not lit	Configuration unlocked and cannot be locked

EX PWR OUT Indicator

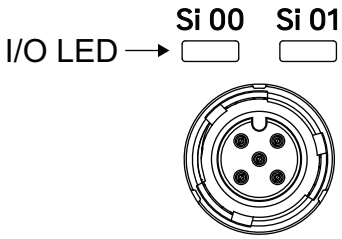
This indicator shows the status of the output power supply of the through-wiring.

Color	Status		Description
Green		Lit	The output power of the through-wiring is supplied.
–		Not lit	The output power of the through-wiring is not supplied.

3-2-2 I/O Indicators

The I/O indicators show the status of the safety input terminals and safety output terminals.

Example: Safety Input Indicator



Safety Input Indicator

This indicator shows the status of the safety input terminal.

Color	Status		Description
Yellow		Lit	The safety input terminal is ON (operating normally).
Red		Lit	One of the following errors was detected. • External Test Signal Failure at Safety Input • Internal Circuit Error at Safety Input • Discrepancy Error at Safety Input
		Flashing	• An error occurred in the safety input terminal for the other channel of the dual channels.
–		Not lit	The safety input terminal is OFF (operating normally).

Safety Output Indicator

This indicator shows the status of the safety output terminal.

Color	Status		Description
Yellow		Lit	The safety output terminal is ON (operating normally)
Red		Lit	One of the following errors was detected. • Short Circuit Detected at Safety Output • Stuck-at-high Detected at Safety Output • Internal Circuit Error at Safety Output • Data error between dual channel outputs*1 • EDM error*1
		Flashing	• An error occurred in another related safety output terminal.

Color	Status		Description
−	☐	Not lit	The safety output terminal is OFF (operating normally)

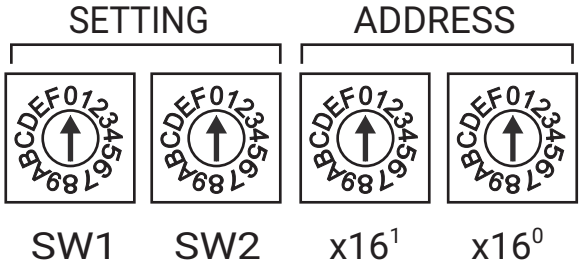
***1.** If the safety output terminals are set to Dual Channel Mode, the safety output indicators of both channels light in red when there is an EDM error or a data error between the dual channel outputs. If they are set to Single Channel Mode, the safety output indicator of only the corresponding channel lights in red for an EDM error.

3-2-3 Unit Identification Indicator

This is used by the Unit identification function and firmware update function.
Refer to *8-8 Unit Identification Function* on page 8-16 and *8-14 Firmware Update Function* on page 8-35 for details.

3-3 Rotary Switches

Configure the application settings and IP address settings with the rotary switches.



An overview is given below.

Rotary switch name	Description
SETTING*1	Select from safety application*2, IP address indication function*3, and I/O wiring checking function*4. Set both SW1 and SW2 to a value below. • *0*: Operates in remote I/O mode. • *1* to *3*: Operates with a fixed application. • *4* to *7*: Reserved • *8*: Operates with the IP address indication function. • *9* to *D*: Operates with an add-on application. • *E*: Operates with I/O wiring checking function. • *F*: Operates with a user-defined application.
ADDRESS*1	The pair of switches represents two hexadecimal digits. The setting range is 00 to FF hex, and the default setting is 00 hex. Refer to *7-10-2 Selecting the Method to Set the IP Address Using the Rotary Switches* on page 7-73 for details on how to set the IP address.

***1.** To reflect the settings configured with the rotary switches, you need to cycle the power supply or perform a restart.
***2.** Refer to *6-7 Safety Applications* on page 6-23 for details on the safety applications.
***3.** Refer to *8-9 IP Address Indication Function* on page 8-19 for details on the IP address indication function.
***4.** Refer to *8-6 I/O Wiring Checking Function* on page 8-13 for details on the I/O wiring checking function.

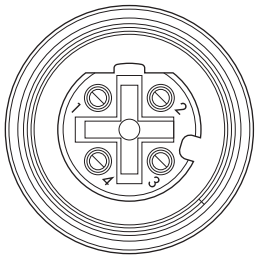
3-4 Connectors

The Safety I/O Block has the following connectors.

- EtherNet/IP communications connectors
- Power supply connectors
- I/O connectors

3-4-1 EtherNet/IP Communications Connectors

The EtherNet/IP communications connectors are used for EtherNet/IP communications. In this manual, they are sometimes referred to as "communications connectors."



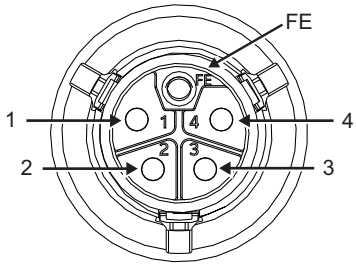
The electrical characteristics, connector structure, and pin arrangement are as follows.

- Electrical specifications
  Conforms to IEEE 802.3 standards.
- Connector structure
  M12 connector (D-coding, female, shielded) x 2
- Pin arrangement

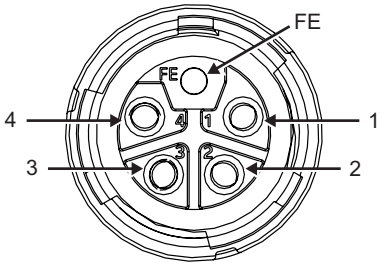
Pin No.	Signal name	Description
1	TD+	Send data +
2	RD+	Receive data +
3	TD-	Send data -
4	RD-	Receive data -

3-4-2 Power Supply Connectors

These connectors are for supplying power to the Safety I/O Block.



Power supply connector (input)
(PWR IN)



Power supply connector (output)
(PWR OUT)

● Power Supply Connector (Input)

This connector is for supplying Unit/input power and output power. Connect the power supply cable of an external power supply.

● Power Supply Connector (Output)

This is the connector for supplying output power from the local node to another node. Use it for power supply sharing with through-wiring.

● Connector Structure and Pin Arrangement

The connector structure and pin arrangement are as follows.

a. Connector structure

Power supply connector (input): M12 connector (L-coding, male, Smartclick support)

Power supply connector (output): M12 connector (L-coding, female, Smartclick support)

b. Pin arrangement

They are common for the power supply connector (input) and power supply connector (output).

Pin No.	Signal name	Description
1	U/IN P+	Unit/input power supply +
2	OUT P-	Output power supply -
3	U/IN P-	Unit/input power supply -
4	OUT P+	Output power supply +
FE (Functional Earth)	FG	Frame ground

Precautions for Safe Use

The maximum power supply current is 9 A, which is the sum of the Unit/input power supply current and the output power supply current. Do not use the Unit beyond the maximum power supply current. Otherwise, an excess current flows through the power supply cable, and it may cause fire.

Precautions for Correct Use

Always use separate power supplies for the Unit/input power supply and the output power supply. If you supply power from the same power supply, load variations in output devices may cause malfunctions.

3-4-3 I/O Connectors

These connectors are used for connecting safety input devices and safety output devices.
The I/O connectors are classified as follows depending on the devices that are connected.
Furthermore, each connector unit is called a "port" in this manual.

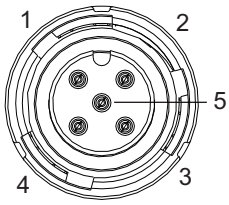
- Safety input ports
- Safety output ports
- Safety I/O ports

Safety Input Ports

I/O connectors with safety input terminals and test output terminals are called safety input ports.
The number of safety input ports and their locations differ depending on the model.

- For NXR-SXD1204-CST: Ports P1 to P6
- For NXR-SXD1204B-CST: Ports P1 to P4

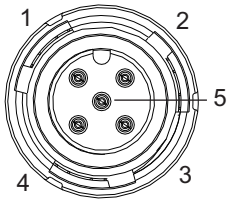
The following shows the pin arrangement of safety input ports.



Pin No.	Signal name	Description	Port					
			P1	P2	P3	P4	P5	P6
1	T (n)	Test output terminal (n)	T00	T02	T04	T06	T08	T10
2	Si (n)	Safety input terminal (n)	Si00	Si02	Si04	Si06	Si08	Si10
3	U/IN P-	Unit/input power supply -	GND					
4	Si (n+1)	Safety input terminal (n+1)	Si01	Si03	Si05	Si07	Si09	Si11
5	T (n+1)	Test output terminal (n+1)	T01	T03	T05	T07	T09	T11

Safety Output Ports

I/O connectors with safety output terminals are called safety output ports.
There are safety output ports on NXR-SXD1204-CST only.
The safety output ports are ports P7 to P8.
The following shows the pin arrangement of safety output ports.

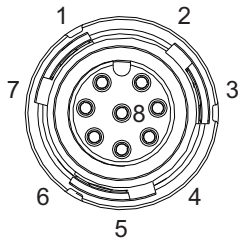


Pin No.	Signal name	Description	Port	
			P7	P8
1	NC	NC	NC	
2	So (n)	Safety output terminal (n)	So00	So02
3	OUT P-	Output power supply -	OUT GND	
4	So (n+1)	Safety output terminal (n+1)	So01	So03
5	OUT P-	Output power supply -	OUT GND	

Safety I/O Ports

I/O connectors with safety input terminals and safety output terminals are called safety I/O ports.
There are safety I/O ports on NXR-SXD1204B-CST only.
The safety I/O ports are ports P5 to P6.

The following shows the pin arrangement of safety I/O ports.



Pin No.	Signal name	Description	Port	
			P5	P6
1	T (n)	Test output terminal (n)	T08	T10
2	Si (n)	Safety input terminal (n)	Si08	Si10
3	U/IN P-	Unit/input power supply -	GND	
4	Si (n+1)	Safety input terminal (n+1)	Si09	Si11
5	T (n+1)	Test output terminal (n+1)	T09	T11
6	So (n)	Safety output terminal (n)	So00	So02
7	So (n+1)	Safety output terminal (n+1)	So01	So03
8	OUT P-	Output power supply -	OUT GND	

4

Designing the Power Supply System

This chapter describes how to design the power supply system for the Safety I/O Block.

4-1 Power Supply Types and Power Supply System 4-2
4-1-1 Power Supply Types and Applications 4-2
4-1-2 Power Supply System 4-2
4-2 Designing the Power Supply System 4-6
4-2-1 Procedure for Designing the Power Supply System 4-6
4-2-2 Design Method for Direct Power Supply 4-6
4-2-3 Design Method for Power Supply System with Through-wiring 4-13
4-3 Selecting Power Supplies and Protective Devices 4-21
4-3-1 Selecting External Power Supplies 4-21
4-3-2 Selecting Protective Devices 4-21

4-1 Power Supply Types and Power Supply System

This section describes the power supply types and applications and the power supply system for the Safety I/O Block.

4-1-1 Power Supply Types and Applications

This section describes the power supply types and applications for the Safety I/O Block.

Types of Power Supplies

There are the following two types of power supplies that supply power to the Safety I/O Block.

- Unit/input power supply
- Output power supply

Power Supply Applications

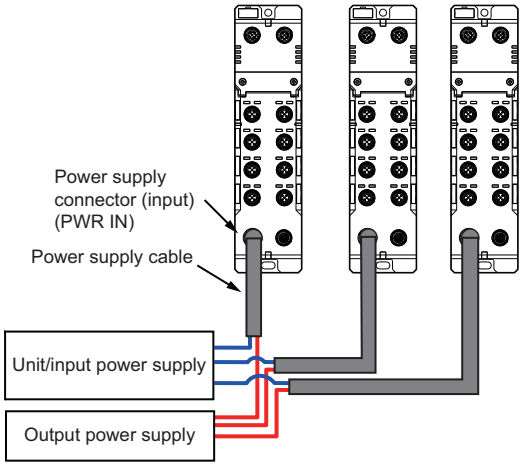
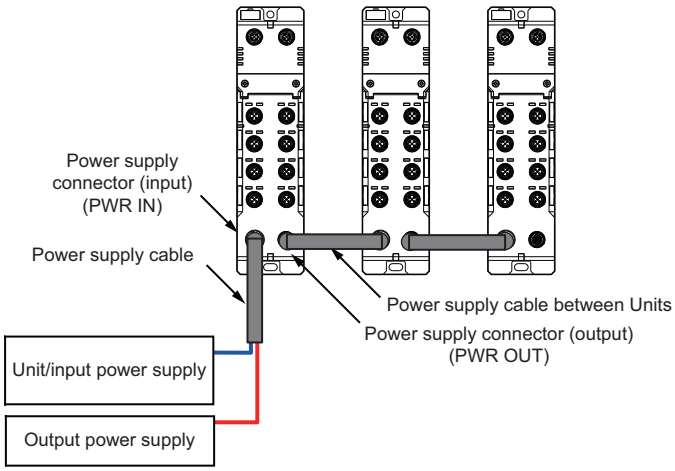
The applications of the power supplies are given below.

Type	Application
Unit/input power supply	A power supply used for operation of the Safety I/O Block and for interfacing with safety input devices. Details are given below. • Operation of Safety I/O Block internal circuits, safety input circuits, and test output circuits • Output of test pulses to safety input device with mechanical contacts • Supply of power to safety input device with semiconductor outputs
Output power supply	A power supply used for interfacing with safety output devices. Details are given below. • Operation of Safety I/O Block output circuits • Load current to safety output device with which PNP output can connect

Both power supplies have voltage and current monitoring, and are protected against overvoltage and overcurrent.

4-1-2 Power Supply System

There are the following two methods to supply power to the Safety I/O Block.

Method	Description	Features
Direct power supply	Connect the external power supplies to the PWR IN power supply connector of each Safety I/O Block. *1  	This method does not cause a voltage drop in through-wiring cables.
Power supply with through-wiring*2	Connect an external power supply to the PWR IN power supply connector of one Safety I/O Block. Then, connect the PWR OUT power supply connector of that Unit to the PWR IN power supply connector of another Safety I/O Block with a power supply cable. In this way, supply power with through-wiring between the subsequent Units with power supply cables. *1  	Through-wiring can reduce the overall length of the power supply cables used in the system. When using this power supply wiring method, you can use the power OFF function for through-wiring output. Refer to *8-5 Power OFF Function for Through-wiring Output* on page 8-11 for details.

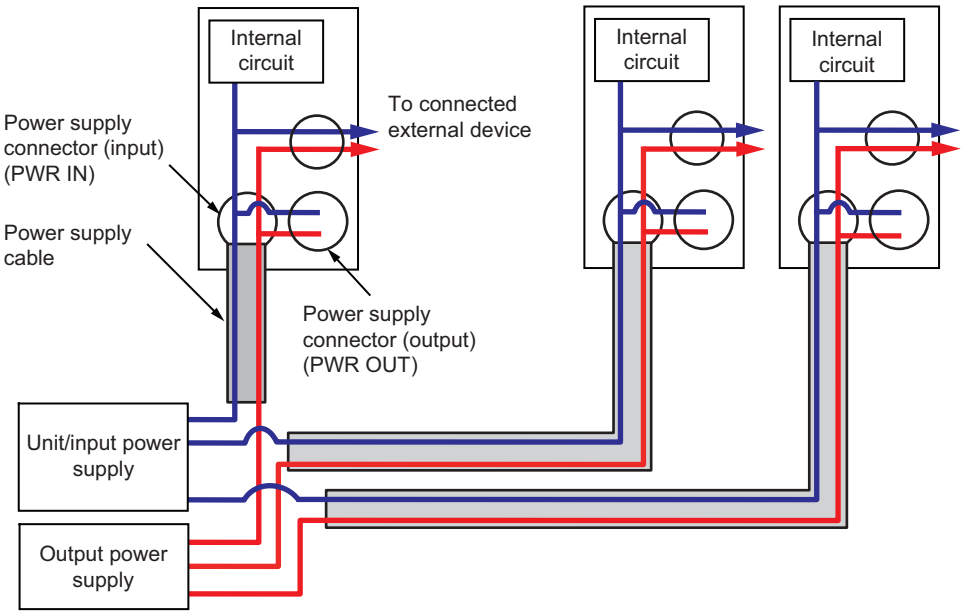
***1.** When using an OMRON Environment-resistive IP67 Power Supply (S8NR-S Series), the GND of the Unit/input power supply and the GND of the output power supply are connected inside the Power Supply Unit. Therefore, the insulation in the Safety I/O Block is not guaranteed. If insulation is required, separate the Unit/input power supply and output power supply.

***2.** The output power supply is supplied from PWR OUT only when Unit/input power is supplied to the Safety I/O Block. When the Unit/input power supply is OFF or the Unit/input power supply is shut off due to an overvoltage or other reason, output power supply from PWR OUT is also shut off.

The details on system configuration are shown below.

● System Configuration for Direct Power Supply

An example is shown below. Connect an external power supply to the PWR IN power supply connector of each Safety I/O Block.

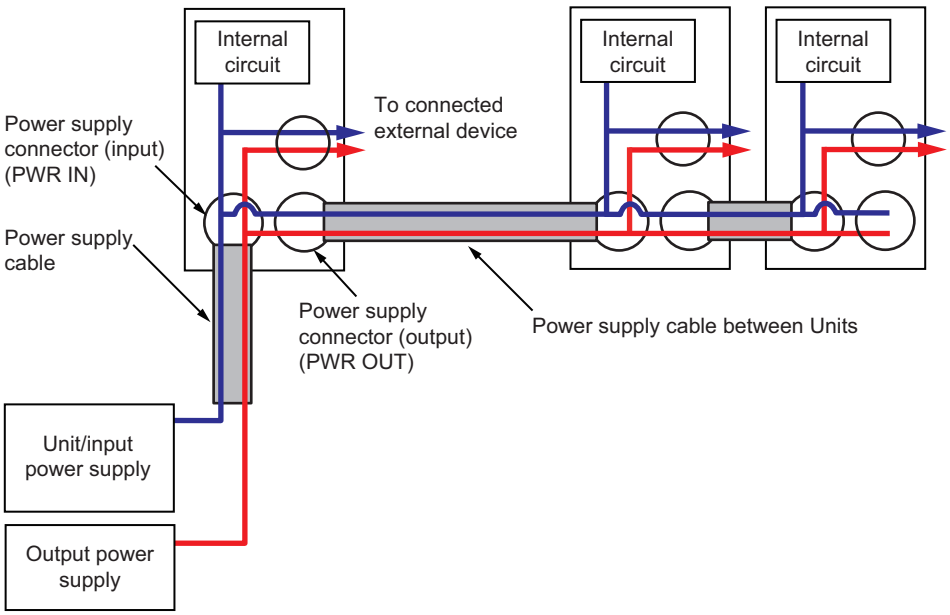


Precautions for Correct Use

- Always use separate power supplies for the Unit/input power supply and the output power supply. If you supply power from the same power supply, load variations in output devices may cause malfunctions.

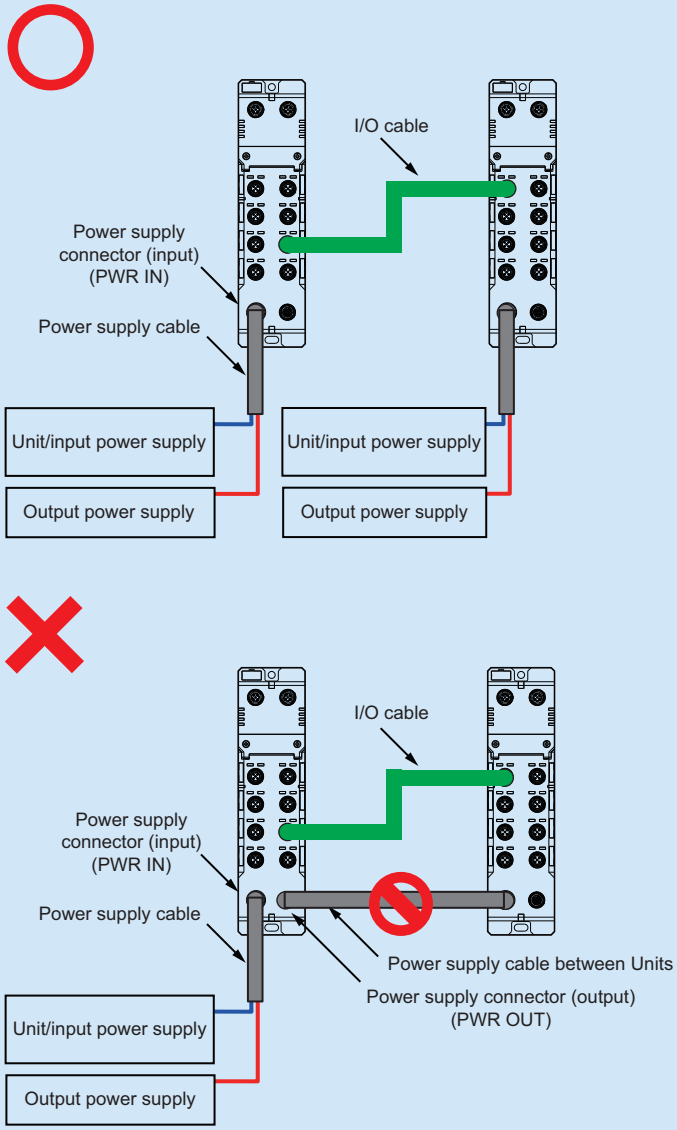
System Configuration for Power Supply with Through-wiring

Connect an external power supply to the PWR IN power supply connector of the first Safety I/O Block. Then, connect the PWR OUT power supply connector of that Unit to the PWR IN power supply connector of another Safety I/O Block with a power supply cable. In this way, connect a power supply cable between the subsequent Units with through-wiring one after another.



Precautions for Correct Use

- Always use separate power supplies for the Unit/input power supply and the output power supply. If you supply power from the same power supply, load variations in output devices may cause malfunctions.
- When connecting safety I/O ports between Units, do not supply power with through-wiring. Since the GND between the power supplies will be connected via an I/O cable, they will not be isolated.



4-2 Designing the Power Supply System

This section describes how to design the power supply system for the Safety I/O Block.

⚠ WARNING

Follow the instructions in this manual to correctly perform power supply design and wiring. Inputting voltages or currents that are outside of the specified ranges, as well as incorrect wiring, may cause failure or fire.

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

The overall procedure for designing the power supply system for the Safety I/O Block is as follows.

Step	Description	Reference
1. Determining the Power Supply Method	Determine the power supply method. There are the following two power supply methods. • Direct power supply • Power supply with through-wiring	*4-1-2 Power Supply System* on page 4-2
↓		
2. Designing the Power Supply System	Depending on the power supply method, perform the following design operations and then confirm that they meet the design conditions. • Designing the Unit/input power supply • Designing the output power supply	• For direct power supply *4-2-2 Design Method for Direct Power Supply* on page 4-6 • For power supply with through-wiring *4-2-3 Design Method for Power Supply System with Through-wiring* on page 4-13
↓		
3. Selecting External Power Supplies and Protective Devices	Calculate the power supply capacity from the current consumption calculated in step 2, and select external power supplies accordingly. In addition, select protective devices (e.g., breakers and fuses) to protect against short circuits and overcurrents in external circuits.	*4-3 Selecting Power Supplies and Protective Devices* on page 4-21

4-2-2 Design Method for Direct Power Supply

This section describes how to design the power supply system when the power supply method is direct power supply.

Design Procedure for Direct Power Supply

Confirm that the power supplies meet the following design conditions (a) to (c). Refer to the reference sections for the confirmation method.

Design condition	Reference for confirmation method
(a) The sum of the total current consumption from the Unit/input power supply and output power supply must not exceed the maximum power supply current of the Safety I/O Block.*1	*Calculating the Total Current Consumption in Direct Power Supply* on page 4-7
(b) The input circuit specifications of the Safety I/O Block and the voltage specifications of the connected external devices are met even if the Unit/input power supply voltage drops.*2	*Calculating the Voltage Drop in Direct Power Supply* on page 4-11
(c) The output circuit specifications of the Safety I/O Block and the voltage specifications of the connected external devices are met even if the output power supply voltage drops.*3	

***1.** The maximum power supply current is 9 A. Do not exceed 9 A.
***2.** For example, for the Safety I/O Block, confirm that the Unit/input power supply voltage is 19.2 to 28.8 VDC.
***3.** For example, for the Safety I/O Block, confirm that the output power supply voltage is 19.2 to 28.8 VDC.

Calculating the Total Current Consumption in Direct Power Supply

Direct power supply is the method to supply power to each Safety I/O Block. Therefore, calculate the total current consumption of each Unit from each power supply. Design the system so that the sum of the total current consumption from each power supply is less than the maximum power supply current of the Safety I/O Block.

The calculation methods for the total current consumption of the Safety I/O Block from the Unit/input power supply and output power supply are given below.

● Total Current Consumption from Unit/Input Power Supply

= (Current consumption from Unit/input power supply)
+ (Current consumed by connected safety input devices)
+ (Current consumed by test outputs)

The items of the formula are described below.

Item	Description
Current consumption from Unit/input power supply	This is the current consumed by the Safety I/O Block. Use the *Unit/input power supply* value of *current consumption* in *2-1-4 Unit Specifications* on page 2-6.
Current consumed by connected safety input devices	Use the following formula to calculate this value. (Current consumption from power supplies of safety input devices) + (Safety Input current × Number of inputs used)
Current consumed by test outputs*1	Use the following formula to calculate this value. (Test output load current × Number of outputs used)

***1.** When connecting a device with semiconductor outputs, the output current of the test output needs to be 0.7 A/point.

● Total Current Consumption from Output Power Supply

= (Current consumption from output power supply)
+ (Current consumed by connected safety output devices)

The items of the formula are described below.

Item	Description
Current consumption from output power supply	This is the current consumed by the Safety I/O Block. Use the *output power supply* value of *current consumption* in *2-1-4 Unit Specifications* on page 2-6.
Current consumed by connected safety output devices *1	Use the following formula to calculate this value. (Safety output load current × Number of outputs used)

*1. For NXR-SXD1204-CST, do not exceed the safety output maximum load current of 2 A/point. For NXR-SXD1204B-CST, do not exceed the safety output maximum load current of 0.7 A/point.

Calculation Example for the Total Current Consumption in Direct Power Supply

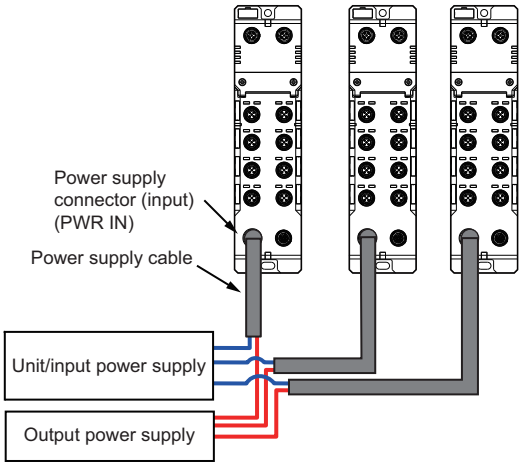
The following shows how to calculate the total current consumption from the Unit/input power supply and output power supply for a given configuration and application conditions as an example.

Precautions for Correct Use

This shows an example calculation. Since customer equipment and facilities vary, please perform calculations according to your specific usage.

● Configuration Example

Assume that there are three Safety I/O Block: SXD1, SXD2, and SXD3 from the left.



● Application Conditions for Connected External Devices

Assume that the following conditions are used for each Safety I/O Block. The conditions for SXD2 and SXD3 are the same.

Conditions for Safety I/O Block				Conditions for connected external device	
Unit name	Safety I/O port			Product name	Specifications
	Port name	Signal name	Terminal number		
SXD1	Safety input port 1	Safety input	Si00 /01	Safety input device	• Current consumption in the safety input device: 50mA • Safety input current: 4.5 mA/point • Test output load current: 200 mA/point
		Test output	T00 /01		
	Safety input port 2	Safety input	Si02 /03	Safety input device	• Current consumption in the safety input device: 50mA • Safety input current: 4.5 mA/point • Test output load current: 200 mA/point
		Test output	T02 /03		
	Safety input ports 3 to 6	Safety input	Si04 to 11	Unused	–
		Test output	T04 to 11	Unused	–
	Safety output port 1	Safety output	So00 /01	Safety output device	• Current consumption in the safety output device: 50mA • Safety output load current: 500 mA/point
	Safety output port 2	Safety output	So02 /03	Unused	–
SXD2 and SXD3	Safety input port 1	Safety input	Si00 /01	Safety input device	• Current consumption in the safety input device: 50mA • Safety input current: 4.5 mA/point • Test output load current: 200 mA/point
		Test output	T00 /01		
	Safety input ports 2 to 6	Safety input	Si02 to 11	Unused	–
		Test output	T02 to 11	Unused	–
	Safety output port 1	Safety output	So00 /01	Safety output device	• Current consumption in the safety output device: 50mA • Safety output load current: 500 mA/point
	Safety output port 2	Safety output	So02 /03	Not used	–

● Calculating the Total Current Consumption

The items to calculate for the total current consumption of each Safety I/O Block from the Unit/input power supply and output power supply are as follows.

Unit name	Types of power supplies	Item to calculate for total current consumption	Calculation result
SXD1	Unit/input power supply	Current consumption from Unit/input power supply	220 mA according to the specifications of the Safety I/O Block.
		Current consumed by connected safety input devices	Safety input ports 1 and 2 are calculated. (Current consumption from power supplies of safety input devices) + (Safety Input current × Number of inputs used) = (50 mA + 50 mA) + (4.5 mA × 4 points) = 118 mA
		Current consumed by test outputs	Safety input ports 1 and 2 are calculated. (Test output load current × Number of outputs used) = 200 mA × 4 points = 800 mA
	Output power supply	Current consumption from output power supply	40 mA according to the specifications of the Safety I/O Block.
		Current consumed by connected safety output devices	Safety output ports 1 is calculated. (Safety output load current × Number of outputs used) = 500 mA × 2 points = 1000 mA
SXD2 and SXD3	Unit/input power supply	Current consumption from Unit/input power supply	220 mA according to the specifications of the Safety I/O Block.
		Current consumed by connected safety input devices	Safety input port 1 is calculated. (Current consumption from power supplies of safety input devices) + (Safety Input current × Number of inputs used) = 50 mA + (4.5 mA × 2 points) = 59 mA
		Current consumed by test outputs	Safety input port 1 is calculated. (Test output load current × Number of outputs used) = 200 mA × 2 points = 400 mA
	Output power supply	Current consumption from output power supply	40 mA according to the specifications of the Safety I/O Block.
		Current consumed by connected safety output devices	Safety output ports 1 is calculated. (Safety output load current × Number of outputs used) = 500 mA × 2 points = 1000 mA

From the above calculation results, the sum of the total current consumption of each Safety I/O Block is calculated as follows.

a. Sum of the total current consumption of SXD1
   (Total current consumption of SXD1 from Unit/input power supply) + (Total current consumption of SXD1 from output power supply)
   = (220 mA + 118 mA + 800 mA) + (40 mA + 1000 mA)
   = (1138 mA) + (1040 mA)
   ≈ (1.14 A) + (1.04 A)
   = 2.18 A

b. Sum of the total current consumption of SXD2

(Total current consumption of SXD2 from Unit/input power supply) + (Total current consumption of SXD2 from output power supply)
= (220 mA + 59 mA + 400 mA) + (40 mA + 1000 mA)
= (679 mA) + (1040 mA)
≈ (0.68 A) + (1.04 A)
= 1.72 A

c. Sum of the total current consumption of SXD3
The formula is the same as that of SXD2.
(Total current consumption of SXD3 from Unit/input power supply) + (Total current consumption of SXD3 from output power supply)
≈ 1.72A

This example is acceptable because the sum of the total current consumption for each Unit is below 9 A, the maximum power supply current of the Safety I/O Block.

Calculating the Voltage Drop in Direct Power Supply

A power supply cable causes a voltage drop.
The voltage drop when using OMRON M12 L-coding power supply cable (XS5F-L521-□12-F, XS5W-L521-□12-F) is as shown in the table below.

Current consumption from Unit/input power supply or output power supply (A)	Voltage drop for each power supply cable length (V)			
	1 m	3 m	5 m	10 m
9	0.80	2.40	4.00	8.00
8	0.71	2.13	3.56	7.11
6	0.53	1.60	2.67	5.33
4	0.36	1.07	1.78	3.56
3	0.27	0.80	1.33	2.67
2	0.18	0.53	0.89	1.78
1	0.09	0.27	0.44	0.89

Design the system so that the voltage specifications of the Safety I/O Block and connected external devices are met even if the voltage of the Unit/input power supply and output power supply drops.

Precautions for Correct Use

This shows an example calculation. Since customer equipment and facilities vary, please perform calculations according to your specific usage.

● Calculation Example for Voltage Drop

The following example explains how to calculate voltage drop under the following conditions.

Item	Conditions
Configuration	Use the conditions specified in *Calculation Example for the Total Current Consumption in Direct Power Supply* on page 4-8.
Application conditions for connected external devices	The conditions lead to the current consumption from each power supply by each Unit below: • SXD1: 2.18 A Current consumption from Unit/input power supply: 1.14 A Current consumption from Output power supply: 1.04 A • SXD2: 1.72 A Current consumption from Unit/input power supply: 0.68 A Current consumption from Output power supply: 1.04 A • SXD3: 1.72 A Current consumption from Unit/input power supply: 0.68 A Current consumption from Output power supply: 1.04 A
Power supply cable length	• Power supply cable connected to SXD1: 1 m • Power supply cable connected to SXD2: 3 m • Power supply cable connected to SXD3: 5 m
Voltage at power supply terminal of external power supply	• Unit/input power supply: 24.0 VDC • Output power supply: 24.0 VDC

The voltage drop for each Unit from each power supply is determined as follows according to the table of voltage drop in power supply cables.

Unit name	Voltage drop	
	Unit/input power supply	Output power supply
SXD1	0.18 V (2 A is used because the cable length is 1 m and the current consumption is 1.14 A.)	0.18 V (2 A is used because the cable length is 1 m and the current consumption is 1.04 A.)
SXD2	0.27 V (1 A is used because the cable length is 3 m and the current consumption is 0.68 A.)	0.53 V (2 A is used because the cable length is 3 m and the current consumption is 1.04 A.)
SXD3	0.44 V (1 A is used because the cable length is 5 m and the current consumption is 0.68 A.)	0.89 V (2 A is used because the cable length is 5 m and the current consumption is 1.04 A.)

From the above results, the voltage of each input power supply to each Unit is calculated as follows.

a. Voltage of each input power supply to SXD1
   Voltage of Unit/input power supply
   = 24.0 V - Voltage drop in power supply cable
   = 24.0 V - 0.18 V
   = 23.82 V
   Voltage of Output power supply
   = 24.0 V - Voltage drop in power supply cable
   = 24.0 V - 0.18 V
   = 23.89 V

b. Voltage of each input power supply to SXD2
   Voltage of Unit/input power supply
   = 24.0 V - Voltage drop in power supply cable
   = 24.0 V - 0.27 V

= 23.73 V
Voltage of Output power supply
= 24.0 V - Voltage drop in power supply cable
= 24.0 V - 0.53 V
= 23.47 V

c. Voltage of each input power supply to SXD3
Voltage of Unit/input power supply
= 24.0 V - Voltage drop in power supply cable
= 24.0 V - 0.44 V
= 23.56 V
Voltage of Output power supply
= 24.0 V - Voltage drop in power supply cable
= 24.0 V - 0.89 V
= 23.11 V

The above voltage values all are acceptable because they meet the voltage specifications (19.2 to 28.8 VDC) of each power supply of the Safety I/O Block.
Also, confirm that the voltage values meet the voltage specifications of the connected safety input devices or safety output devices. However, this confirmation is omitted in this example.
If the voltage specifications are not met, review the length of power supply cable and the connected external devices.

4-2-3 Design Method for Power Supply System with Through-wiring

This section describes how to design the power supply system when the power supply method is power supply with through-wiring.

Procedure for Designing a Power Supply System with Through-wiring

Confirm that the power supplies meet the following design conditions (a) to (c). Refer to the reference sections for the confirmation method.

Design condition	Reference for confirmation method
(a) The sum of the total current consumption from the Unit/input power supply and output power supply must not exceed the maximum power supply current of the Safety I/O Block.*1	*Calculating the Total Current Consumption in Power Supply with Through-wiring* on page 4-14
(b) The input circuit specifications of the Safety I/O Block and the voltage specifications of the connected external devices are met even if the Unit/input power supply voltage drops.*2	*Calculating the Voltage Drop in Power Supply with Through-wiring* on page 4-17
(c) The output circuit specifications of the Safety I/O Block and the voltage specifications of the connected external devices are met even if the output power supply voltage drops.*3	

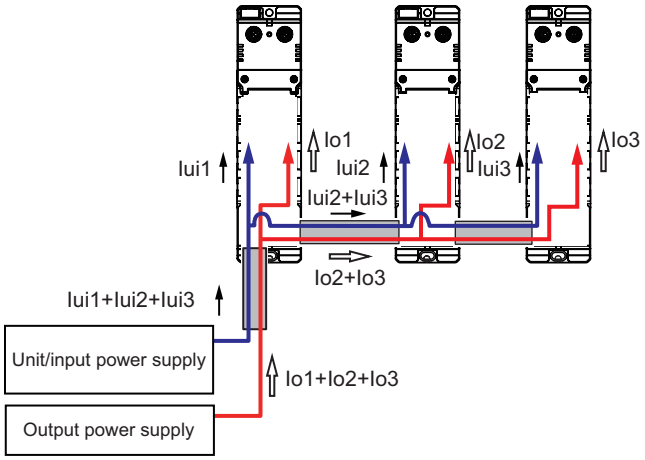
***1.** The maximum power supply current is 9 A. Do not exceed 9 A.
***2.** For example, for the Safety I/O Block, confirm that the Unit/input power supply voltage is 19.2 to 28.8 VDC.
***3.** For example, for the Safety I/O Block, confirm that the output power supply voltage is 19.2 to 28.8 VDC.

Calculating the Total Current Consumption in Power Supply with Through-wiring

When the power supply method is power supply with through-wiring, unlike the case of direct power supply, all the current to be consumed by other Safety I/O Block to which power is supplied flows through the Safety I/O Block connected to external power supplies. In other words, you need to design the system so that the sum of the current consumption from each Unit is less than the maximum power supply current of the Safety I/O Block.

The following is an example. In this example, confirm that the following expression is met.
Assume that there are three Safety I/O Block: SXD1, SXD2, and SXD3 from the left.

(Iui1 + Iui2 + Iui3 + Io1 + Io2 + Io3) < (Maximum power supply current of SXD1*1)

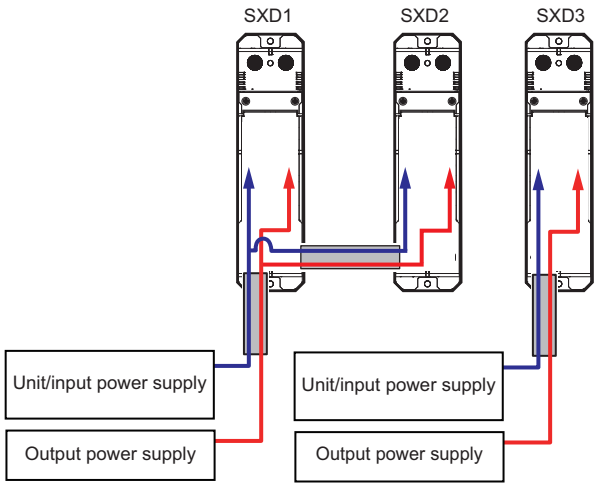


Iui1: Total current consumption of SXD1 from Unit/input power supply
Iui2: Total current consumption of SXD2 from Unit/input power supply
Iui3: Total current consumption of SXD3 from Unit/input power supply
Io1: Total current consumption of SXD1 from output power supply
Io2: Total current consumption of SXD2 from output power supply
Io3: Total current consumption of SXD3 from output power supply

***1.** If the maximum power supply current of SXD1 is not exceeded, then that of SXD2 and SXD3 is not exceeded.

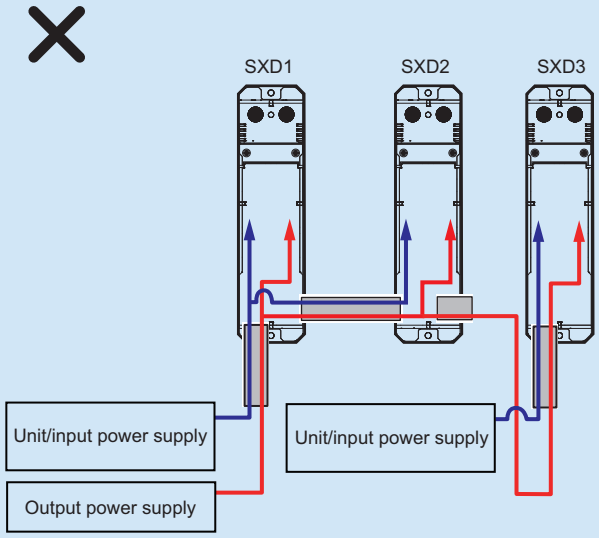
The calculation method for the total current consumption of each Unit from the Unit/input power supply or output power supply is the same as that for direct power supply. Refer to *Calculating the Total Current Consumption in Direct Power Supply* on page 4-7.
If the calculated value does not meet the specified condition, add external power supplies so that the condition is met.

Example: A system with additional external power supplies



Precautions for Correct Use

Be sure to add a set of Unit/input power supply and output power supply. It is not allowed to add only one of them.



Calculation Example for the Total Current Consumption in Power Supply with Through-wiring

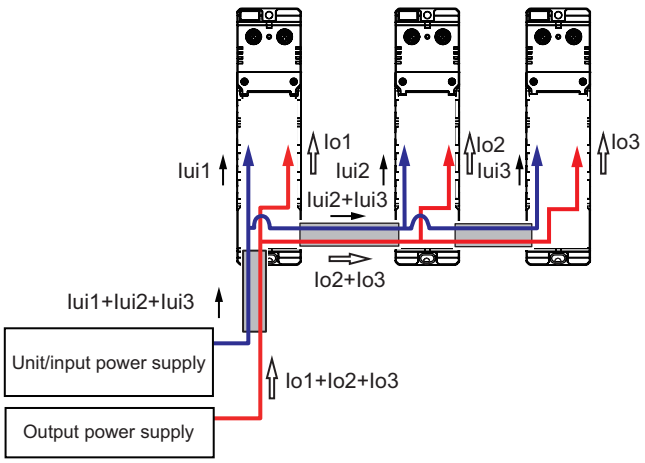
The following shows how to calculate the total current consumption when the power supply method is power supply with through-wiring for a given configuration and application conditions as an example.

Precautions for Correct Use

This shows an example calculation. Since customer equipment and facilities vary, please perform calculations according to your specific usage.

● Configuration Example

Assume that there are three Safety I/O Block: SXD1, SXD2, and SXD3 from the left.



● Application Conditions for Connected External Devices

The conditions are the same as those in *Calculation Example for the Total Current Consumption in Direct Power Supply* on page 4-8.

● Calculating the Total Current Consumption

The total current consumption of each Unit is calculated as follows, according to *Calculation Example for the Total Current Consumption in Direct Power Supply* on page 4-8.

1. Sum of the total current consumption of SXD1
   (Total current consumption of SXD1 from Unit/input power supply) + (Total current consumption of SXD1 from output power supply)
   (Iui1 + Io1)
   = (220 mA + 118 mA + 800 mA) + (40 mA + 1000 mA)
   = (1138 mA) + (1040 mA)
   ≈ (1.14 A) + (1.04 A)
   = 2.18 A

2. Sum of the total current consumption of SXD2
   (Total current consumption of SXD2 from Unit/input power supply) + (Total current consumption of SXD2 from output power supply)
   (Iui2 + Io2)
   = (220 mA + 59 mA + 400 mA) + (40 mA + 1000 mA)
   = (679 mA) + (1040 mA)
   ≈ (0.68 A) + (1.04 A)
   = 1.72 A

3. Sum of the total current consumption of SXD3
   The formula is the same as that of SXD2.
   (Total current consumption of SXD3 from Unit/input power supply) + (Total current consumption of SXD3 from output power supply)
   (Iui3 + Io3)
   ≈ 1.72A

The sum of the total current consumption of each Unit supplied from external power supplies is calculated as follows.
(Iui1 + Iui2 + Iui3 + Io1 + Io2 + Io3)
= (2.18 A + 1.72 A + 1.72 A)
= 5.62 A

This example is acceptable because the calculation result is below 9 A, the maximum current of power supply of the Safety I/O Block.

Calculating the Voltage Drop in Power Supply with Through-wiring

When the power supply method is power supply with through-wiring, a voltage drop occurs due to the following elements.

- Internal circuit of the Safety I/O Block
- Power supply cables

When the power supply method is power supply with through-wiring, the current to be consumed by other Units flows through the Safety I/O Block, which causes a voltage drop in the internal circuits of the Unit.
When using OMRON M12 L-coding power supply cables (XS5F-L521-□12-F, XS5W-L521-□12-F), the voltage drop in the internal circuits of the Safety I/O Block and power supply cables is as shown in the table below depending on the current consumption of the Unit/input power supply and output power supply.

Current consumption from Unit/input power supply (A)	Voltage drop in the internal circuits of Unit (V)	Voltage drop for each power supply cable length (V)			
		1 m	3 m	5 m	10 m
9	0.40	0.80	2.40	4.00	8.00
8	0.36	0.71	2.13	3.56	7.11
6	0.27	0.53	1.60	2.67	5.33
4	0.18	0.36	1.07	1.78	3.56
3	0.13	0.27	0.80	1.33	2.67
2	0.09	0.18	0.53	0.89	1.78
1	0.04	0.09	0.27	0.44	0.89

Current consumption from Output power supply (A)	Voltage drop in the internal circuits of Unit (V)	Voltage drop for each power supply cable length (V)			
		1 m	3 m	5 m	10 m
9	0.50	0.80	2.40	4.00	8.00
8	0.44	0.71	2.13	3.56	7.11
6	0.33	0.53	1.60	2.67	5.33
4	0.22	0.36	1.07	1.78	3.56
3	0.17	0.27	0.80	1.33	2.67
2	0.11	0.18	0.53	0.89	1.78
1	0.06	0.09	0.27	0.44	0.89

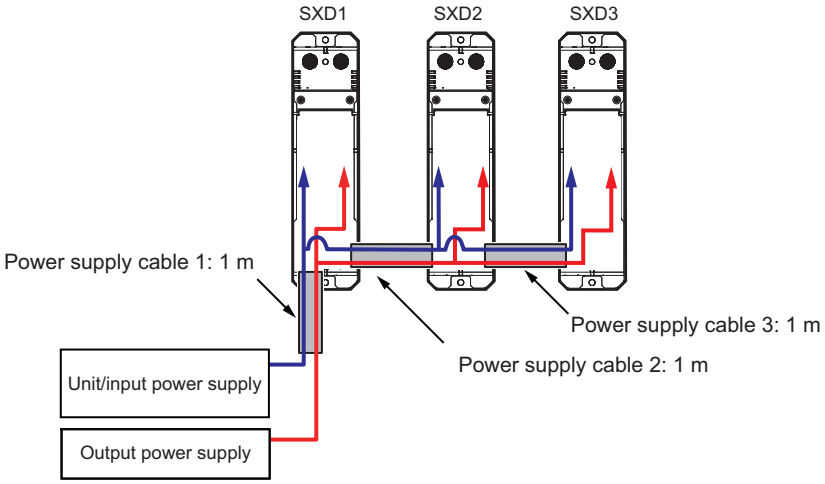
Design the system so that the voltage specifications of the Safety I/O Block and connected external devices are met even if the voltage of the Unit/input power supply and output power supply drops.

Precautions for Correct Use

This shows an example calculation. Since customer equipment and facilities vary, please perform calculations according to your specific usage.

● Calculation Example for Voltage Drop

The following example explains how to calculate voltage drop under the following conditions.

Item	Conditions
Configuration	Use the conditions specified in *Calculation Example for the Total Current Consumption in Power Supply with Through-wiring* on page 4-15.
Application conditions for connected external devices	
Power supply cable length	The cable length is as follows. 
Voltage at power supply terminal of external power supply	• Unit/input power supply: 24.0 VDC • Output power supply: 24.0 VDC

According to the table of voltage drop in the internal circuits of the Safety I/O Block and power supply cables, the voltage drop for each Unit from each power supply is determined as follows.

Unit name	Voltage drop in internal circuits of Unit	Voltage drop in power supply cables	Remarks
SXD1	–	• Voltage drop in power supply cable 1: 0.53 V	Use the voltage drop at 6 A because the sum of the current consumption of each unit from external power supplies is 5.62 A.
SXD2	Voltage drop in internal circuits of SXD1 • Unit/input power supply : 0.18 V • Output power supply : 0.22 V	• Voltage drop in power supply cable 1: 0.53 V • Voltage drop in power supply cable 2: 0.36 V	For the voltage drop in power supply cable 1, use the value of SXD1. For the voltage drop in power supply cable 2 and internal circuits of SXD1, use the current value calculated as follows. (Sum of current consumption of each Unit from external power supplies) - (Sum of total current consumption of SXD1) = 5.62 A - 2.18 A = 3.44 A Therefore, use the value at 4 A.

Unit name	Voltage drop in internal circuits of Unit	Voltage drop in power supply cables	Remarks
SXD3	Voltage drop in internal circuits of SXD1 • Unit/input power supply : 0.18 V • Output power supply : 0.22 V Voltage drop in internal circuits of SXD2 • Unit/input power supply : 0.09 V • Output power supply : 0.11 V	• Voltage drop in power supply cable 1: 0.53 V • Voltage drop in power supply cable 2: 0.36 V • Voltage drop in power supply cable 3: 0.18 V	For the voltage drop in power supply cable 1 and power supply cable 2, and voltage drop in the internal circuits of SXD1, use the values of SXD1 and SXD2. For the voltage drop in power supply cable 3 and internal circuits of SXD2, use the current value calculated as follows. (Sum of current consumption of each Unit from external power supplies) - (Sum of total current consumption of SXD1 and SXD2) = 5.62 A - 2.18 A - 1.72 A = 1.72 A Therefore, use the value at 2 A.

From the above results, the voltage of each input power supply to each Unit is calculated as follows.

a. Voltage of each input power supply to SXD1
   Voltage of Unit/input power supply
   = 24.0 V - Voltage drop in power supply cable 1
   = 24.0 V - 0.53 V
   = 23.47 V
   Voltage of Output power supply
   = 24.0 V - Voltage drop in power supply cable 1
   = 24.0 V - 0.53 V
   = 23.47 V

b. Voltage of each input power supply to SXD2
   Voltage of Unit/input power supply
   = 24.0 V - (Voltage drop in power supply cable 1 + Voltage drop in the internal circuits of SXD1 + Voltage drop in power supply cable 2)
   = 24.0 V - (0.53 V + 0.18 V + 0.36 V)
   = 22.93 V
   Voltage of Output power supply
   = 24.0 V - (Voltage drop in power supply cable 1 + Voltage drop in the internal circuits of SXD1 + Voltage drop in power supply cable 2)
   = 24.0 V - (0.53 V + 0.22 V + 0.36 V)
   = 22.89 V

c. Voltage of each input power supply to SXD3
   Voltage of Unit/input power supply
   = 24.0 V - (Voltage drop in power supply cable 1 + Voltage drop in the internal circuits of SXD1 + Voltage drop in power supply cable 2 + Voltage drop in the internal circuits of SXD2 + Voltage drop in power supply cable 3)
   = 24.0 V - (0.53 V + 0.18 V + 0.36 V + 0.09 V + 0.18 V)
   = 22.66 V
   Voltage of Output power supply

= 24.0 V - (Voltage drop in power supply cable 1 + Voltage drop in the internal circuits of SXD1 + Voltage drop in power supply cable 2 + Voltage drop in the internal circuits of SXD2 + Voltage drop in power supply cable 3)
= 24.0 V - (0.53 V + 0.22 V + 0.36 V + 0.11 V + 0.18 V)
= 22.6 V

The above voltage values all are acceptable because they meet the voltage specifications (19.2 to 28.8 VDC) of each power supply of the Safety I/O Block.
Also, confirm that the voltage values meet the voltage specifications of the connected safety input devices or safety output devices. However, this confirmation is omitted in this example.
If the voltage specifications are not met, review the length of power supply cable and the connected external devices.

4-3 Selecting Power Supplies and Protective Devices

This section describes how to select the external power supplies, i.e., Unit/input power supply and output power supplies, and protective devices for the Safety I/O Block.

4-3-1 Selecting External Power Supplies

The following describes how to select the recommended power supplies for external power supplies and their power supply capacity.

Power Supply Used

Use a SELV power supply or OMRON Environment-resistive IP67 Power Supply (S8NR-S Series) which meets the following conditions for the Unit/input power supply and output power supply for the external power supplies of the Safety I/O Block.

- Has overcurrent protection.
- Has double or reinforced insulation between the input and output.
- Has an output voltage of 24 VDC (19.2 to 28.8 VDC).

Recommended power supplies: S8VK-S Series (OMRON) and S8NR-S Series (OMRON)

Power Supply Capacity

Calculate the total current consumptions from the Unit/input power supply and output power supply and the power supply capacity of each power supply according to the calculation methods described in *4-2 Designing the Power Supply System* on page 4-6.

Precautions for Safe Use

Inrush current may flow in the Unit/input power supply and output power supply in the following cases.

a. When power is turned ON.
b. When the power supply to connected external devices is started.
c. When connected external devices are turned ON and OFF.

In addition, overcurrent may flow until the protection is activated when there is a short-circuit in I/O cables. Consider these currents and select power supplies with sufficient extra capacity. The inrush current may prevent the power supply from operating correctly, or cause the power supply to turn OFF.

4-3-2 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.
An overcurrent is a current that flows when the equipment is used beyond the following ratings, such as in the case of a short circuit or device failure.

- Unit/input power supply and output power supply (common): Maximum power supply current

- Unit/input power supply: Rated current to test output terminal
- Output power supply: Maximum load current to safety output device

Refer to *2-1-4 Unit Specifications* on page 2-6 for the above ratings.

Selecting Protective Devices

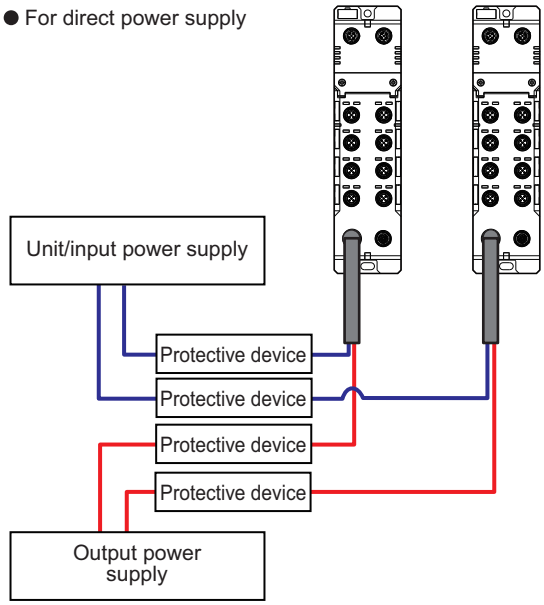
Consider the following when you select protective devices.

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

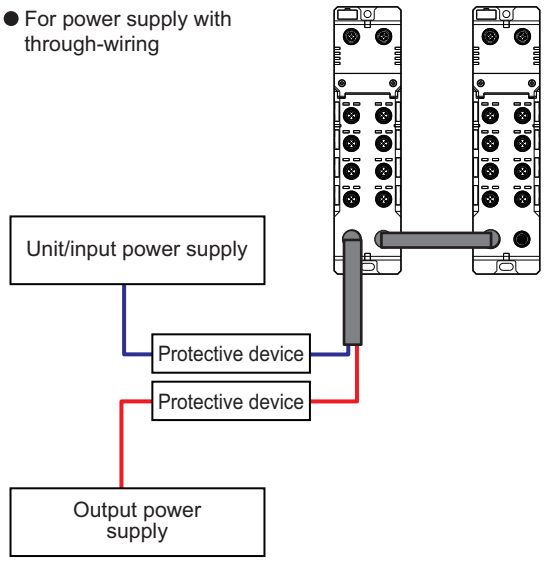
Installation Locations for Protective Devices

Install protective devices for each of the Unit/input power supply and output power supply as shown in the following figure.

● For direct power supply



● For power supply with through-wiring



5

Installation and Wiring

This chapter describes how to install and wire the Safety I/O Block.

5-1 Installing Units 5-2
5-1-1 Installation Precautions 5-2
5-1-2 Installation Orientations 5-2
5-1-3 Installation Method 5-3

5-2 EtherNet/IP Network Wiring 5-5
5-2-1 Installation Precautions 5-5
5-2-2 Connecting Communications Cables 5-6

5-3 Wiring the Power Supply 5-12
5-3-1 Installation Precautions 5-12
5-3-2 Power Supply Cables, Tightening Tools and Tightening Torque to Use 5-12
5-3-3 Connecting Power Supply Cables to External Power Supplies 5-13
5-3-4 Connecting Power Supply Cables 5-14

5-4 Wiring I/O Cables 5-19
5-4-1 Installation Precautions 5-19
5-4-2 Connecting I/O Cables 5-19
5-4-3 Wiring Examples 5-24

5-5 Connected Devices 5-29
5-5-1 Ethernet Cables 5-29
5-5-2 Power Supply Cables 5-31
5-5-3 I/O Cables 5-34
5-5-4 Waterproof Covers for Connectors 5-38

5-6 Options 5-39
5-6-1 Markers 5-39

5-1 Installing Units

This section describes how to install the Safety I/O Block.

5-1-1 Installation Precautions

To increase the reliability of the Safety I/O Block and take complete advantage of its functionality, observe the following precautions.

Do not install the Unit in the following locations.

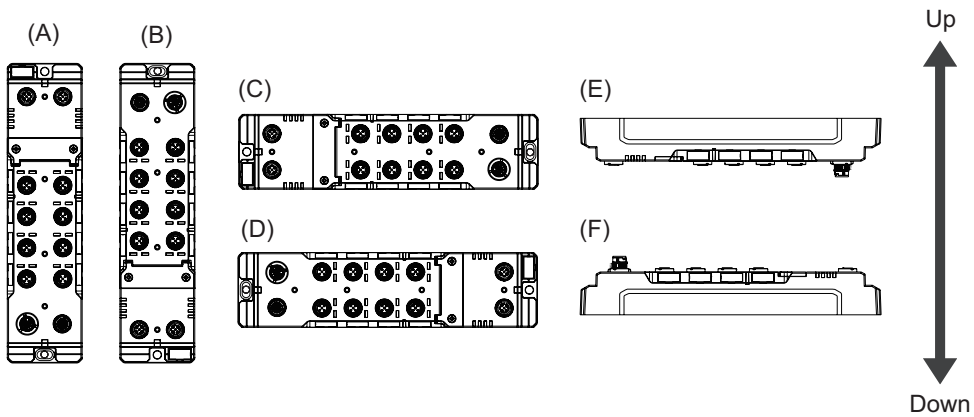
- Locations subject to direct sunlight
- Locations subject to ambient temperatures or humidity outside the range specified in the specifications of the Unit
- Locations subject to condensation as the result of severe changes in temperature
- Locations subject to corrosive or flammable gases
- Locations subject to dust (especially iron dust) or salts
- Locations subject to exposure to acid, oil, or chemicals
- Locations subject to shock or vibration
- Locations close to power lines

Take appropriate and sufficient countermeasures during installation in the following locations.

- Locations subject to static electricity or other forms of noise
- Locations subject to strong electromagnetic fields
- Locations subject to possible exposure to radioactivity
- Locations close to power supply lines

5-1-2 Installation Orientations

The Safety I/O Block can be installed in any of the following six orientations.



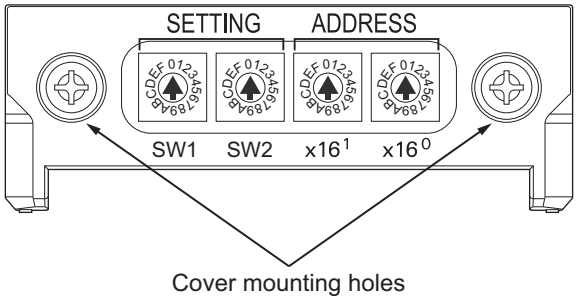
5-1-3 Installation Method

This section describes how to install the following of the Safety I/O Block.

- Installing the rotary switch cover
- Installing the Unit

Installing the Rotary Switch Cover

Use the two cover mounting holes to secure the rotary switch cover with screws.



Tighten the M3 screws to the following torque. You can maintain the IP65/IP67 protective structure when the screws are tightened to the specified tightening torque.

Tightening location	Screw size	Tightening torque
Rotary switch cover mounting holes	M3	0.4 to 0.6 N·m

Precautions for Correct Use

- Do not allow oil to adhere to the screws. Oil adhesion may damage the screws.
- Tighten the screws with an appropriate screwdriver. Tightening a screw with an inappropriate screwdriver may damage the screw.

Additional Information

The cover is installed at shipment.

Installing the Unit

Secure the Safety I/O Block with screws using the two Unit mounting holes.
There is a mounting hole at the top and another at the bottom of the Unit. Refer to *A-1 Dimensions* on page A-2 for details on the installation dimensions.
Tighten the M5 screws to the following torque.

Tightening location	Screw size	Tightening torque
Unit mounting holes	M5	1.47 to 1.96N·m

Precautions for Correct Use

- Install the Unit properly. The Unit may be affected by vibration if it is not installed properly, which may cause failure.
- Do not allow oil to adhere to the screws. Oil adhesion may damage the screws.
- Tighten the screws with an appropriate screwdriver. Tightening a screw with an inappropriate screwdriver may damage the screw.

5-2 EtherNet/IP Network Wiring

This section describes how to install the EtherNet/IP network for the Safety I/O Block.

5-2-1 Installation Precautions

Basic precautions for the installation of an EtherNet/IP network for the Safety I/O Block are provided below.

Precautions when Installing a Network

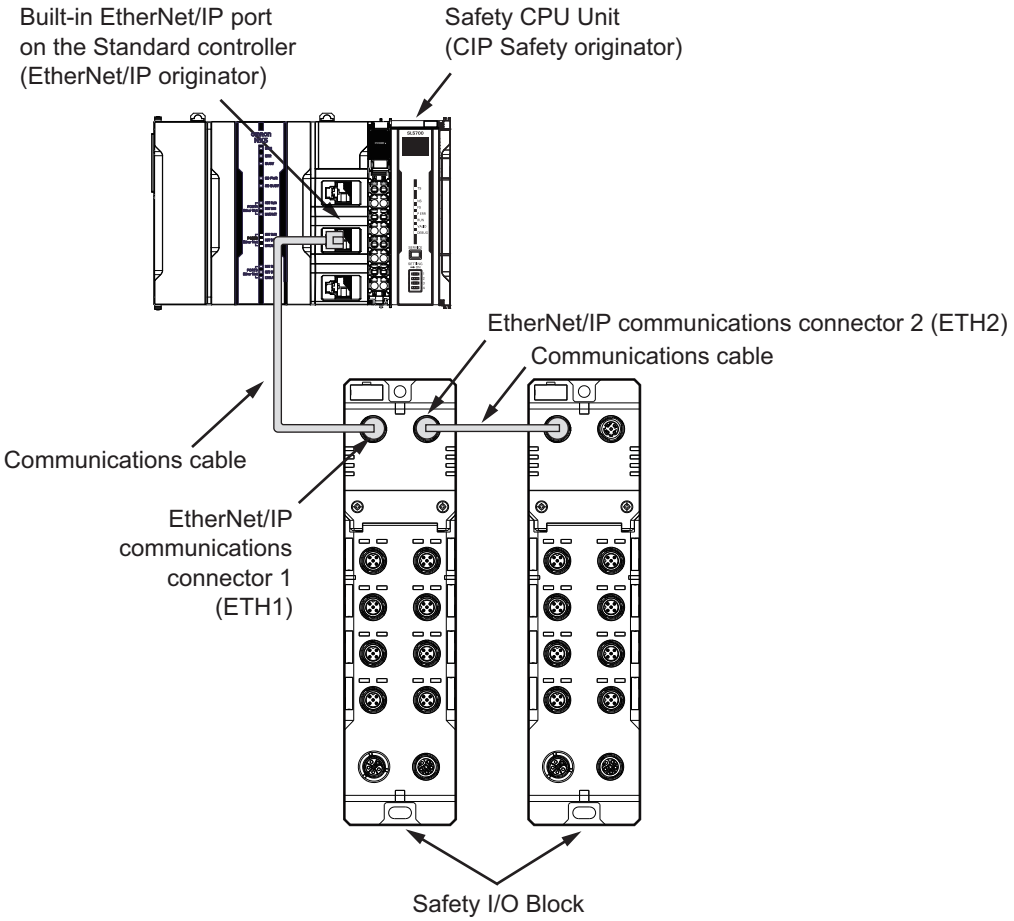
- When you install an EtherNet/IP network, take sufficient safety precautions and perform the installation according to all applicable standards and specifications.
  An expert well versed in safety measures and the standards and specifications should be asked to perform the installation.
- Do not install EtherNet/IP network equipment near sources of noise. If the network must be installed in an area with noise, take steps to address the noise, such as placing equipment in metal cases.

Precautions When Installing Communications Cables

- To maintain the IP65/IP67 protective structure of the Safety I/O Block, use the communications cables shown in *5-5-1 Ethernet Cables* on page 5-29 for the communications connectors used.
- To maintain the IP65/IP67 protective structure of the Safety I/O Block, use the waterproof covers shown in *5-5-4 Waterproof Covers for Connectors* on page 5-38 for any unused communications connectors.
- When using screw connectors, use the correct wiring tool to tighten them to the specified torque.
- When you connect a communications cable to a device with an RJ45 modular connector, firmly insert the communications cable connector until it locks in place.
- Check the following items on the communications cables that are used.
  Are there any breaks?
  Are there any shorts?
  Are there any connector problems?
- Do not lay the communications cables together with high-voltage lines.
- Do not lay the communications cables near devices that generate noise.
- Do not lay the communications cables in locations subject to high temperatures or high humidity.
- Do not use the communications cables in locations subject to excessive dust, oil mist, or other contaminants.
- There are limitations on the bending radius of communications cables. Check the specifications of the communications cable for the bending radius.
- Using a communications cable whose cable shield is not connected to the connector hoods at both ends may decrease noise immunity. For communications cables, use Ethernet cables shown in the Connected Devices section. These communications cables have a cable shield that is connected to the connector hoods at both ends.

5-2-2 Connecting Communications Cables

Cable connections can be made freely in EtherNet/IP networks.
The following figure shows a connection example of line topology.
Connect the communications cable from the EtherNet/IP originator to a communications connector on the first Safety I/O Block. Then, connect another communications cable from the other communications connector on the first Unit to a communications connector on the second Safety I/O Block.



There is no need to distinguish between the communications connectors, i.e., ETH1 and ETH2. To establish a star connection that uses only one connector, you can connect the communications cable to either ETH1 or ETH2.

Connection Procedure Using Smartclick Connectors

This section describes the procedures for connecting and disconnecting when using Smartclick connector type cables.

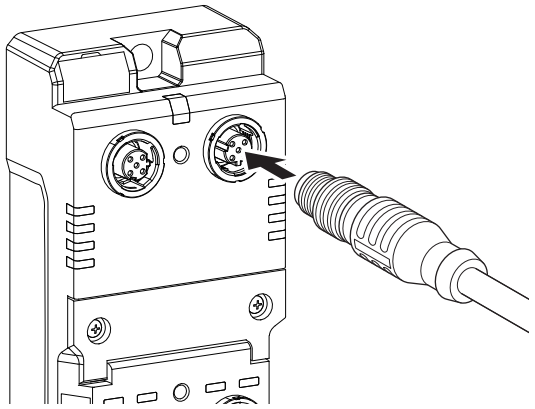
● Communications Cables

For communications cables, use the Ethernet cables shown in *5-5-1 Ethernet Cables* on page 5-29.

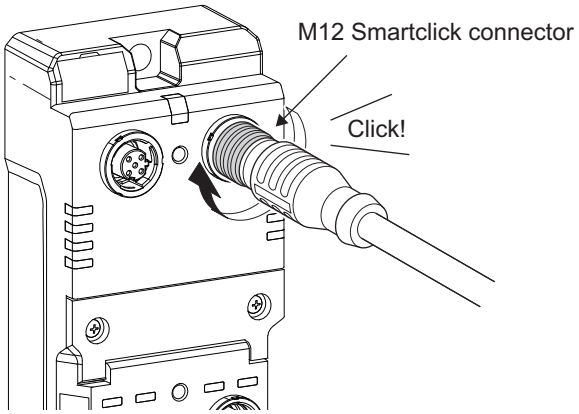
● Connection Procedure (Smartclick Connector)

The procedure to connect a communications cable is as follows. Turn OFF the Unit/input power supply and output power supply to the Safety I/O Block and the power supply to the devices to communicate with the Unit before you connect a communications cable.

1 Push the M12 plug (male) of the Ethernet cable into the communications connector (female) of the Safety I/O Block while being careful about the orientation of the communications connector.



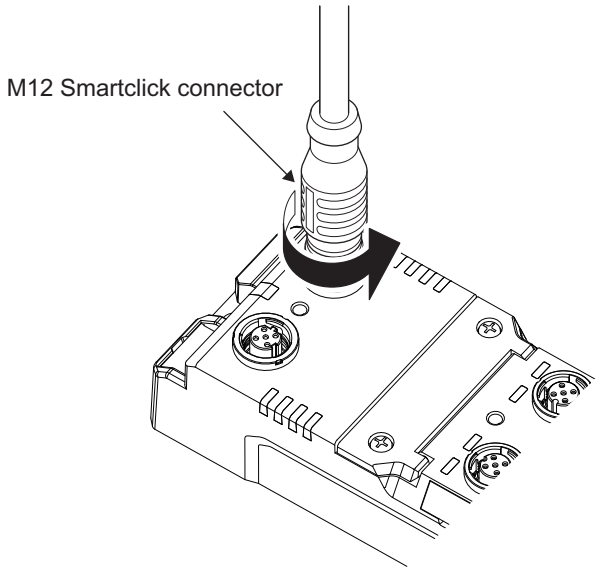
2 Insert the M12 Smartclick connector of the Ethernet cable all the way in and then turn it approximately 1/8 of a turn in the direction shown in the figure below.



● Removal Procedure (Smartclick Connector)

The procedure to remove a communications cable is as follows. Turn OFF the Unit/input power supply and output power supply to the Safety I/O Block and the power supply to the devices to communicate with the Unit before you remove a communications cable.

1 Turn the M12 Smartclick connector of the Ethernet cable approximately 1/8 of a turn in the direction shown in the figure below and then remove the cable.



Connection Procedure Using Screw Connectors

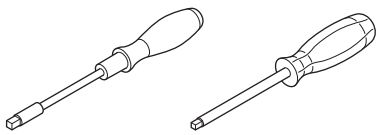
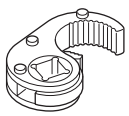
This section describes the procedures for connecting and disconnecting when using screw connector type cables.

● Communications Cables

For communications cables, use the Ethernet cables shown in *5-5-1 Ethernet Cables* on page 5-29.

● Tightening Tools

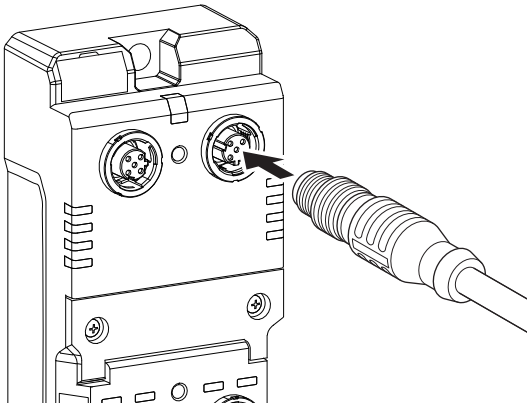
Use the following tools to tighten the M12 screw connectors of the Ethernet cables to the specified torque.

Name and appearance	Manufacturer	Model
• M12 torque handle Product, setting aid for torque  • M12 attachment 	Weidmuller	Screwty-M12-DM

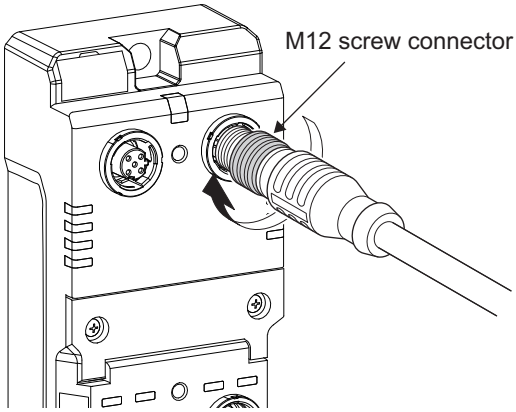
● Connection Procedure (Screw Connector)

The procedure to connect a communications cable is as follows. Turn OFF the Unit/input power supply and output power supply to the Safety I/O Block and the power supply to the devices to communicate with the Unit before you connect a communications cable.

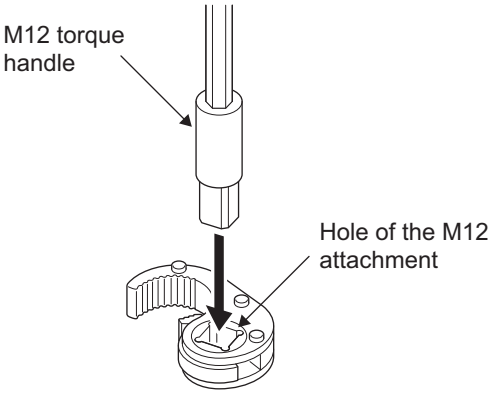
1 Push the M12 plug (male) of the Ethernet cable into the communications connector (female) of the Safety I/O Block while being careful about the orientation of the communications connector.



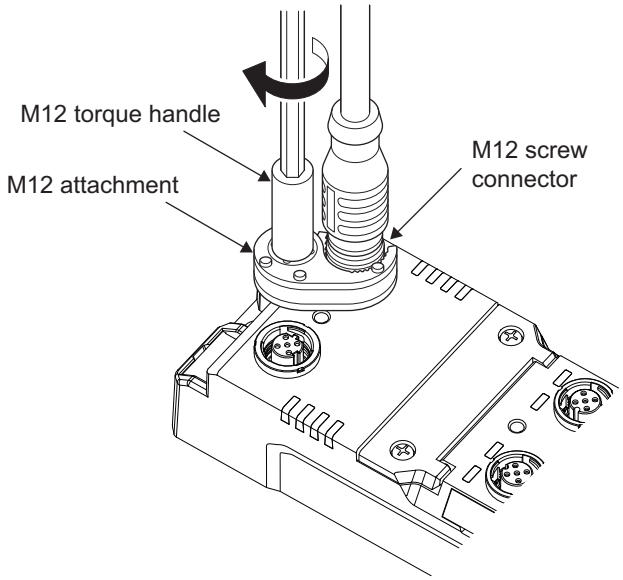
2 Rotate the M12 screw connector of the Ethernet cable in the direction shown in the following figure to tighten it. Tighten the connector before tightening it to the specified torque.



3 Set the M12 torque handle to the specified torque. Then, insert the torque handle into the tightening hole of the M12 attachment. When you tighten the connector, place the M12 attachment in the orientation shown in the following figure and insert the torque handle.
Refer to *Tightening Torque* on page 5-11 for information on the specified torque.



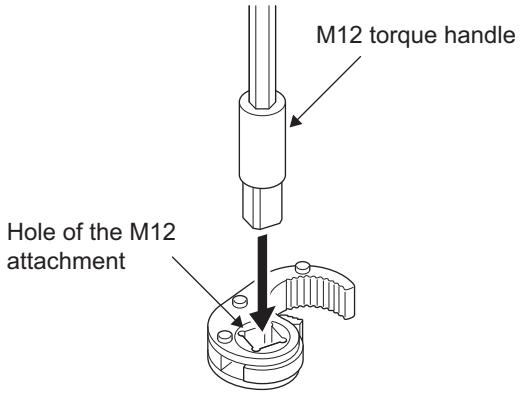
4 Mount the M12 attachment on the M12 screw connector of the Ethernet cable. After you mount the M12 attachment, rotate the M12 torque handle in the direction shown in the following figure to tighten the M12 screw connector to the specified torque.



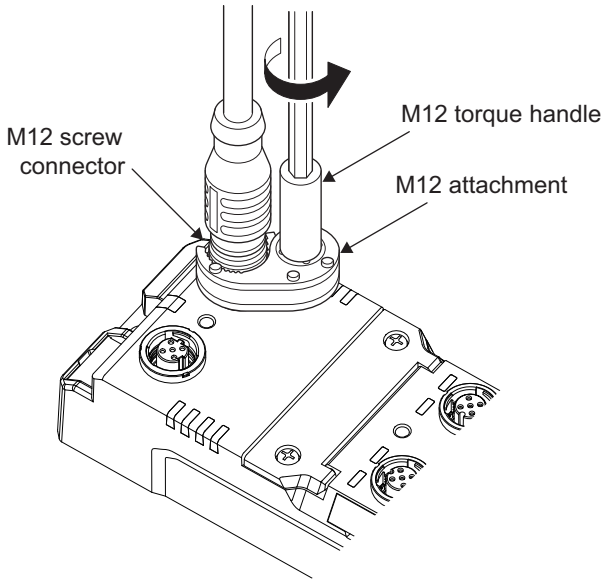
● Removal Procedure (Screw Connector)

The procedure to remove a communications cable is as follows. Turn OFF the Unit/input power supply and output power supply to the Safety I/O Block and the power supply to the devices to communicate with the Unit before you remove a communications cable.

1 Insert the M12 torque handle into the tightening hole of the M12 attachment. When you remove the connector, place the M12 attachment upside down so as it is in the opposite orientation to that for connecting.



2 Mount the M12 attachment on the M12 screw connector of the Ethernet cable. After you mount the M12 attachment, rotate the M12 torque handle in the direction shown in the following figure to loosen the M12 screw connector.



3 Rotate the M12 screw connector of the Ethernet cable in the direction opposite to the connection direction to remove the cable.

Tightening Torque

Tighten the M12 screw connectors of Ethernet cables to the following torque.
You can maintain the IP65/IP67 protective structure when the screw connectors are tightened to a suitable tightening torque.

Tightening location	Screw size	Tightening torque
EtherNet/IP Communications Connectors	M12	0.5 to 0.6 N·m*1

***1.** For the Smartclick connector type, torque management is not required. Insert the connectors all the way in and then turn the approximately 1/8 of a turn.

Waterproof Covers

Attach the waterproof covers shown in *5-5-4 Waterproof Covers for Connectors* on page 5-38 to any unused EtherNet/IP communications connectors.

5-3 Wiring the Power Supply

This section describes how to wire the Unit/input power supply and output power supply to the Safety I/O Block.

⚠ 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.
- Follow the instructions in this manual to correctly perform power supply design and wiring. Inputting voltages or currents that are outside of the specified ranges, as well as incorrect wiring, may cause failure or fire.



5-3-1 Installation Precautions

Basic precautions for the installation of power supplies to the Safety I/O Block are provided below.

- To maintain the IP65/IP67 protective structure of the Safety I/O Block, use the power supply cables shown in *5-5-2 Power Supply Cables* on page 5-31 for the power supply connectors.
- To maintain the IP65/IP67 protective structure of the Safety I/O Block, use the waterproof covers shown in *5-5-4 Waterproof Covers for Connectors* on page 5-38 for any unused power supply connectors.
- Do not lay the communications cables in locations subject to high temperatures or high humidity.
- Do not use the communications cables in locations subject to excessive dust, oil mist, or other contaminants.
- There are limitations on the bending radius of power supply cables. Check the specifications of the power supply cables for the bending radius.

5-3-2 Power Supply Cables, Tightening Tools and Tightening Torque to Use

This section describes the power supply cables, tightening tools and tightening torque to use with the Safety I/O Block.

● Power Supply Cables

For power supply cables, use the power supply cables shown in *5-5-2 Power Supply Cables* on page 5-31.

● Tightening Tools

For the screw connector type power supply cable, please use the tightening tool recommended by the respective manufacturer.
For the Smartclick connector type power supply cable, the tightening tools are not required.

● Tightening Torque

Tighten to the following torque for the screw connector type power supply cable. You can maintain the IP65/IP67 protective structure when the screw connectors are tightened to a suitable tightening torque.

Tightening location	Screw size	Tightening torque
Power supply connector	M12	0.39 to 0.49 N·m*1

***1.** For the Smartclick connector type, torque management is not required. Insert the connectors all the way in and then turn the approximately 1/8 of a turn.

5-3-3 Connecting Power Supply Cables to External Power Supplies

Use a power supply cable shown in *5-5-2 Power Supply Cables* on page 5-31 for an external power supply. This section describes the connection method when using OMRON M12 L-coding power supply cables (XS5F-L521-□12-F, XS5W-L521-□12-F).

The XS5W-L521-□12-F is a cable with connectors on both ends, and the XS5F-L521-□12-F is a discrete wire cable.

Connect the M12 socket end (female end) of the power supply cable to the power supply connector (input) of the Safety I/O Block, and the other end to the Power Supply Unit.

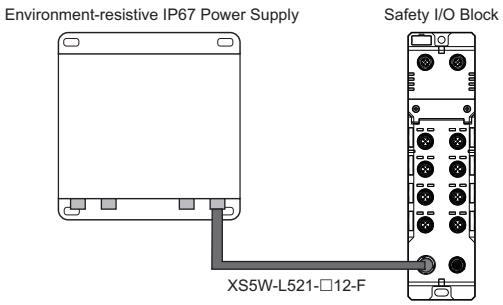
Connecting with Environment-resistive IP67 Power Supply (S8NR-S Series)

When using an Environment-resistive IP67 Power Supply (S8NR-S Series), use a power supply cable with connectors on both ends (XS5W-L521-□12-F).

The appearance of the XS5W-L521-□12-F is shown below.



Connect the M12 plug end (male end) to the Environment-resistive IP67 Power Supply as shown below.



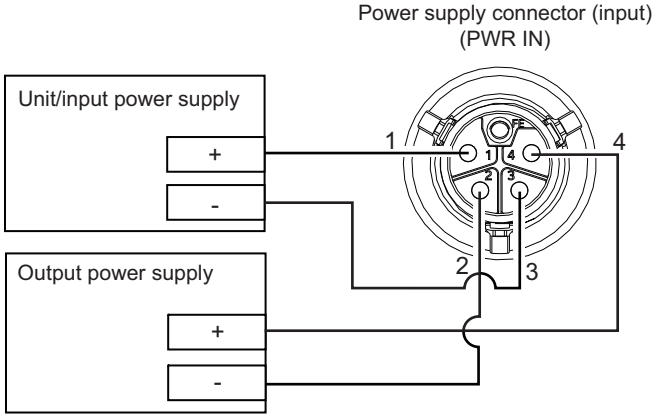
Connecting with a General-purpose Power Supply Unit

When using a general-purpose power supply unit, use a discreet wire power supply cable (XS5F-L521-□12-F).

The appearance of the XS5F-L521-□12-F is shown below.



Connect the discrete wire end of the power supply cable to an external power supply according to the following wiring diagram.

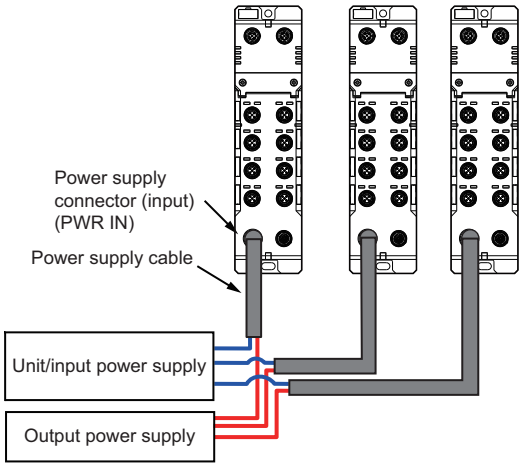


Pin arrangement of power supply connector (input)		External power supply wiring	Color of power supply cable discrete wire
Pin No.	Signal name		
1	U/IN P+	Connect the positive (+) side of the Unit/input power supply.	Brown
2	OUT P-	Connect the negative (-) side of the output power supply.	White
3	U/IN P-	Connect the negative (-) side of the Unit/input power supply.	Blue
4	OUT P+	Connect the positive (+) side of the output power supply.	Black
FE (Functional Earth)	FG	Frame ground	Gray

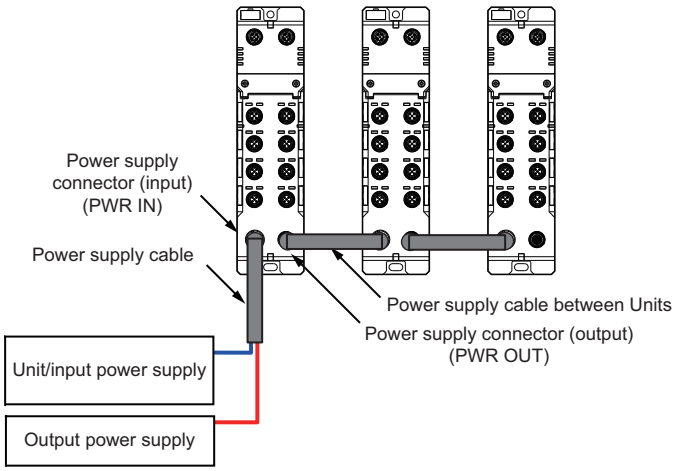
5-3-4 Connecting Power Supply Cables

There are two methods to supply external power to the Safety I/O Block as shown below.

- Direct power supply



- Power supply with through-wiring



For the direct power supply, the power supply connector (output) of each Safety I/O Block is not used.
For the power supply with through-wiring, the power supply connector (output) of each Safety I/O Block is used. However, the power supply connector (output) of the last Unit to supply power is not used.

Refer to *4-1-2 Power Supply System* on page 4-2 for details on the power supply method.

Precautions for Safe Use

The maximum power supply current is 9 A, which is the sum of the Unit/input power supply current and the output power supply current. Do not use the Unit beyond the maximum power supply current. Otherwise, an excess current flows through the power supply cable, and it may cause fire.

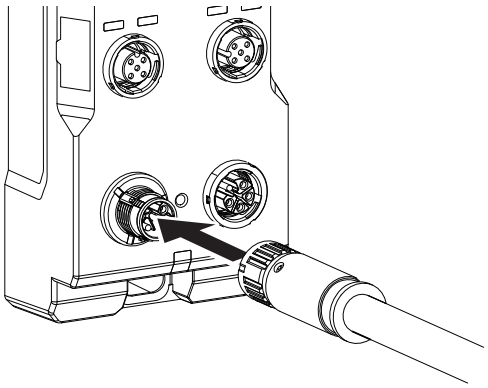
Precautions for Correct Use

Always use separate power supplies for the Unit/input power supply and the output power supply. If you supply power from the same power supply, load variations in output devices may cause malfunctions.

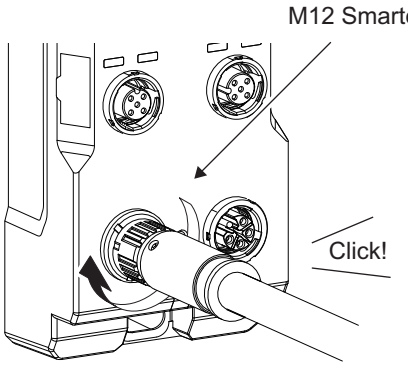
Connection Procedure

This section describes the procedures for connecting when using OMRON M12 L-coding power supply cables (XS5F-L521-□12-F, XS5W-L521-□12-F).
Use the following procedures to connect a power supply cable. Turn OFF the Unit/input power supply and output power supply before you connect a power supply cable.

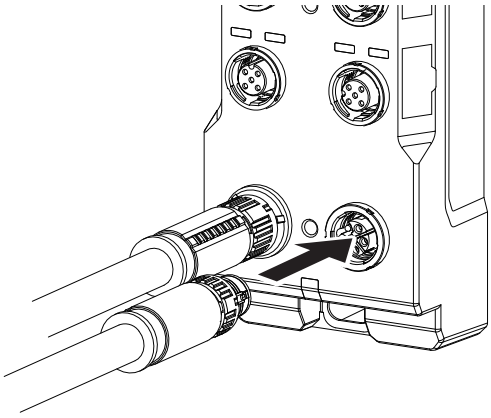
1 Push the M12 socket (female) of the power supply cable into the power supply connector (input) (male) of the Safety I/O Block while being careful about the orientation of the power supply connector.



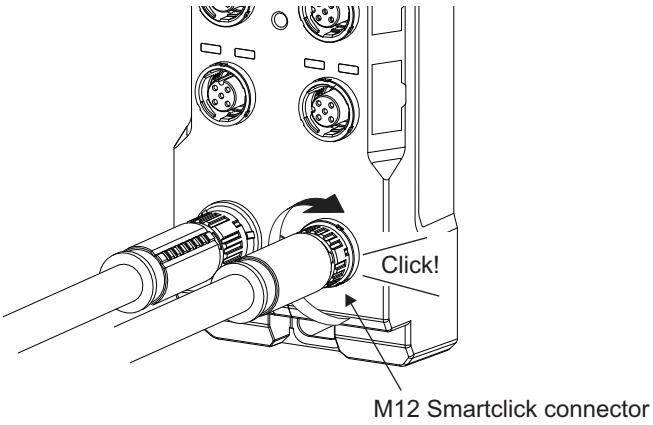
2 Insert the M12 Smartclick connector of the power supply cable all the way in and then turn it approximately 1/8 of a turn in the direction shown in the figure below.



3 When the power is supplied with through-wiring, push the M12 socket (male) of the power supply cable into the power supply connector (output) (female) of the Safety I/O Block while being careful about the orientation of the power supply connector.



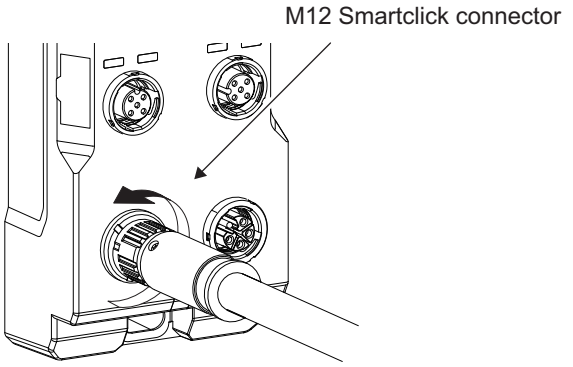
4 Insert the M12 Smartclick connector of the power supply cable all the way in and then turn it approximately 1/8 of a turn in the direction shown in the figure below.



Removal Procedure

This section describes the procedures for removing when using OMRON M12 L-coding power supply cables (XS5F-L521-□12-F, XS5W-L521-□12-F).
The procedure to remove a power supply cable is as follows. Turn OFF the Unit/input power supply and output power supply before you remove a power supply cable.

1 Turn the M12 Smartclick connector of the power supply cable approximately 1/8 of a turn in the direction shown in the figure below and then remove the cable.



2 Remove the cable with the same procedure also when supplying power with through-wiring.

Waterproof Covers

Attach the waterproof covers shown in *5-5-4 Waterproof Covers for Connectors* on page 5-38 to any unused power supply connectors.

5-4 Wiring I/O Cables

This section describes how to wire I/O cables for connecting external devices to the Safety I/O Block.

5-4-1 Installation Precautions

Basic precautions for the installation of I/O cables for the Safety I/O Block are provided below.

- To maintain the IP65/IP67 protective structure of the Safety I/O Block, use the I/O cables shown in *Smartclick Connector Types* on page 5-34 and *Screw Connectors* on page 5-37 for the I/O connectors.
- To maintain the IP65/IP67 protective structure of the Safety I/O Block, use the waterproof covers shown in *5-5-4 Waterproof Covers for Connectors* on page 5-38 for any unused I/O connectors.
- When using screw connectors, use the correct wiring tool to tighten them to the specified torque.
- Do not lay the communications cables in locations subject to high temperatures or high humidity.
- Do not use the communications cables in locations subject to excessive dust, oil mist, or other contaminants.
- There are limitations on the bending radius of I/O cables. Check the specifications of the I/O cables to be used for the bending radius.

5-4-2 Connecting I/O Cables

This section describes the connection procedure, removal procedure, tightening torque, and waterproof covers for I/O cables.

Connection Procedure Using Smartclick Connectors

This section describes the procedures for connecting and disconnecting I/O cables when using Smartclick connector type cables.

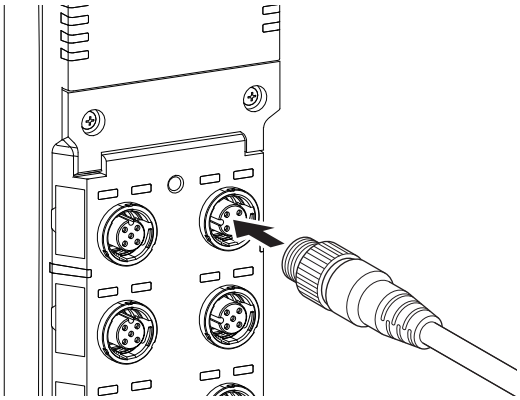
● I/O Cables

For I/O cables, use the I/O cables shown in *Smartclick Connector Types* on page 5-34.

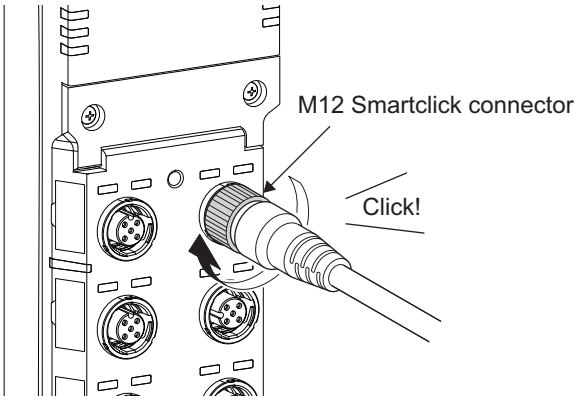
● Connection Procedure (Smartclick Connector)

The procedure to connect an I/O cable is as follows. Turn OFF the Unit/input power supply and output power supply of the Safety I/O Block before you connect an I/O cable.

1 Push the M12 plug (male) of the I/O cable into the I/O connector (female) of the Safety I/O Block while being careful about the orientation of the I/O connector.



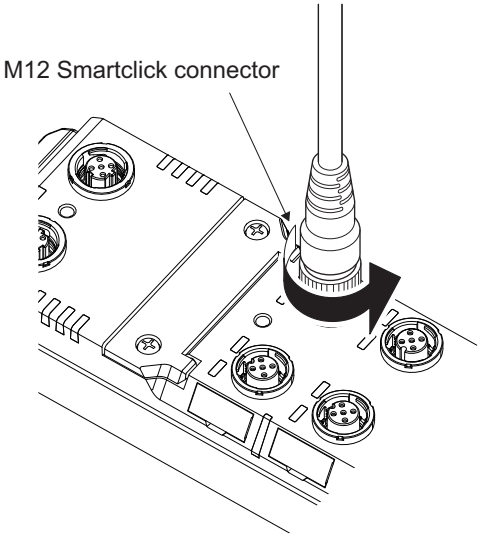
2 Insert the M12 Smartclick connector of the I/O cable all the way in and then turn it approximately 1/8 of a turn in the direction shown in the figure below.



● Removal Procedure (Smartclick Connector)

The procedure to remove an I/O cable is as follows. Turn OFF the Unit/input power supply and output power supply of the Safety I/O Block before you remove an I/O cable.

1 Turn the M12 Smartclick connector of the I/O cable approximately 1/8 of a turn in the direction shown in the figure below and then remove the cable.



Connection Procedure Using Screw Connectors

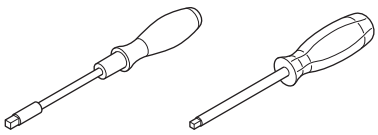
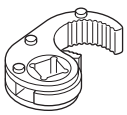
This section describes the procedures for connecting and disconnecting I/O cables when using screw connector type cables.

● I/O Cables

For I/O cables, use the I/O cables shown in *Screw Connectors* on page 5-37.

● Tightening Tools

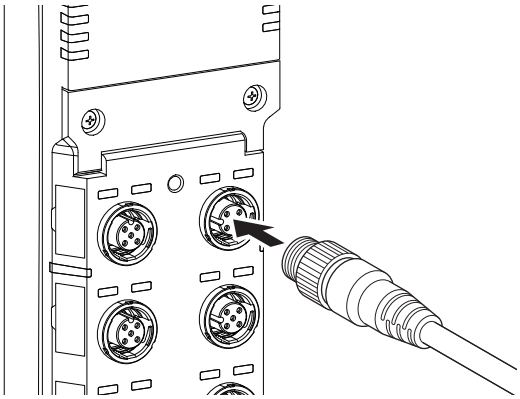
Use the tools shown below to tighten the M12 screw connectors of I/O cables to the specified torque.

Name and appearance	Manufacturer	Model
• M12 torque handle Product, setting aid for torque  • M12 attachment 	Weidmuller	Screwty-M12-DM

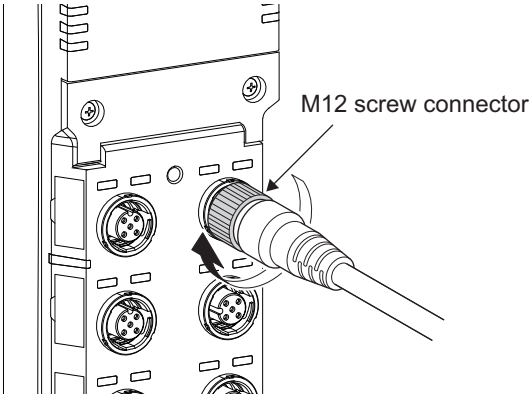
● Connection Procedure (Screw Connector)

The procedure to connect an I/O cable is as follows. Turn OFF the Unit/input power supply and output power supply of Safety I/O Block before you connect an I/O cable.

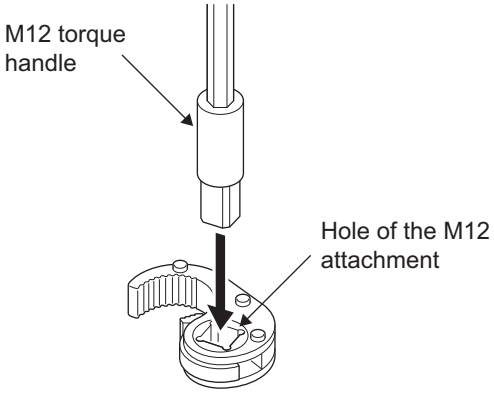
1 Push the M12 plug (male) of the I/O cable into the I/O connector (female) of the Safety I/O Block while being careful about the orientation of the I/O connector.



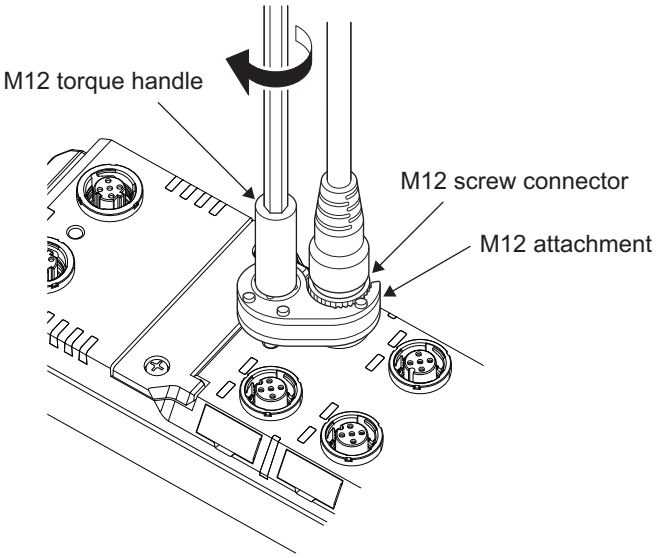
2 Rotate the M12 screw connector of the I/O cable in the direction shown in the following figure to tighten it. Tighten the connector before tightening it to the specified torque.



3 Set the M12 torque handle to the specified torque. Then, insert the torque handle into the tightening hole of the M12 attachment. When you tighten the connector, place the M12 attachment in the orientation shown in the following figure and insert the torque handle.
Refer to *Tightening Torque* on page 5-24 for information on the specified torque.



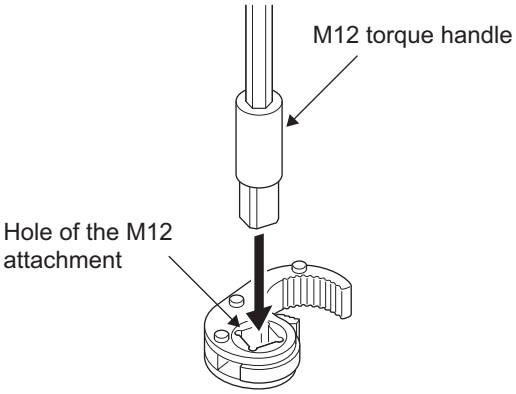
4 Mount the M12 attachment on the M12 screw connector of the I/O cable. After you mount the M12 attachment, rotate the M12 torque handle in the direction shown in the following figure to tighten the M12 screw connector to the specified torque.



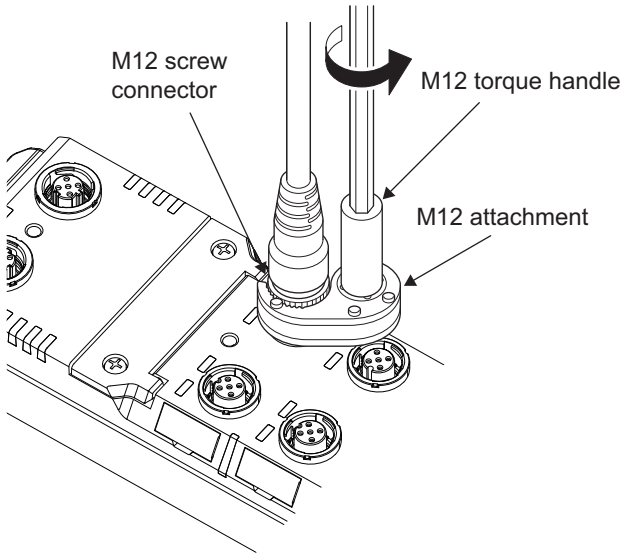
● Removal Procedure (Screw Connector)

The procedure to remove an I/O cable is as follows. Turn OFF the Unit/input power supply and output power supply of the Safety I/O Block before you remove an I/O cable.

1 Insert the M12 torque handle into the tightening hole of the M12 attachment. When you remove the connector, place the M12 attachment upside down so as it is in the opposite orientation to that for connecting.



2 Mount the M12 attachment on the M12 screw connector of the I/O cable. After you mount the M12 attachment, rotate the M12 torque handle in the direction shown in the following figure to loosen the M12 screw connector.



3 Rotate the M12 screw connector of the I/O cable in the direction opposite to the connection direction to remove the cable.

Tightening Torque

Tighten the M12 screw connectors of the I/O cables to the following torque.
You can maintain the IP65/IP67 protective structure when the screw connectors are tightened to a suitable tightening torque.

Tightening location	Screw size	Tightening torque
I/O connector	M12	0.5 to 0.6 N·m*1

***1.** For the Smartclick connector type, torque management is not required. Insert the connectors all the way in and then turn the approximately 1/8 of a turn.

Waterproof Covers

Attach the waterproof covers shown in *5-5-4 Waterproof Covers for Connectors* on page 5-38 to any unused I/O connectors.

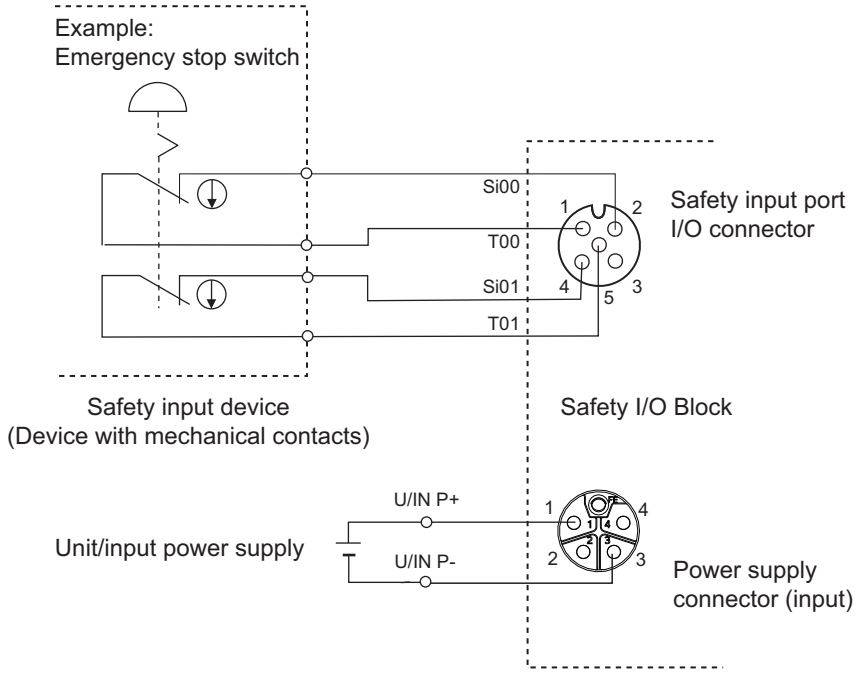
5-4-3 Wiring Examples

Examples of wiring between the I/O connectors of the Safety I/O Block and a connected external device are provided below.

- Safety input devices (devices with mechanical contacts)
- Safety input devices (devices with semiconductor outputs)
- Safety input devices (safety light curtains)
- Safety output devices
- DC shutoff box (S8R-BB Series)
- Connecting I/O cables between units

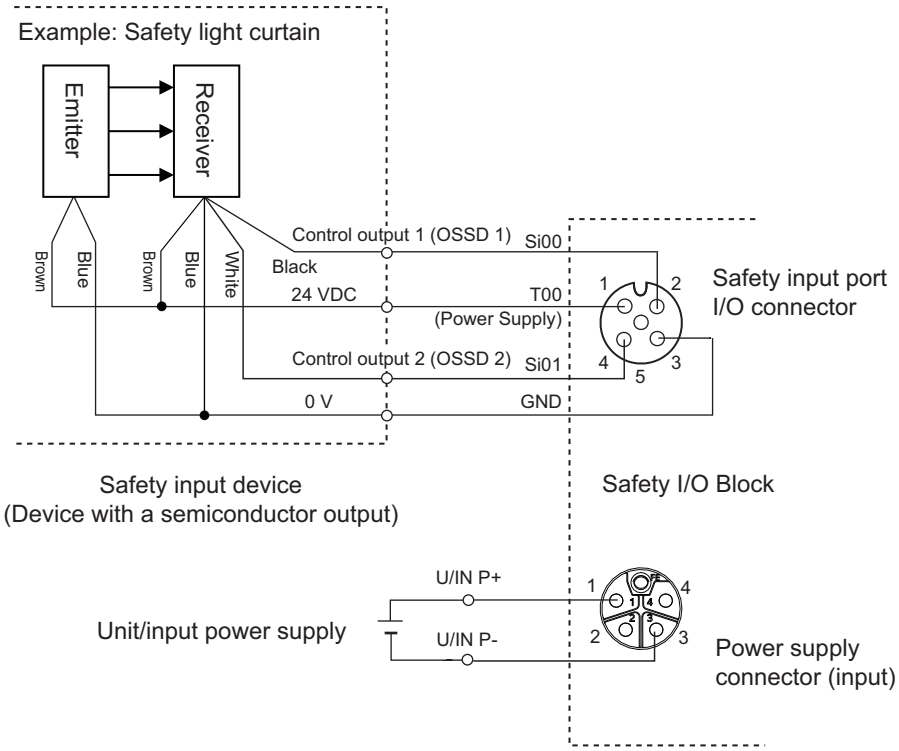
Safety Input Devices (Devices with Mechanical Contacts)

The following figure shows an example of the wiring between an emergency stop switch, safety limit switch, or other safety input device with mechanical contacts and the Safety I/O Block.



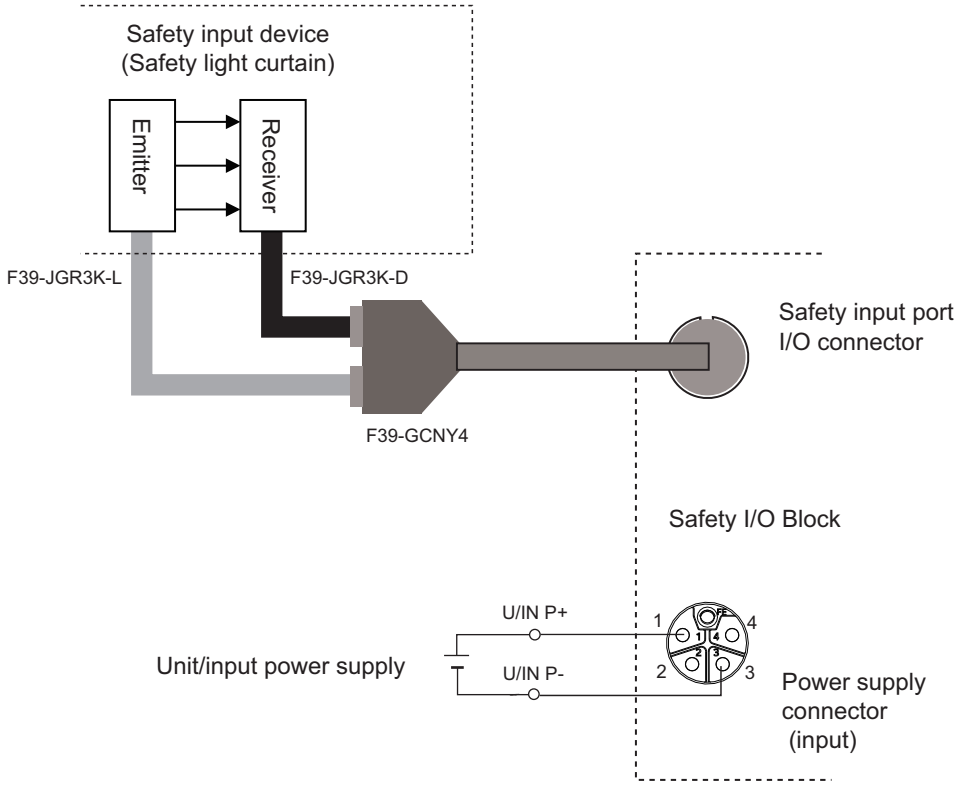
Safety Input Devices (Devices with Semiconductor Outputs)

The following shows an example of the wiring between a light curtain or other safety input device with semiconductor output and the Safety I/O Block.



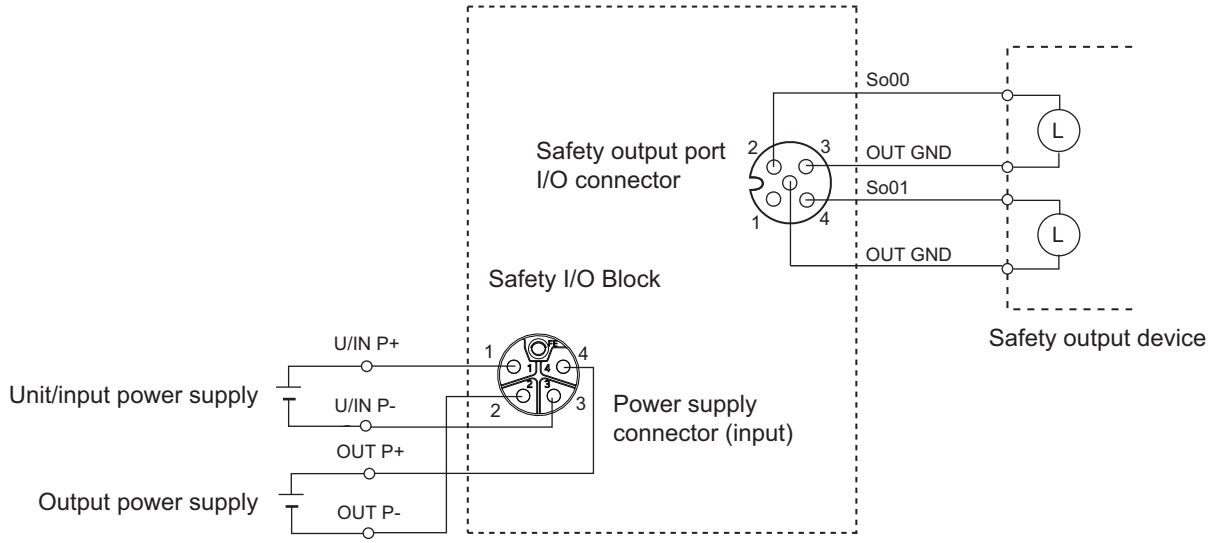
Safety Input Devices (Safety Light Curtains)

The following figure shows a wiring example when using the F39-GCNY4 to connect with a light curtain.



Safety Output Devices

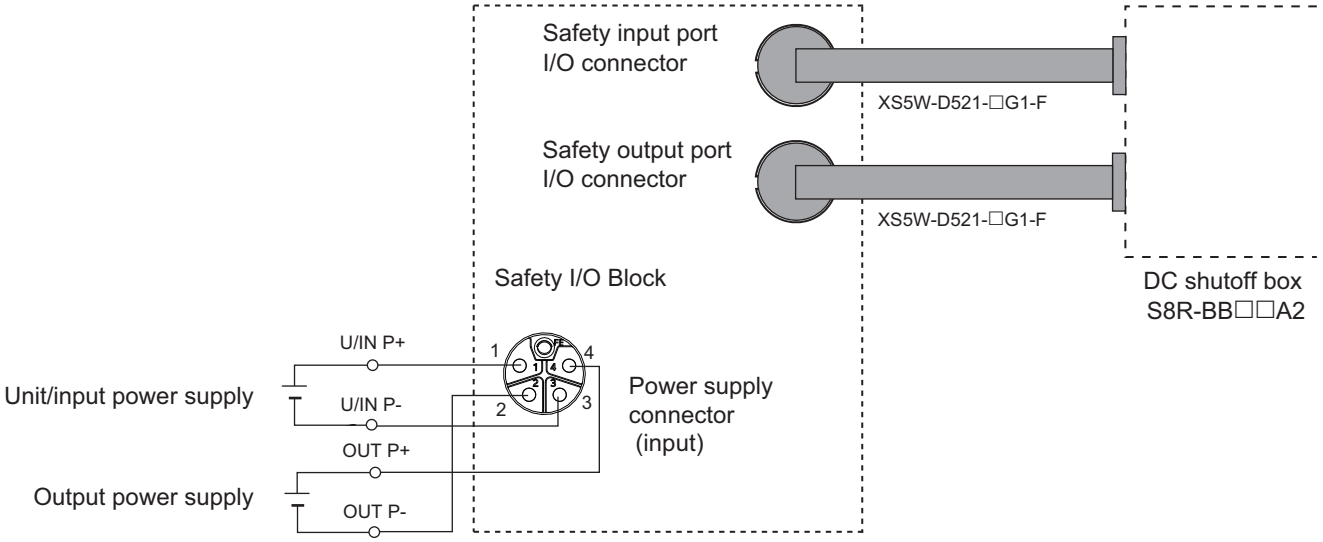
The following figure shows an example of the wiring between a safety relay or other safety output device and the Safety I/O Block.
The output is PNP output.



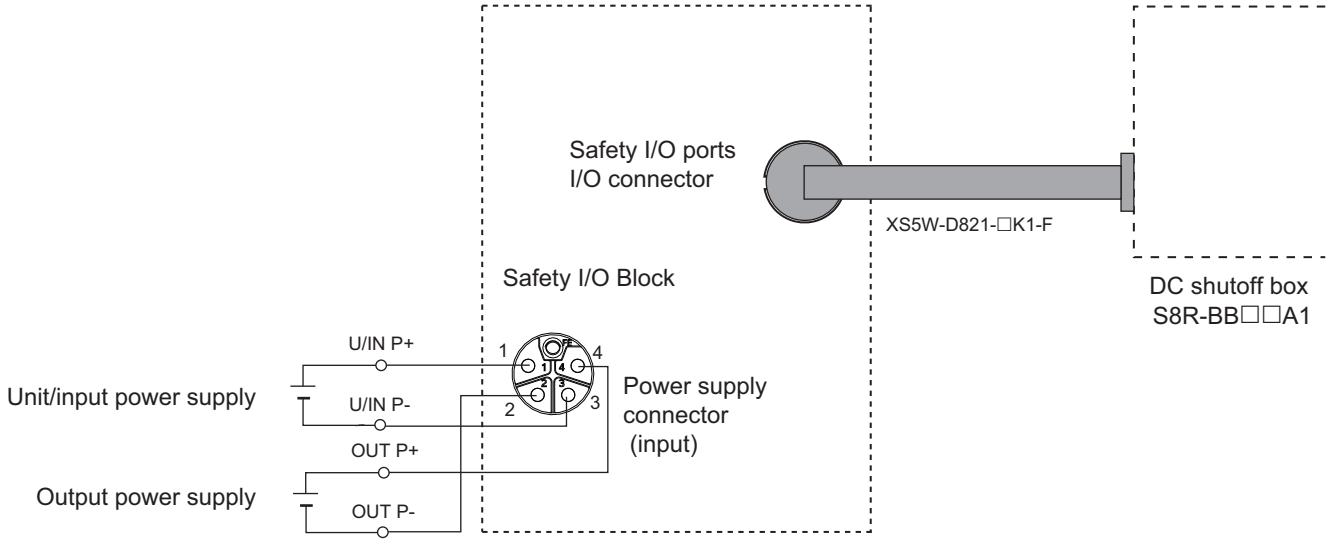
DC Shutoff Box (S8R-BB Series)

The following figures show examples of the wiring between the DC shutoff box (S8R-BB series) and the Safety I/O Block. Turn OFF the Unit/input power supply and output power supply to the Safety I/O Block and the power supply to the devices to communicate with the Unit before you connect a communications cable.

- When using NXR-SXD1204-CST

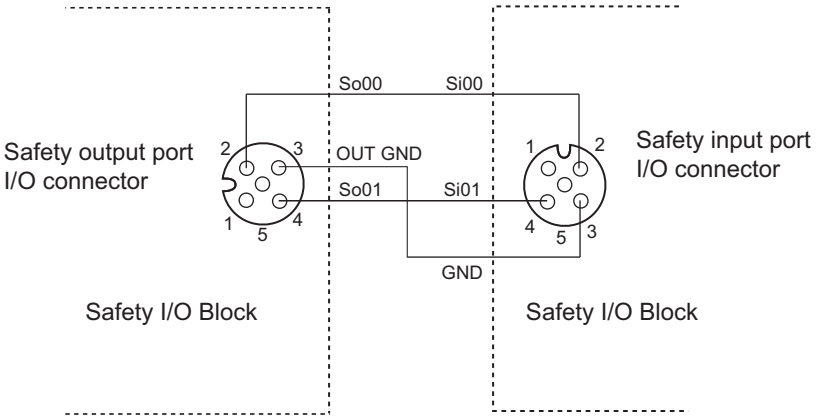


- When using NXR-SXD1204B-CST



Connecting I/O cables between units

The following figure shows an example of wiring when connecting safety I/O ports between units.



Precautions for Correct Use

- When connecting I/O cables between units, do not connect pin number 5. A short circuit occurs between the **Test output** of the safety input port and the **Output power supply -** of the safety output port, resulting in an overcurrent abnormality at the test output terminal.
- When connecting 5-pin I/O cables between units, set the test output mode to **Not Used** in the safety input terminal settings.

5-5 Connected Devices

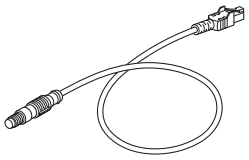
This section introduces connection related equipment for wiring the Safety I/O Block.

5-5-1 Ethernet Cables

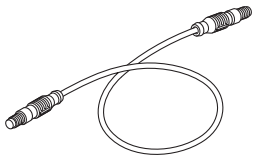
This section introduces the Ethernet cables to use with the Safety I/O Block.
There are the following connectors.

- Smartclick connector
- Screw connector

● Connection Cables Between the Safety I/O Block and EtherNet/IP Target with RJ45 Connector

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
Industrial Ethernet Connectors with Cable 	OMRON Corporation	M12 plug (D-coding, male) to RJ45	4	Smart-click connector	Straight/ straight	0.5 m	XS5W-T421-BMC-SS
						1 m	XS5W-T421-CMC-SS
						2 m	XS5W-T421-DMC-SS
						3 m	XS5W-T421-EMC-SS
						5 m	XS5W-T421-GMC-SS
						10 m	XS5W-T421-JMC-SS
				Screw connector		0.5 m	XS2W-T421-BMC-SS
						1 m	XS2W-T421-CMC-SS
						2 m	XS2W-T421-DMC-SS
						3 m	XS2W-T421-EMC-SS
						5 m	XS2W-T421-GMC-SS
						10 m	XS2W-T421-JMC-SS

● Connection Cables Between Safety I/O Block

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
Industrial Ethernet Connectors with Cable 	OMRON Corporation	M12 plug (D-coding, male) to M12 plug (D-coding, male)	4	Smartclick connector	Straight/straight	0.5 m	XS5W-T421-BM2-SS
						1 m	XS5W-T421-CM2-SS
						2 m	XS5W-T421-DM2-SS
						3 m	XS5W-T421-EM2-SS
						5 m	XS5W-T421-GM2-SS
						10 m	XS5W-T421-JM2-SS
				Screw connector		0.5 m	XS2W-T421-BM2-SS
						1 m	XS2W-T421-CM2-SS
						2 m	XS2W-T421-DM2-SS
						3 m	XS2W-T421-EM2-SS
						5 m	XS2W-T421-GM2-SS
						10 m	XS2W-T421-JM2-SS

5-5-2 Power Supply Cables

This section shows the power supply cables that are used with the Safety I/O Block.

There are the following connectors.

- Screw connector
- Smartclick connector

● Screw Connectors

This section shows the power supply cables with screw connectors.

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
M12 L-coding power supply cable (M12 straight female to discrete wires)	OMRON Corporation	M12 socket (L-coding, female) to discrete wires	5	Screw connector	Straight	2 m	XS2FP-L521-0200
						5 m	XS2FP-L521-0500
						10 m	XS2FP-L521-1000
	Murrelektronik GmbH	M12 socket (L-coding, female) to discrete wires	5	Screw connector	Straight	2 m	7000-P4221-P040200
						5 m	7000-P4221-P040500
						10 m	7000-P4221-P041000
M12 L-coding power supply cable (M12 straight male to M12 straight female)	OMRON Corporation	M12 plug (L-coding, male) to M12 socket (L-coding, female)	5	Screw connector	Straight/ straight	2 m	XS2WP-L521-0200
						5 m	XS2WP-L521-0500
						10 m	XS2WP-L521-1000
	Murrelektronik GmbH	M12 plug (L-coding, male) to M12 socket (L-coding, female)	5	Screw connector	Straight/ straight	2 m	7000-P4241-P040200
						5 m	7000-P4241-P040500
						10 m	7000-P4241-P041000

● Smartclick Connector Types

This section shows the power supply cables with Smartclick connectors. The protective structure of XS5F-L521-□12-F and XS5W-L521-□12-F is IP65.

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
M12 L-coding power supply cable (M12 straight female to discrete wires) 	OMRON Corporation	M12 socket (L-coding, female) to discrete wires	5	Smartclick connector	Straight	0.5 m	XS5F-L521-B12-F
						1 m	XS5F-L521-C12-F
						2 m	XS5F-L521-D12-F
						3 m	XS5F-L521-E12-F
						5 m	XS5F-L521-G12-F
						10 m	XS5F-L521-J12-F
						15 m	XS5F-L521-K12-F
						20 m	XS5F-L521-L12-F

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
M12 L-coding power supply cable (M12 straight male to M12 straight female) 	OMRON Corporation	M12 plug (L-coding, male) to M12 socket (L-coding, female)	5	Smartclick connector	Straight/straight	0.5 m	XS5W-L521-B12-F
						1 m	XS5W-L521-C12-F
						2 m	XS5W-L521-D12-F
						3 m	XS5W-L521-E12-F
						5 m	XS5W-L521-G12-F
						10 m	XS5W-L521-J12-F
						15 m	XS5W-L521-K12-F
						20 m	XS5W-L521-L12-F

5-5-3 I/O Cables

This section shows the I/O cables that are used with the Safety I/O Block.

Direct Connection or Extension Connection Cables

These cables can be used to directly connect to a device with an M12 plug. They can also be used for an extension connection from a device or external device with an M12 plug.
There are the following connectors.

- Smartclick connector
- Screw connector

● Smartclick Connector Types

This section shows the I/O cables with Smartclick connectors.

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
XS5W Connector with Cable (M12 socket/M12 plug) 	OMRON Corporation	M12 socket (A-coding, female) to M12 plug (A-coding, male), uses DC	5	Smartclick connector	Straight/straight	0.5 m	XS5W-D521-BG1-F
						1 m	XS5W-D521-CG1-F
						2 m	XS5W-D521-DG1-F
						3 m	XS5W-D521-EG1-F
						5 m	XS5W-D521-GG1-F
						10 m	XS5W-D521-JG1-F
						15 m	XS5W-D521-KG1-F
						20 m	XS5W-D521-LG1-F
XS5H Connector with Cable (M12 plug/discrete wires) 	OMRON Corporation	M12 plug (A-coding, male), discrete wires	5	Smartclick connector	Straight	0.5 m	XS5H-D521-BG0-F
						1 m	XS5H-D521-CG0-F
						2 m	XS5H-D521-DG0-F
						3 m	XS5H-D521-EG0-F
						5 m	XS5H-D521-GG0-F

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
Safety Light Curtain Y-Joint Plug/Socket, Connectors on Both Ends (for Safety I/O Block) 	OMRON Corporation	M12 plug (A-coding, male), M12 socket (A-coding, female, 5-wire) / M12 socket (A-coding, female, 8-wire)	5 to 5/8	Smartclick connector	Straight/straight	0.5 m	F39-GCNY4
XS5W Connector with Cable (M12 Socket/M12 Plug) for NXR-SXD1204B-CST 	OMRON Corporation	M12 socket (A-coding, female) to M12 plug (A-coding, male)	8	Smartclick connector	Straight/straight	0.5 m	XS5W-D821-BK1-F
						1 m	XS5W-D821-CK1-F
						2 m	XS5W-D821-DK1-F
						3 m	XS5W-D821-EK1-F
						5 m	XS5W-D821-GK1-F
						10 m	XS5W-D821-JK1-F
						15 m	XS5W-D821-KK1-F
						20 m	XS5W-D821-LK1-F

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
XS5H Connector with Cable (M12 Plug/Discrete Wires) for NXR-SXD1204B-CST 	OMRON Corporation	M12 plug (A-coding, male), discrete wires	8	Smartclick connector	Straight	0.5 m	XS5H-D821-BK0-F
						1 m	XS5H-D821-CK0-F
						2 m	XS5H-D821-DK0-F
						3 m	XS5H-D821-EK0-F
						5 m	XS5H-D821-GK0-F

● Screw Connectors

This section shows the I/O cables with screw connectors.

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
XS2W Connector with Cable (M12 socket/M12 plug) 	OMRON Corporation	M12 socket (A-coding, female) to M12 plug (A-coding, male), uses DC	5	Screw connector	Straight/straight	2 m	XS2W-D521-DG1-A
						5 m	XS2W-D521-GG1-A
			8			2 m	XS2W-D821-DH1-C
						5 m	XS2W-D821-GH1-C

Name and appearance	Manufacturer	Specification	Number of cable conductors	Available connectors	Cable connection direction	Cable length	Model
XS2H Connector with Cable (M12 plug/discrete wires) 	OMRON Corporation	M12 plug (A-coding, male), discrete wires	5	Screw connector	Straight	0.3 m	XS2H-D521-AG0-A
						0.5 m	XS2H-D521-BG0-A
						1 m	XS2H-D521-CG0-A
						2 m	XS2H-D521-DG0-A
						5 m	XS2H-D521-GG0-A
			8			0.3 m	XS2H-D821-AH0-C
						1 m	XS2H-D821-CH0-C

5-5-4 Waterproof Covers for Connectors

These are waterproof covers for unused M12 connectors.
When you use these waterproof covers, you can maintain the IP65/IP67 protective structure.
There are the following waterproof covers.

Name and appearance	Manufacturer	Specification	Available connectors	Model
M12 Waterproof Cover 	OMRON Corporation	• M12 A-coding • M12 D-coding • M12 L-coding	Smartclick connector	XS5Z-12

5-6 Options

This section provides an overview of the options for the Safety I/O Block.

5-6-1 Markers

The following non-OMRON markers can be used as Unit identification markers and I/O identification markers. You can also print markers with a printer.

Name and appearance	Manufacturer	Specification	Model
Markers 	Phoenix Contact	White 17.5 mm × 7.5 mm	0825495

6

Operation of the Safety I/O Block

This chapter describes the various operations of the Safety I/O Block.

6-1 Overview of Operations 6-2

6-2 CIP Safety Communications 6-4

6-3 EtherNet/IP Communications 6-6

6-3-1 Tag Data Link Communications 6-6

6-3-2 Explicit Message Communications 6-6

6-4 Safety Input Functions 6-8

6-4-1 Connectable Devices 6-8

6-4-2 Test Output Function 6-10

6-4-3 Test Pulse Evaluation Function 6-10

6-4-4 Dual Channel Evaluation 6-11

6-4-5 Errors Detectable by the Diagnosis Function of Safety Input Terminals 6-12

6-4-6 Input Filter Function 6-13

6-4-7 Input Error Latch Time 6-15

6-5 Safety Output Functions 6-16

6-5-1 Connectable Devices 6-16

6-5-2 Test Pulse Evaluation Function 6-16

6-5-3 Dual Channel Evaluation 6-17

6-5-4 Errors Detectable by the Diagnosis Function of Safety Output Terminals 6-18

6-5-5 Output Error Latch Time 6-18

6-5-6 EDM Feedback 6-19

6-5-7 Output Delay 6-19

6-6 Logic Function 6-20

6-6-1 Logical Processing 6-20

6-7 Safety Applications 6-23

6-7-1 Purpose of Safety Applications 6-23

6-7-2 Types of Safety Applications 6-23

6-7-3 Fixed Application Details 6-27

6-8 Operating Modes 6-47

6-8-1 Operating Mode Types 6-47

6-8-2 Functions Executable in Each Operating Mode 6-48

6-8-3 Web UI Functions Executable in Each Operating Mode 6-50

6-8-4 Operating Mode Changing and Power-on Mode 6-51

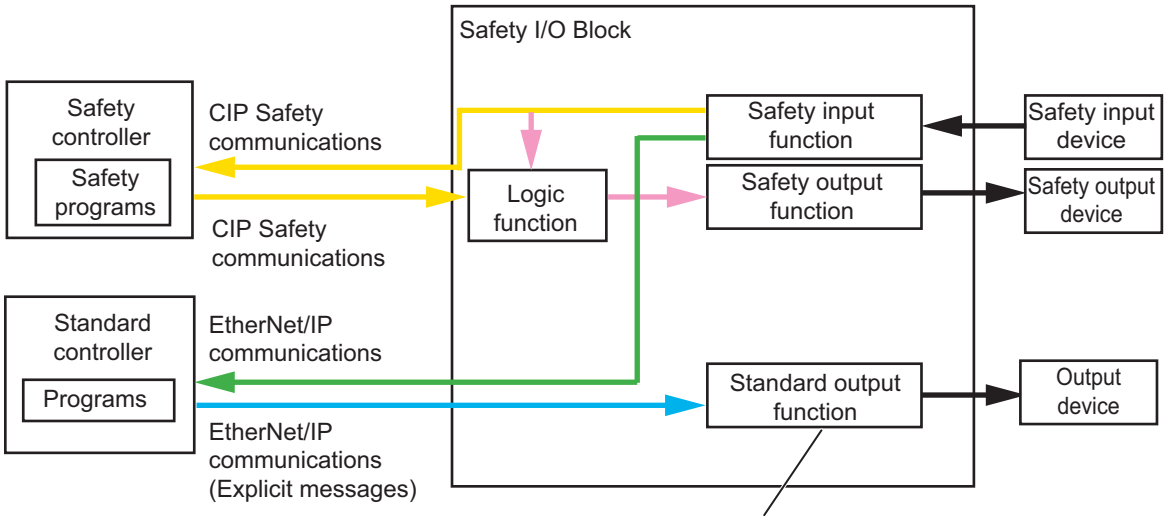
6-1 Overview of Operations

The main operations of the Safety I/O Block are performed using combinations of following functions.

Function	Description
CIP Safety communications	Communications performed between a safety controller (CIP Safety originator) and Safety I/O Block (CIP Safety target)
EtherNet/IP communications	Communications performed between a standard controller (EtherNet/IP originator) and Safety I/O Block (EtherNet/IP target)
Safety input function	The Safety I/O Block obtains safety input data from a safety input device.
Safety output function	The Safety I/O Block outputs safety output data to a safety output device.
Logic function	Process that is executed for safety input data inside the Safety I/O Block. The process result is passed to the safety output function as safety output data.

The following shows the relationship between these functions and the peripheral devices of the Safety I/O Block.

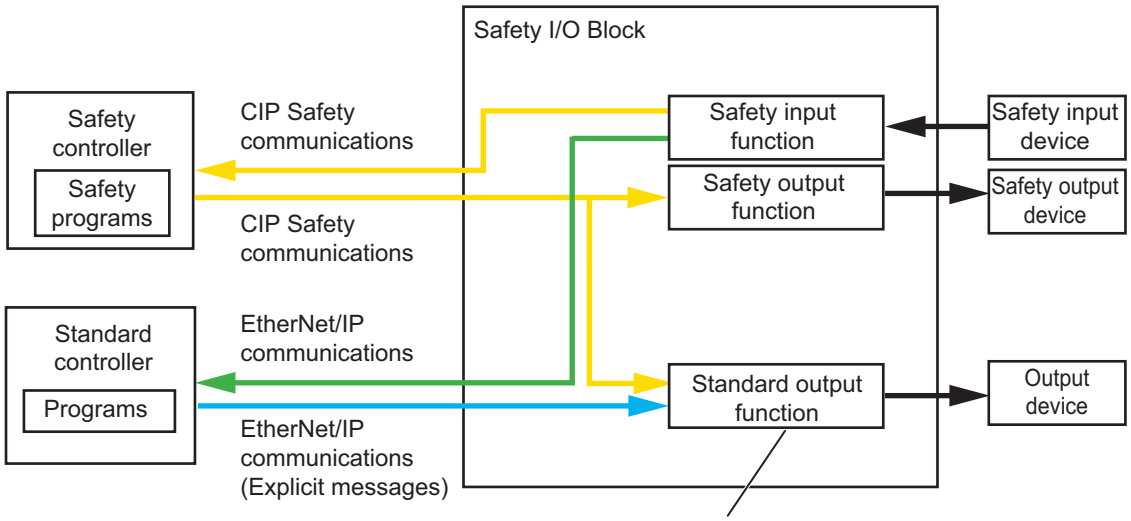
- The logic function inside the Safety I/O Block processes the safety input data obtained from the safety input function according to the logic settings, and then passes that result to the safety output function.
- In addition, the safety output data that is transmitted from the safety controller can also be combined with the logic function.
- Furthermore, the safety input data obtained from the safety input function is processed by a standard controller, and that result can also be passed to the standard output function.



If the test output mode for the test output terminals of the Safety I/O Block is set to “Standard Output,” the test output terminals can be used as standard outputs.

When the logic function is not used, operation is as shown in the figure below.

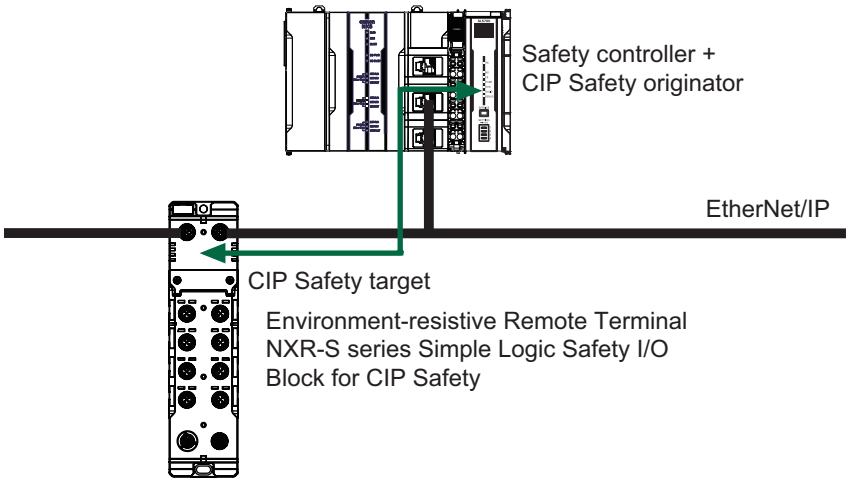
- The safety controller processes the data obtained from the safety input function, and then passes that result to the safety output function.
- In addition, the safety output data transmitted from the safety controller can also be passed to the standard output function.
- Furthermore, the safety input data obtained from the safety input function is processed by a standard controller, and that result can also be passed to the standard output function.



If the test output mode for the test output terminals of the Safety I/O Block is set to “Standard Output,” the test output terminals can be used as standard outputs.

6-2 CIP Safety Communications

CIP Safety communications use CIP Safety on EtherNet/IP communications between CIP Safety devices on an EtherNet/IP network.
The node that requests establishing a CIP Safety connection is called the CIP Safety originator, and the node that receives the request is called the CIP Safety target. The Safety I/O Block supports only the CIP Safety target function.



When a CIP Safety connection is established, safety I/O data is exchanged cyclically between the CIP Safety originator and CIP Safety target.
This enables sending the safety input status of the Safety I/O Block to a higher level safety controller, and receiving the safety output data from the safety controller.

CIP Safety Connection Setting Parameters

A CIP Safety connection has the following setting parameters.

● Open Types

The open types are settings to indicate the open request method of the CIP Safety connection.
This **open type** can be specified when a CIP Safety originator requests the Safety I/O Block to open a CIP Safety connection.
The following open types are available.

Open type	Description
Configure Target Device (Type 1)	Configure the Safety I/O Block when establishing a connection.
Check Safety Signature (Type 2a)	Use a safety signature to check that the Safety I/O Block is configured properly when establishing a connection. The safety signature consists of the Safety Configuration CRC and the Safety Configuration Time Stamp.
Open Only (Type 2b)	A configuration check of the Safety I/O Block is not performed when establishing a connection.

⚠ WARNING

If you set the open type to **Open Only**, make sure to verify that the originator and target have the correct configurations before use.
Serious injury may possibly occur due to loss of required safety functions.

Connection Type

You can select a multi-cast connection or single cast (point-to-point) connection as the connection type in the CIP Safety connection settings.
With a multi-cast connection, you can send one input assembly in one packet to multiple originator devices. In contrast, with a single-cast connection, you can send one input assembly to each originator device individually.
Therefore, when sending one input assembly to multiple originator devices, you can decrease the communications load by using a multi-cast connection.
Note that the case of using a multi-cast connection to send one input assembly in one packet to multiple originator devices is permitted only if the connection type of each connection that receives it is a multi-cast connection, and the connection I/O type, expected packet interval (EPI), and timeout value are all identical.

Precautions for Correct Use

If multi-cast connections are used, however, use an Ethernet switch that has multicast filtering, unless packets are received by all nodes in the network.
If an Ethernet switch without multicast filtering is used, multicast 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.

Expected Packet Interval (EPI)

The expected packet interval (EPI) is the I/O data refresh interval on the Ethernet line in CIP Safety communications. With EtherNet/IP, data is exchanged on the communications line at the EPI that is set for each connection, regardless of the number of nodes.
With the built-in EtherNet/IP port, you can set EPI for each connection.

Precautions for Correct Use

The performance of communications devices is limited to some extent by the limitations of each product's specifications. Consequently, the expected packet interval (EPI) cannot be set to unlimited.
Refer to *NX-series Safety Control Unit/Communication Control Unit User's Manual (Cat. No. Z395)* for details, and then set an appropriate expected packet interval (EPI).

I/O Assembly

An I/O assembly is a unit of I/O data cyclically exchanged between an originator and target.
Several I/O assemblies are defined and provided for the Safety I/O Block. Select from the defined I/O assemblies to set one I/O assembly per connection.
The I/O assemblies settable between the Safety I/O Block and CIP Safety originator are as follows.

- Input connection: 25C hex (2 bytes), 3C0 hex (5 bytes), 3C1 hex (9 bytes)
- Output connection: 233 hex (1 byte), 371 hex (3 bytes), 372 hex (1 byte), 373 hex (1 byte), 380 hex (3 bytes)

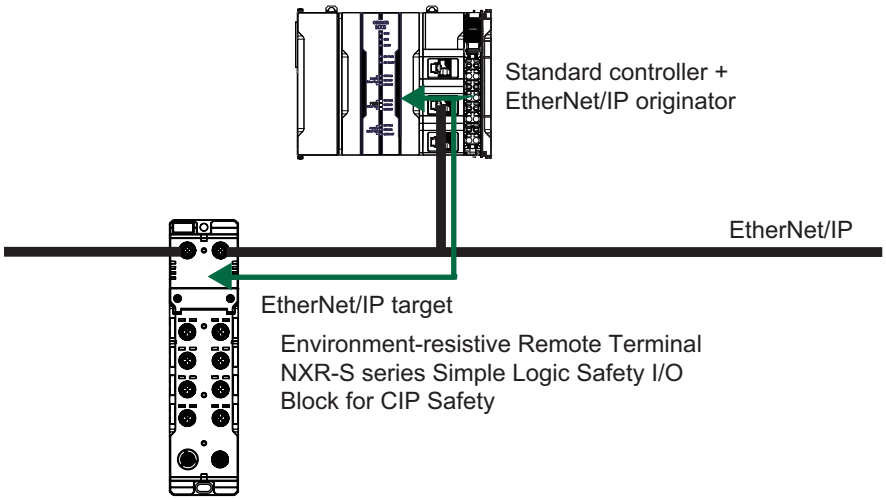
Refer to *A-2 Safety I/O Assembly Data* on page A-4 for details on I/O assembly data.

6-3 EtherNet/IP Communications

EtherNet/IP communications are for exchanging data between devices on an EtherNet/IP network. Tag data link communications and explicit message communications are available as communications methods.

6-3-1 Tag Data Link Communications

Tag data link communications are communications to exchange I/O data cyclically between devices on an EtherNet/IP network.
With a tag data link communications, one node requests the connection (opening) of a communications line to exchange I/O data with another node.
The node that requests establishing a tag data link communications connection is called the EtherNet/IP originator, and the node that receives the request is called the EtherNet/IP target. The Safety I/O Block supports only the EtherNet/IP target function.



The unit subject to I/O data exchange is called a tag, and the data is exchanged cyclically between the originator and target.
Several I/O assemblies are defined and provided for the Safety I/O Block.
Refer to *Setting Procedure for Tag Data Link Communications* on page 7-38 for how to set tag data link communications, including the I/O assembly data settings.

6-3-2 Explicit Message Communications

Explicit message communications are CIP communications to exchange settings and statuses of equipment in request/response format on an EtherNet/IP network.
Communications are performed by an explicit message server sending responses to requests from an explicit message client.
The Safety I/O Block supports only the explicit message server function.

Explicit Message Server Function

Accessing CIP objects of the Safety I/O Block in explicit messages from an explicit message client using the explicit message server function enables the following operations.

- Troubleshooting the Safety I/O Block by reading event logs, clearing event logs, etc.
- Configuring the device parameter settings, and the IP address and other communications parameters for the Safety I/O Block

Furthermore, if a device with the explicit message client function does not support tag data link (i.e., implicit message) communications, you can use explicit messages as an alternative means to control the I/O of the Safety I/O Block.

Refer to *A-4 Supported CIP Objects* on page A-16 for details on CIP objects that are supported by the Safety I/O Block.

Refer to the manual of the Controller used for the method to access CIP objects of the Safety I/O Block through an explicit message.

6-4 Safety Input Functions

This section describes the safety input functions in the Safety I/O Block.

6-4-1 Connectable Devices

The Safety I/O Block diagnoses the connected external devices through the safety input terminals.
The safety input devices and standard input devices that can be connected to the safety input terminals are listed in the following table.

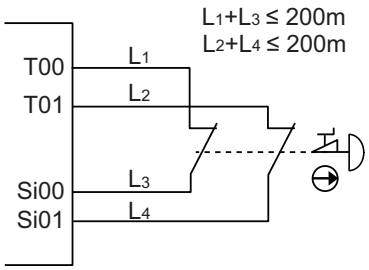
Input device type	Channel mode			Test output terminal
	Dual channel (equivalent input)	Dual channel (complementary input)	Single channel	Test Output Mode
Safety input devices (Devices with mechanical contacts)	• Emergency stop switch (2NC contact) • Safety door switch (2NC contact) • Safety limit switch (2NC contact) • Safety key selector switch (2NC contact) • Enable switch (2NC contact) • Mechanical contact for dual-channel equivalent input (2NC contact)	• Safety door switch (1NC/1NO contact) • Safety limit switch (1NC/1NO contact) • Two-hand switches (1NO/1NC contact) • Safety key selector switch (1NC/1NO contact) • Mechanical contact for dual-channel complementary input (1NC/1NO contact)	• Emergency stop switch (1NC contact) • Safety door switch (1NC contact) • Safety limit switch (1NC contact) • Safety key selector switch (1NC contact) • EDM Feedback (1NC contact) • Mechanical contact for single channel (1NC contact)	Test Output
Safety input devices (Devices with semiconductor outputs)	• Safety light curtain • Safety laser scanner • High-coded door switch • High-coded door switch (for gate) • High-coded door switch (guard lock model) • Semiconductor output for dual-channel equivalent input	• Semiconductor output for dual-channel complementary input	• Semiconductor output for single channel	• Power Supply Output • Standard Output • Not Used
Standard input devices	Not applicable	Not applicable	• Reset switch with test pulse (1NO contact)	Test Output
	Not applicable	Not applicable	• Reset switch without test pulse (1NO contact)	Power Supply Output

The safety input devices can be broadly classified into two types.
One is devices with mechanical contacts, and the other is devices with semiconductor outputs.

Devices with Mechanical Contacts

Connect a device with a contact output, such as an emergency stop switch or safety limit switch, to a safety input.
Use a safety input (Si) and test output (T) in combination.

The following shows the case of use with dual channel input as a connection example.



Only the same number can be used for the combination of a safety input and test output. The above example shows the combinations of "Si00" and "T00", and "Si01" and "T01".
In this case, the Test Output Mode setting of "T00" and "T01" becomes **Test Output**.

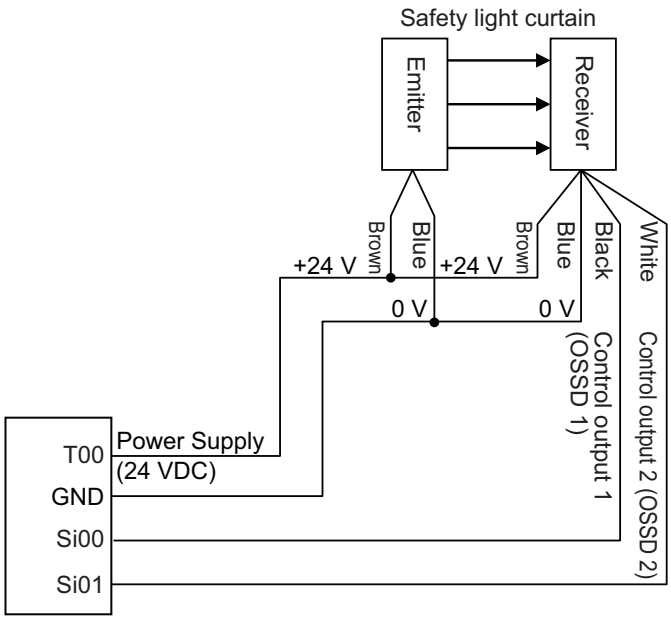
Precautions for Correct Use

The total length of cable connected to one test output must be 200 m or less.

Devices with Semiconductor Outputs

Connect a device with a semiconductor output, such as a light curtain, to a safety input terminal (Si).

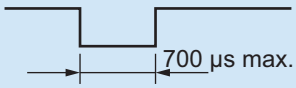
The following shows the case of use with dual channel input as a connection example.



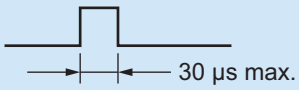
Connect the outputs of the light curtain to "Si00" and "Si01" of the safety inputs, and use the "T00" test output as the power supply to the light curtain.
In this case, the Test Output Mode setting of "T00" becomes **Power Supply Output**.

Precautions for Correct Use

- The power to the light curtains is supplied from the test output terminal. The output current that can be supplied from the test output is a 0.7 A/point max.
- Some types of devices with semiconductor outputs, such as safety light curtains, output a pulse to detect wiring errors. Observe the following when connecting a device with a semiconductor output to a safety input terminal.
  a) The OFF pulse width when the semiconductor output is ON must be 700 µs max.



  b) The ON pulse width when the semiconductor output is OFF must be 30 µs max.



6-4-2 Test Output Function

The test output terminals operate as safety input auxiliaries, such as a test output during test pulse evaluation (device with mechanical contacts) and a power supply to a device with semiconductor outputs.
The test output function (function of test output terminals) is as follows.

With/without test pulse	Test Output Mode	Description
With test pulse (Devices with mechanical contacts)	**Test Output**	Outputs 24 VDC that has a test pulse with a specific period from a test output terminal. Refer to *6-4-3 Test Pulse Evaluation Function* on page 6-10 for details on the test pulse evaluation.
Without test pulse (Devices with mechanical contacts)	**Power Supply Output**	Outputs 24 VDC from a test output terminal.
Without test pulse (Devices with semiconductor outputs)	**Power Supply Output**	Outputs 24 VDC from a test output terminal. Use it as a power supply to a device with semiconductor outputs.
	Standard Output	Standard output from the Controller is possible by using a test output terminal. *1 Use it as a non-safety digital signal output terminal. For example, you can use it for monitor output by connecting it to the input of an indicator light or PLC. Refer to *7-5-2 Setting Procedure for Standard Output Functions* on page 7-47 for the setting procedure.

***1.** The standard output function from the Controller is not a safety function.

The test output terminal also has a function to detect overcurrent. If an overcurrent is detected, it will be recorded in the event log. Refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details.

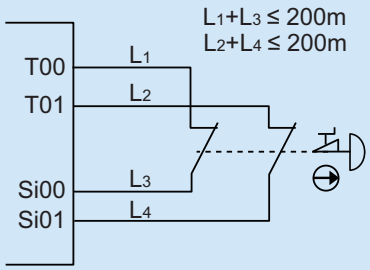
6-4-3 Test Pulse Evaluation Function

When there is a test pulse (device with mechanical contacts), 24 VDC that has a test pulse with a specific period can be output from a test output terminal to detect wiring errors and failures of the externally connected device.

With/without test pulse	Test Output Mode	Description
With test pulse (Devices with mechanical contacts)	**Test Output**	The test output signal (test pulse) is input to the safety input terminal through mechanical contacts. Contact of the input signal line with the power line (positive side) and short-circuiting with another input signal line can be detected.

Precautions for Correct Use

Only the same number can be used for the combination of a safety input terminal and test output terminal.
The following example shows the combinations of "Si00" and "T00", and "Si01" and "T01".



6-4-4 Dual Channel Evaluation

Safety input terminals can be used as dual channels (to create redundancy). Dual channel evaluation evaluates the discrepancy time of data between two inputs.
The discrepancy time is the time from one input value changing to the other one changing.
An error is determined to have occurred if there is no change to the other input despite exceeding the time set in **Discrepancy Time**.

Setting the Dual Channel Evaluation Function

Select the devices of dual channel mode for the input devices and set **Discrepancy time**.

The following table shows the settings.

Setting data name	Description	Setting range
Channel mode	Select the devices of dual channel mode for the input devices.	Select from the following. • Dual-channel equivalent input • Dual-channel complementary input Refer to *6-4-1 Connectable Devices* on page 6-8 for details on the channel modes and devices.
Discrepancy time	The discrepancy time *1 of data between two inputs is monitored. If the discrepancy exceeds this value, an error occurs.	Set a value from 10 to 64,000 (ms). Set this in 5 (ms) increments. Factory default is 500 (ms).

***1.** The discrepancy time is the time from one input value changing to the other one changing.

Refer to *7-5-1 Setting Procedure for Safety Input Functions* on page 7-44 for the setting procedure.

Relationship Between the Input Signals of the Safety Input Terminals and the Safety Input Data

The relationship between the safety input signals and safety input data is as follows.

Channel mode	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 input	0	0	0	0*1	Inactive (OFF)
	0	1	0	0*1	Data discrepancy between two inputs
	1	0	0	0*1	Data discrepancy between two inputs
	1	1	1	0*1	Active (ON)
Dual-channel complementary input	0	0	0	0*1	Data discrepancy between two inputs
	0	1	0	0*1	Inactive (OFF)
	1	0	1	0*1	Active (ON)
	1	1	0	0*1	Data discrepancy between two inputs

***1.** If the terminals are set to Dual Channel Mode, the safety input data of the even-numbered terminals is used by the safety program in the safety controller.

6-4-5 Errors Detectable by the Diagnosis Function of Safety Input Terminals

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.

Parameter settings		Error detection			
Channel mode	Test pulse	Connection to power line (positive side)	Ground fault*1	Disconnection	Short circuits in input wiring
Single channel	Without test pulse (Devices with semiconductor outputs)	Not detectable	Not detectable	Not detectable	−
	With test pulse (Devices with mechanical contacts)	Detectable	Detectable when input turns ON	Not detectable	−
Dual-channel (equivalent input)	Without test pulse (Devices with semiconductor outputs)	Not detectable*2	Detectable when input turns ON	Not detectable*3	Not detectable*2
	With test pulse (Devices with mechanical contacts)	Detectable	Detectable when input turns ON	Not detectable*3	Detectable

Parameter settings		Error detection			
Channel mode	Test pulse	Connection to power line (positive side)	Ground fault*1	Disconnection	Short circuits in input wiring
Dual-channel (complementary input)	Without test pulse (Devices with semiconductor outputs)	Detectable when switching from ON to OFF or from OFF to ON	Detectable when switching from ON to OFF or from OFF to ON	Detectable when switching from ON to OFF or from OFF to ON	Detectable
	With test pulse (Devices with mechanical contacts)	Detectable	Detectable when switching from ON to OFF or from OFF to ON	Detectable when switching from ON to OFF or from OFF to ON	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.
***3.** Detection is possible only if one of the signal lines is broken when the input turns ON.

6-4-6 Input Filter Function

The input filter function prevents malfunctions caused by chattering or noise from an external device that is connected to a safety input terminal.
Set **ON->OFF Delay time** or **OFF->ON Delay time** to filter out chattering or noise from the external device.

The following table shows the settings.

Setting data name	Description	Setting range
ON->OFF Delay time	This is the delay time for the input data to turn from ON to OFF.	Set a value from 0 to 1,600 (ms). Set this in 5 (ms) increments. Factory default is 0 (ms).
OFF->ON Delay time	This is the delay time for the input data to turn from OFF to ON.	Set a value from 0 to 1,600 (ms). Set this in 5 (ms) increments. Factory default is 0 (ms).

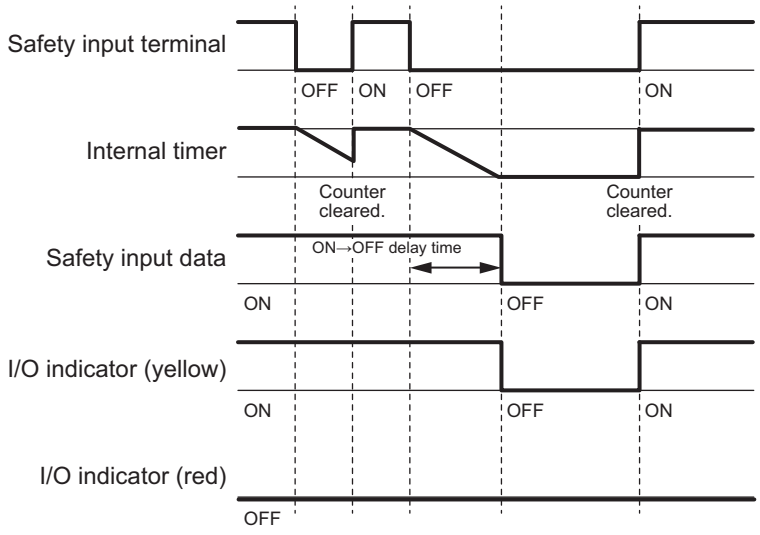
Refer to *7-5-1 Setting Procedure for Safety Input Functions* on page 7-44 for the setting procedure.

Precautions for Correct Use

Setting a longer delay time increases the resistance to chattering and noise, but the response to input signals becomes slower.

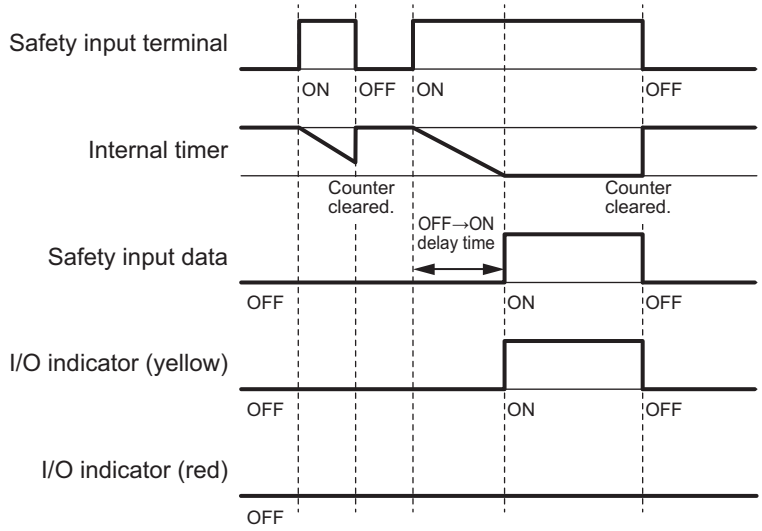
Operation with OFF Delay Time Set

You can filter out OFF pulses that are shorter than the time set in **ON->OFF Delay time**.



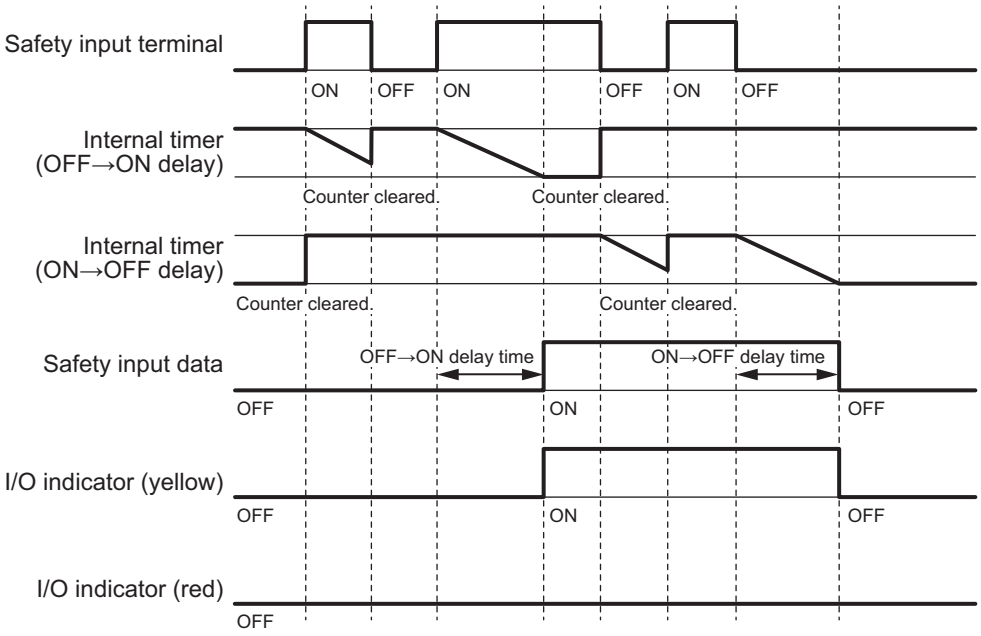
Operation with ON Delay Time Set

You can filter out ON pulses that are shorter than the time set in **OFF->ON Delay time**.



Operation with Both ON Delay Time and OFF Delay Time Set

You can filter out ON pulses that are shorter than the time set with the **OFF->ON Delay time** and filter out OFF pulses that are shorter than the time set with the **ON->OFF Delay time**.



6-4-7 Input Error Latch Time

The input error latch time is a parameter that is applied to all input terminals.
Set the time to latch the error state when an error occurs in an input terminal.
Set the minimum latch time so that the Safety I/O Block can detect an error that occurs intermittently.
For the error latch time, set the optimal value with which an error can be detected, taking into account the network response time between the Safety I/O Block and originator device.

The following table shows the settings.

Setting data name	Description	Setting range
Input error latch time	Set the minimum time from error occurrence to reset.*1	Set a value from 0 to 65530 (ms). Set this in 10 (ms) increments. In the case of 0 (ms), there is no error latch. Factory default is 1000 (ms).

***1.** When the cause of the error is removed and the corresponding safety input is made inactive (OFF), the error is reset.

6-5 Safety Output Functions

This section describes the safety output functions in the Safety I/O Block.

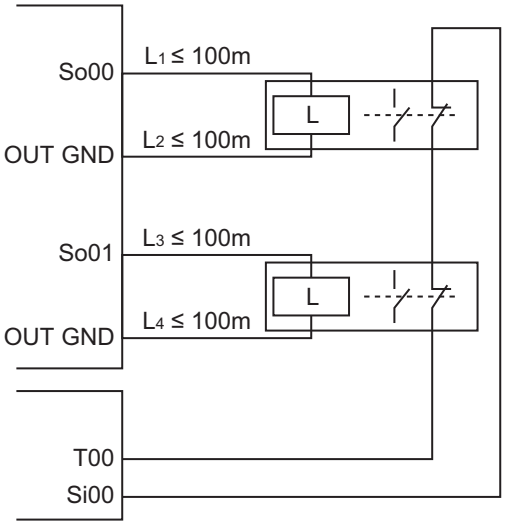
6-5-1 Connectable Devices

The Safety I/O Block diagnoses the connected external devices through the safety output terminals.
The safety output devices that can be connected to the safety output terminals are listed in following table.

Channel mode		Setting of output terminal
Dual channel	**Single channel**	**Test pulse**
• Safety relay (dual channel) • Dual-channel equivalent output (with test pulse)	• Safety relay (single channel) • Single channel (with test pulse)	With test pulse
• Dual-channel equivalent output (without test pulse)	• Single channel (without test pulse)	Without test pulse

Connect a safety relay, contactor, solenoid valve, or other device to the safety output device.
The output is PNP output.

The following shows the case of use with a safety relay or contactor as a connection example.



Precautions for Correct Use

The line length from the safety output terminals to the safety output devices (L1, L2, L3, and L4) is 100 m max. per line.

6-5-2 Test Pulse Evaluation Function

This function outputs a test pulse at a specific interval from a safety output terminal to detect errors in wiring of the output terminal.
The following table shows the settings.

Setting data name	Description	Setting range
Test pulse	Select a device with a test pulse for the safety output device.	Select from the following. • Safety relay (dual channel) • Dual-channel equivalent output (with test pulse) • Safety relay (single channel) • Single channel (with test pulse)

Precautions for Correct Use

When the test pulse evaluation function is used, OFF pulse signals with a pulse width of 500 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.

Additional Information

A safety relay is a device **with test pulse** for both dual channel and single channel.

6-5-3 Dual Channel Evaluation

Safety output terminals can be used as dual channels (to create redundancy). Dual channel evaluation evaluates the signals between two outputs to check for discrepancies.
If an error is detected in either of the two output terminals, both outputs are turned OFF.

Setting the Dual Channel Evaluation Function

Set the dual channel evaluation function by selecting the devices of dual channel mode for the output devices.

The following table shows the settings.

Setting data name	Description	Setting range
Channel mode	Select the devices of dual channel mode for the output devices.	Select from the following. • Safety relay (dual channel) • Dual-channel equivalent output (with test pulse) • Dual-channel equivalent output (without test pulse) Refer to *6-5-1 Connectable Devices* on page 6-16 for details on the channel modes and devices.

Refer to *7-6-1 Safety Output Function Setting Procedure* on page 7-50 for the setting procedure.

Relationship Between Safety Output Data and Signals Output from Safety Output Terminals

For a device in dual channel mode, the relationship between safety output data and safety output signals is as follows.

Channel mode	Safety output data		Output signal on the safety output terminal		Meaning of status
	So (n)	So (n+1)	So (n)	So (n+1)	
• Safety relay (dual channel) • Dual-channel equivalent output (with test pulse) • Dual-channel equivalent output (without test pulse)	0	0	0 (OFF)	0 (OFF)	Inactive (OFF)
	0	1	0 (OFF)	0 (OFF)	Inactive (OFF)*1
	1	0	0 (OFF)	0 (OFF)	Inactive (OFF)*1
	1	1	1 (ON)	1 (ON)	Active (ON)

***1.** This becomes inactive due to a data error occurring between dual channel outputs.

6-5-4 Errors Detectable by the Diagnosis Function of Safety Output Terminals

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.

Parameter settings		Error detection						
		Connection to power line (positive side)		Ground fault*1		Short circuits in output wiring*2		
Setting of output terminal	Description	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.
***2.** The detection of short circuits in output wiring is enabled only in dual channel mode.

6-5-5 Output Error Latch Time

The output error latch time is a parameter that is applied to all output terminals.
Set the time to latch the error state when an error occurs with an output terminal.
Set the minimum latch time so that the Safety I/O Block can detect an error that occurs intermittently.
For the error latch time, set the optimal value with which an error can be detected, taking into account the network response time between the Safety I/O Block and originator device.

The following table shows the settings.

Setting data name	Description	Setting range
Output error latch time	Set the minimum time from error occurrence to reset.*1	Set a value from 0 to 65530 (ms). Set this in 10 (ms) increments. In the case of 0 (ms), there is no error latch. The factory default setting is 1000 (ms).

***1.** When the cause of the error is removed and the corresponding safety output is made inactive (OFF), the error is reset.

6-5-6 EDM Feedback

If a safety application is a user-defined application, the EDM feedback setting is displayed.

The following table shows the settings.

Setting data name	Description	Setting range
EDM feedback	Select from the terminals with **EDM feedback** registered on the safety input device.	Select from the following. • 0: Unused • 1: Si00 to 12: Si11 The factory default setting is 0 (Unused).

6-5-7 Output Delay

If a safety application is a user-defined application, a delay time can be set for output to an external device connected to a safety output terminal. This function is used for applications such as preventing machine damage due to a sudden stop by delaying output considering the time until a motor, robot arm, or other external device completely stops, and turning the safety output ON after operation has stabilized once the external device has recovered.

The following table shows the settings.

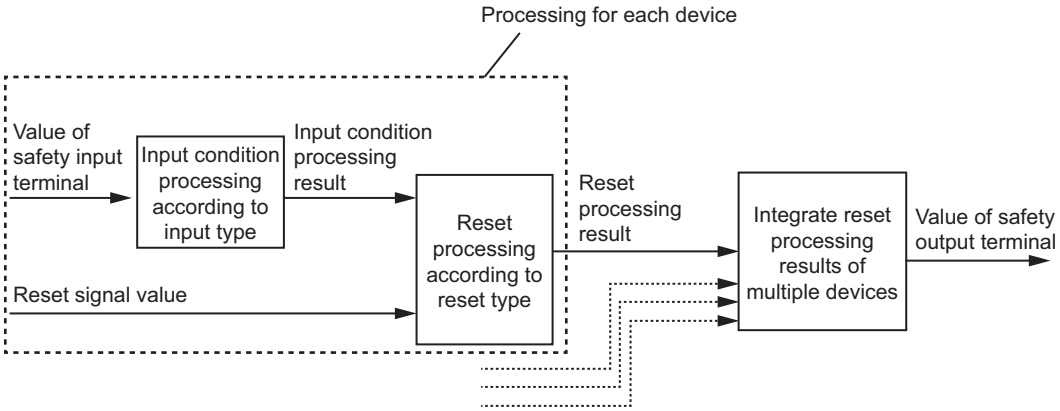
Setting data name	Description	Setting range
ON->OFF Delay time	This is the delay time for the output data to turn from ON to OFF. It is used to prevent machine damage due to a sudden stop by delaying output considering the time until a motor, robot arm, or other external device completely stops.	The output is delayed by the value of the set value × 100 (ms). Set a value from 0 to 1500. Factory default is 0 (ms).
OFF->ON Delay time	This is the delay time for the output data to turn from OFF to ON. It is used to turn safety output ON after operation has stabilized once the external device has recovered.	

6-6 Logic Function

The logic function is a process that is execute for safety input data inside the Safety I/O Block. The process result is passed to the safety output as safety output data.
This section describes the mechanism of the logic process.

6-6-1 Logical Processing

In the logic settings, you need to set three types of parameters: *Input type*, *Reset type*, and *Output values to safety output terminals So00 to So03*.
Logical processing involves first executing the input condition processing according to *Input type* and reset processing according to *Reset type* for the values of the safety input terminals SiXX for each device. Then executing integration of the reset processing results of multiple devices, and finally determining the values of safety output terminals SoXX. You need to keep the details of these processes in mind while configuring the logic settings.



Input Condition Processing According to Input Type

With input condition processing, you can integrate the input values from two types of device according to the setting of *Input type* to obtain the input condition processing result. This enables processing such as stopping a device only when both of two pairs of safety light curtains are interrupted.
There are three setting options for the *Input type* setting: **2 Input (OR)**, **2 Input (AND)**, and unset. The relationship between each setting and input condition processing result is shown below.

Input type	Input condition processing result
2 Input (OR)	OR processing result of input values from two types of device
2 Input (AND)	AND processing result of input values from two types of device
Unset	Input values from two types of device are not integrated. The input value of one type of device becomes the input condition processing result as-is.

Reset Processing According to Reset Type

Once the output value for each device becomes FALSE, it will not be returned to TRUE until a reset is performed. *Reset types* are methods to reset the output value for each device, and there are two types: **Manual (SiXX)** and **Auto**. The relationship between each setting and reset condition is shown below.

Reset type	Reset condition
Manual (SiXX)	The value of safety input terminal SiXX is used as the reset signal. When a reset is executed, the output value of the corresponding device is reset.
Auto	A reset signal is not used. The output value is reset at the point in time when the input condition processing result of the corresponding device becomes TRUE.

Reset signal in the table is the pulse signal of Low-High-Low for resetting the output of the corresponding device. The reset signal can be registered automatically and the setting can be changed after registration. Refer to *7-7-1 Logic Setting Procedure* on page 7-53 for each of the procedures.

Reset processing is executed for each device based on the input condition processing result and whether the reset condition is met. The relationship between the input condition processing result, whether the reset condition is met or not met, and the reset processing result is shown below.

Input condition processing result	Reset condition	Reset condition processing result
TRUE	Condition is met	TRUE
	Condition is not met	Keep the present value.
FALSE	Condition is met	FALSE
	Condition is not met	FALSE

Precautions for Correct Use

When using the reset type set to Auto, ensure that unexpected starts or dangerous machine movements do not occur as a result of a restart or reset, posing no risk of injury to personnel. If you cannot confirm this, do not use the reset type Auto.

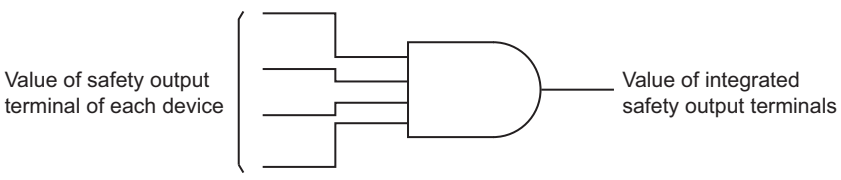
Setting the Values Output to Safety Output Terminals So00 to So03

The settings of *Output values to safety output terminals So00 to So03* assign the reset processing result of each of the devices to an safety output terminal. Assign setting value **0** or **1** for each device to an safety output terminal from So00 to So03. The meaning of each setting value is as follows.

Setting value	Meaning
0	The reset processing result is reflected for the corresponding safety output terminal.
1	The reset processing result is not reflected for the corresponding safety output terminal.

Integrating Output Processing Results of Multiple Devices

When multiple devices are connected, the values of the safety output terminals become an integrated value by performing the AND operation on the value of the safety output terminal of each device. In other words, if even one of the multiple devices has a safety output terminal value of FALSE, the safety output terminal value becomes FALSE.



Setting Example

The following table shows setting examples of the logic settings.

Input	Device	Input type	Reset type	So00	So02
Si00	Emergency stop switch (dual-channel equivalent input)	-	Manual (Si10)	0	0
Si02	Safety light curtain	2 Input (OR)	Manual (Si11)	1	0
Si04	Safety light curtain				
Si06	Safety door switch (dual-channel equivalent input)	-	Auto	0	1
Ro1-01	Remote Output 1-01	2 Input (OR)	Manual (Si10)	0	0
Ro2-01	Remote Output 2-01				

With these settings, the value of So00 becomes FALSE if even one of the following conditions occurs.

- An emergency stop switch is pressed.
- A door with a safety door switch installed is opened.
- The values of Remote Output 1-01 and Remote Output 2-01 both become FALSE.

Furthermore, the value of So02 becomes FALSE if even one of the following conditions occurs.

- An emergency stop switch is pressed.
- Both of the two pairs of safety light curtains are interrupted.
- The values of Remote Output 1-01 and Remote Output 2-01 both become FALSE.

If the following conditions are met when the value of So00 or So02 has become FALSE, a reset is performed and the value is returned to TRUE.

Reason why the value of So00 or So02 became FALSE	Condition to reset the value of So00 or So02
An emergency stop switch is pressed.	The reset condition of Si10 is met.
Both of the two pairs of safety light curtains are interrupted.	The reset condition of Si11 is met.
A door with a safety door switch installed is opened.	A door with a safety door switch installed is closed.
The values of Remote Output 1-01 and Remote Output 2-01 both became FALSE.	The reset condition of Si10 is met.

6-7 Safety Applications

This section describes the purposes and types of safety applications, and details on the fixed applications preset in the Safety I/O Block.

6-7-1 Purpose of Safety Applications

If you use the logic functions of safety applications, you can achieve high-speed responses by performing control locally without going through the safety controller.
In addition, safety applications allow control to be enhanced flexibility by combining safety output data transmitted from the safety controller with internal logic as needed.

6-7-2 Types of Safety Applications

There are four types of safety applications: remote I/O mode applications, fixed applications, user-defined applications, and add-on applications.
An overview, application details, selection criteria, and corresponding safety control system are given below for each of them.

Safety application	Description	Selection criteria	Safety control system
Remote I/O mode application	A safety application with only I/O terminal settings that does not use the logic function. The safety controller performs control because the logic function is not used.	• Wish to build a complicated, large-scale system that is difficult to implement with the logic function of the Safety I/O Block.	*Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)* on page 1-8 *Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI)* on page 1-9
Fixed application	A safety application with a logic function and I/O configuration settings. It comes preset in the Safety I/O Block, and the specifications cannot be customized. The Safety I/O Block performs control.	• There are applications that can be used as-is among the fixed applications.	*Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application* on page 1-10

Safety application	Description	Selection criteria	Safety control system
User-defined application	A safety application with a logic function and I/O configuration settings. The user can customize each of the settings. The Safety I/O Block performs control.	• This is an application that can be implemented with the logic function of the Safety I/O Block for simple processing. • There are no applications that can be used as-is among the fixed applications. • Wish to manage a safety application on the safety controller side to perform the same processing on multiple Safety I/O Block units.	*Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 1-11
Add-on application		• This is an application that can be implemented with the logic function of the Safety I/O Block for simple processing. • There are no applications that can be used as-is among the fixed applications. • Wish to manage a safety application on the Safety I/O Block side to use a single Safety I/O Block alone.	*Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 1-12

Remote I/O Mode Application

A remote I/O mode application is an application for a user to define only the I/O configuration settings using Sysmac Studio. The logic settings are not configured. It is used in combination with the safety program of a safety controller. This application is suitable for building a complicated, large-scale system that is difficult to implement with the logic functions of the Safety I/O Block.

There are the following two ways to configure a remote I/O mode application for the Safety I/O Block.

- Method using Type 1 Safety Open from the safety controller
- Method using configuration via the Web UI

Fixed Applications

Fixed applications are safety applications that come pre-installed in the Safety I/O Block. The specifications cannot be customized.

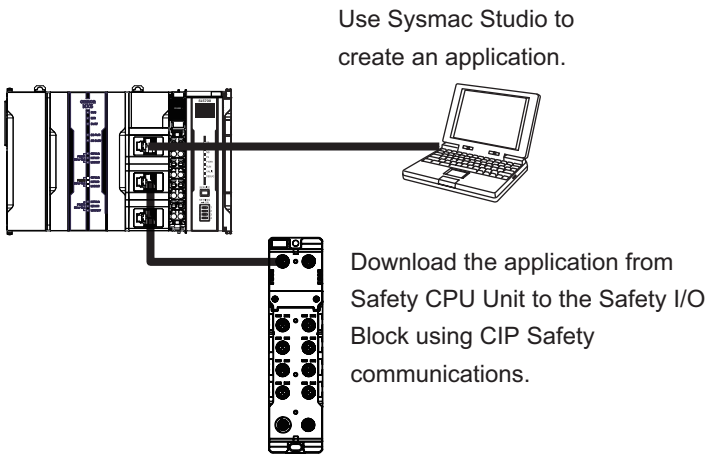
There are the following three types of fixed application. They are all applications that use a device such as an emergency stop switch or safety light curtain to stop a drive unit or robot before a hazardous situations occurs. If there is an application that matches the application you want to implement, use it. Details on each application are provided in the references listed in the table below.

Numbers of SETTING SW1 and SW2 rotary switches	Name	Application	Reference
1	Partial stop + entire stop application	This is an application to perform a partial stop using a safety light curtain and perform an entire stop using an emergency stop switch. There is no external device monitoring (EDM).	*No. 1 Partial Stop + Entire Stop Application* on page 6-27
2	Partial stop + entire stop application (with EDM)	This is an application to perform a partial stop using a safety light curtain and perform an entire stop using an emergency stop switch. There is external device monitoring (EDM).	*No. 2 Partial Stop + Entire Stop Application (With EDM)* on page 6-34
3	Worker and robot automatic switching application	This is an application to perform automatic switching of the worker and robot and perform an entire stop using an emergency stop switch and guard.	*No. 3 Worker and Robot Automatic Switching Application* on page 6-38

Fixed applications are pre-assigned to rotary switch numbers. Any fixed application can be started by setting the rotary switches.

User-defined Applications

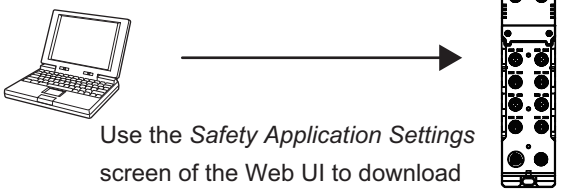
User-defined applications are applications that users can build themselves using Sysmac Studio. Download an application from the Safety CPU Unit to the Safety I/O Block using CIP Safety communications to use it.
A user-defined application is configured on the Safety I/O Block by setting the open type *Type1 Safety Open* connection using CIP Safety communications.



Add-on Applications

Add-on applications are safety applications that do not come pre-installed in the Safety I/O Block, but are instead used by downloading safety application files to the Safety I/O Block as needed.
Use Sysmac Studio to configure your own custom logic settings and I/O configuration settings, and create the safety application file.
Use the *Safety Application Settings* screen of the Web UI to download that safety application file to the Safety I/O Block.

Use Sysmac Studio to create a safety application file.



Use the *Safety Application Settings* screen of the Web UI to download that safety application file from PC to the Safety I/O Block.

6-7-3 Fixed Application Details

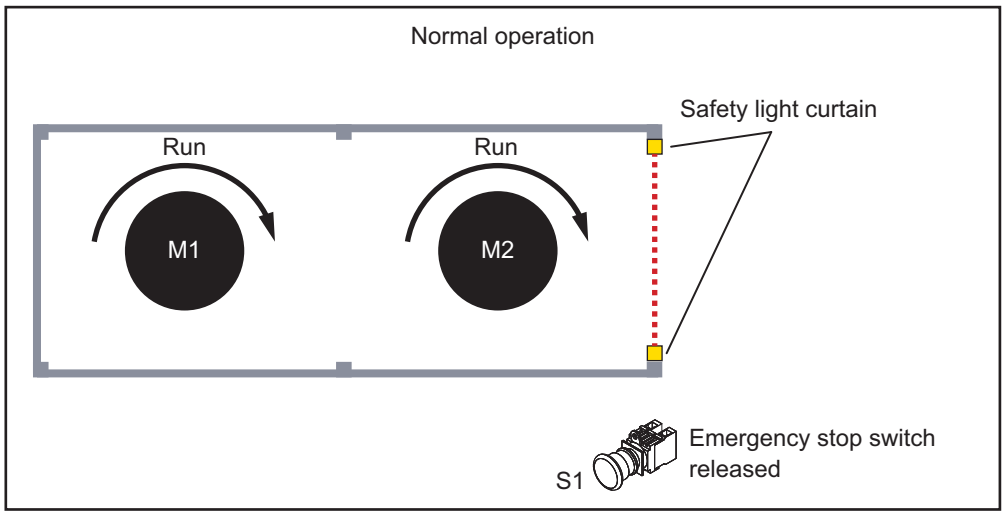
This section describes the logic and I/O configuration settings for each fixed application.

No. 1 Partial Stop + Entire Stop Application

Partial stop + entire stop application is an application to perform a partial stop using a safety light curtain and an entire stop using an emergency stop switch. External device monitoring (EDM) is not used. Use is differentiated between an entire stop of both of two drive devices and a partial stop of only one of them.

● Overview of the Application

At the production site, two drive devices, M1 and M2, are running.
The space where the drive devices are installed is surrounded by walls on three sides, but one direction is left open to allow a worker to work and has safety light curtains installed.
If the worker presses an emergency stop switch in the event of an abnormality, both drive devices stop.
If the safety light curtains are interrupted, only drive device M2 that is nearest to the safety light curtains stops, and drive device M1 continues to operate.



Safety category/PL/SIL	Specifications
Safety category	Up to Cat.3*1
PL	Up to PLe
SIL	Up to SIL3

***1.** Since the safety category of the safety servo driver that is supposed to be connected is Cat.3, the safety category of this application is also Cat.3.

Operation

The specifications for operation using an input signal from each device is as follows.

When emergency stop switch S1 is pressed

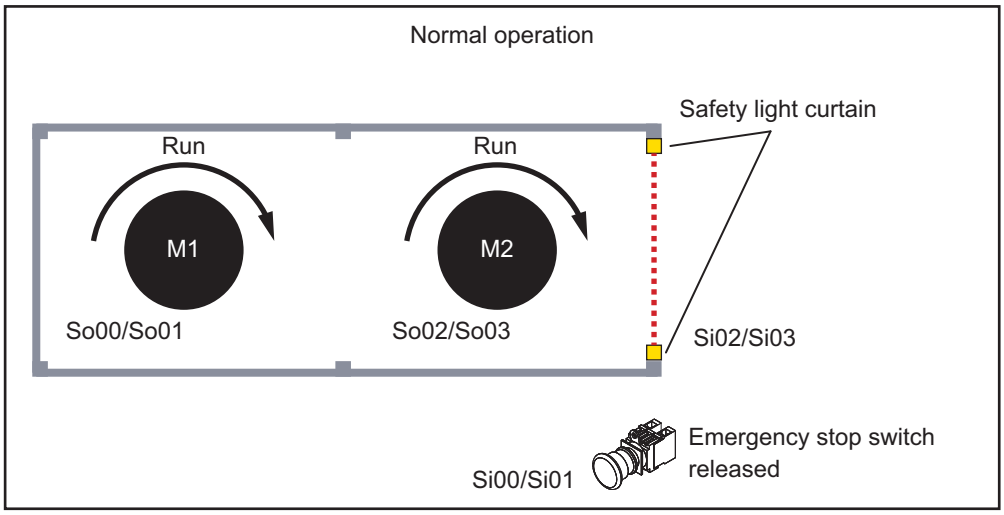
- If emergency stop switch S1 is pressed, the power supply to drive devices M1 and M2 is shut off immediately.
- The power supply to drive devices M1 and M2 is retained in the shut-off state until the emergency stop switch S1 is released and reset switch S2 is pressed.

When the safety light curtain is interrupted (emergency stop switch S1 is not pressed)

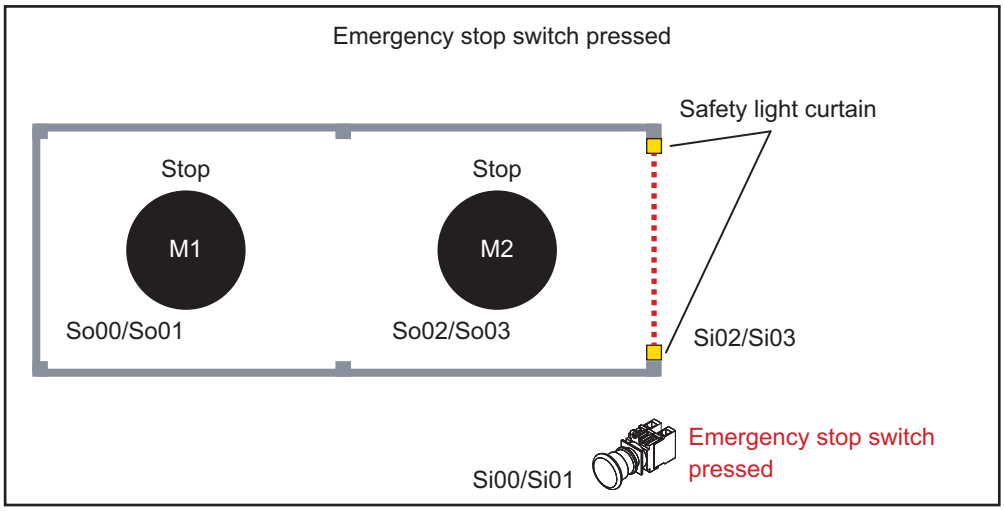
- When the safety light curtain is interrupted, the power supply to drive device M2 is shut off immediately. Power continues to be supplied to drive device M1.
- The power supply to drive device M2 is retained in the shut-off state until reset switch S2 is pressed.

The operation in each situation is illustrated in the figures.

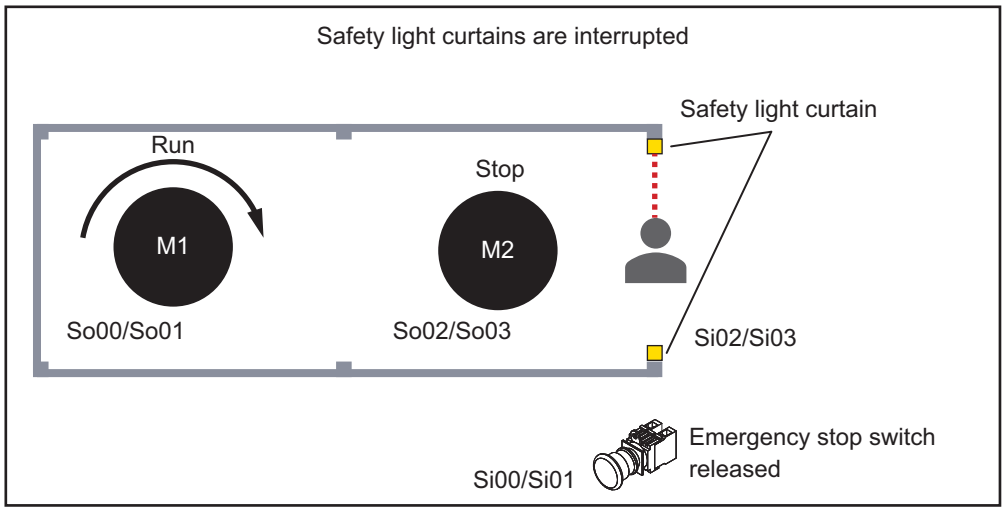
In normal operation, two drive devices, M1 and M2, are running.



When emergency stop switch S1 is pressed, both drive devices M1 and M2 stop.

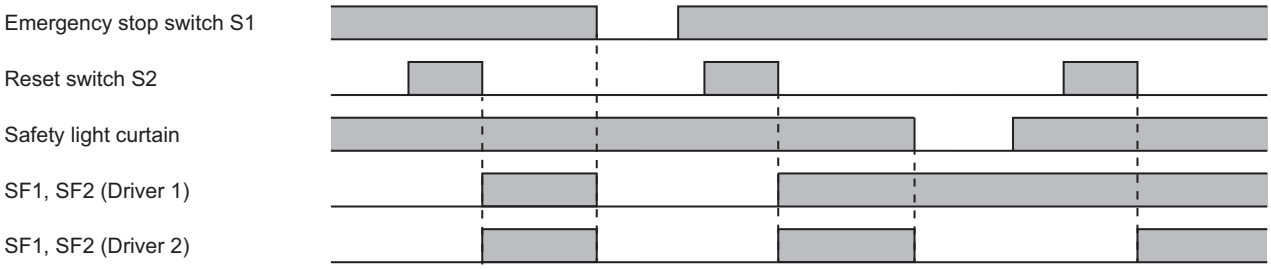


When the safety light curtain is interrupted, only drive device M2 stops.



● Timing Chart

The timing chart is shown below.



● I/O Configuration Settings

The details of the I/O configuration settings are as follows.

Inputs

Input	Device	Test Output Mode	ON->OFF delay time	OFF->ON delay time	Discrepancy time
Si00/T00	Emergency stop switch (dual-channel equivalent input)	Test Output	0 ms	0 ms	500 ms
Si01/T01		Test Output	0 ms	0 ms	
Si02/T02	Safety light curtain	Power Supply Output	0 ms	0 ms	500 ms
Si03/T03		Standard Output	0 ms	0 ms	
Si04/T04	-	Not Used	-	-	-
Si05/T05	-	Not Used	-	-	-
Si06/T06	Reset switch	Test Output	0 ms	0 ms	-
Si07/T07	-	Standard Output	-	-	-
Si08/T08	-	Not Used	-	-	-
Si09/T09	-	Not Used	-	-	-
Si10/T10	-	Not Used	-	-	-
Si11/T11	-	Not Used	-	-	-

Input error latch signal: 1,000 ms

Outputs

Output	Device	EDM feedback setting	ON->OFF delay time	OFF->ON delay time
So00/So01	Dual-channel equivalent output (with test pulse)	Unused	0 × 100 ms	0 × 100 ms
So02/So03	Dual-channel equivalent output (with test pulse)	Unused	0 × 100 ms	0 × 100 ms

Output error latch signal: 1,000 ms

Logic

Input	Device	Input type	Reset type	So00/So01	So02/So03
Si00/Si01	Emergency stop switch (dual-channel equivalent input)	-	Manual(Si06)	0	0
Si02/Si03	Safety light curtain	-	Manual(Si06)	1	0

Reset signal	Minimum ON pulse width [ms]	Maximum ON pulse width [ms]
Si06	350	2,000

Power-on mode Executing

Signature

Safety Configuration CRC (SCCRC): 519F5023

Safety Configuration Time Stamp (SCTS): 4D0C00000000

● Connecting Line Diagrams

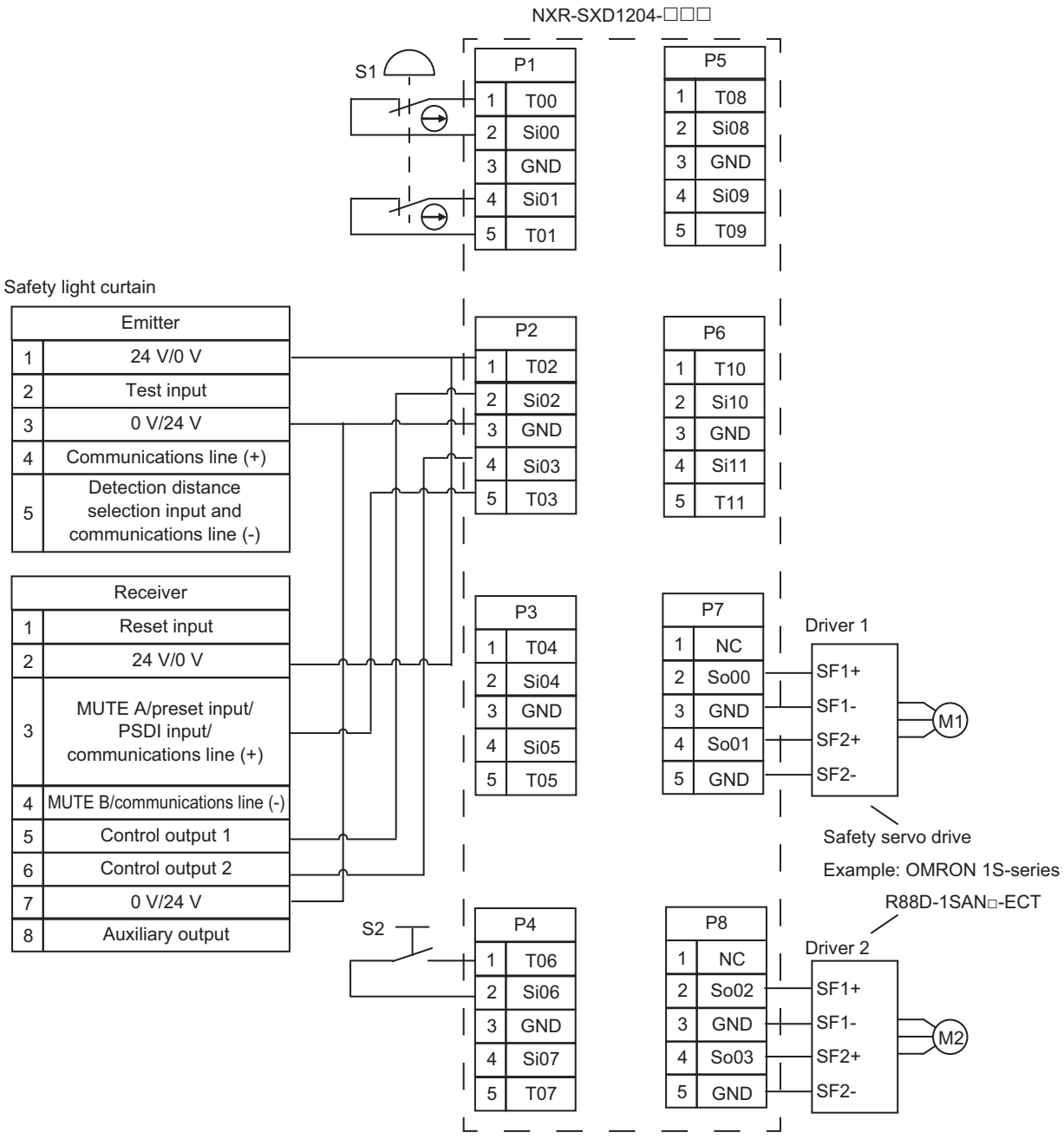
The connecting line diagram for the NXR-SXD1204-□□□ is shown below.

S1: Emergency stop switch

S2: Reset switch

SF1, SF2: Safety inputs of STO function of safety servo drive

M1, M2: Drive device



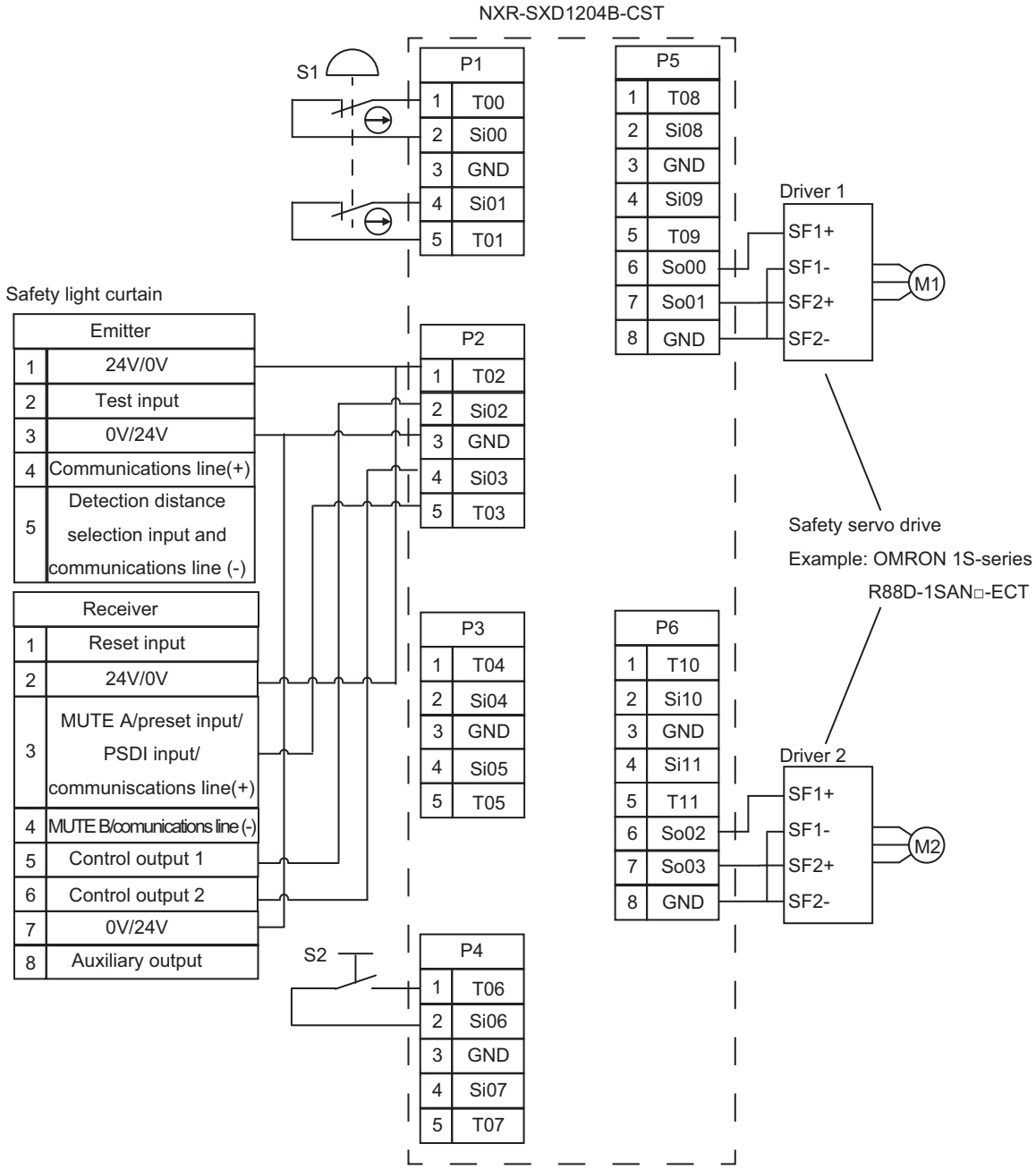
The connecting line diagram for the NXR-SXD1204B-CST is shown below.

S1: Emergency stop switch

S2: Reset switch

SF1, SF2: Safety inputs of STO function of safety servo drive

M1, M2: Drive device



Precautions

Precautions for Correct Use

- Select the safety light curtains and emergency stop switches according to the safety requirement level of the system.
- For the safety servo drives, select devices that can achieve the safety requirement level of the system without using EDM.
- Test the functionality every six months to detect faults in the safety input circuits of the servo drives.
- 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.

No. 2 Partial Stop + Entire Stop Application (With EDM)

Partial stop + entire stop application (with EDM) is an application to perform a partial stop using a safety light curtain and an entire stop using an emergency stop switch. It is an application with external device monitoring (EDM) added to *partial stop + entire stop application*.

● Overview of the Application

The details of the application are the same as for *partial stop + entire stop application*.

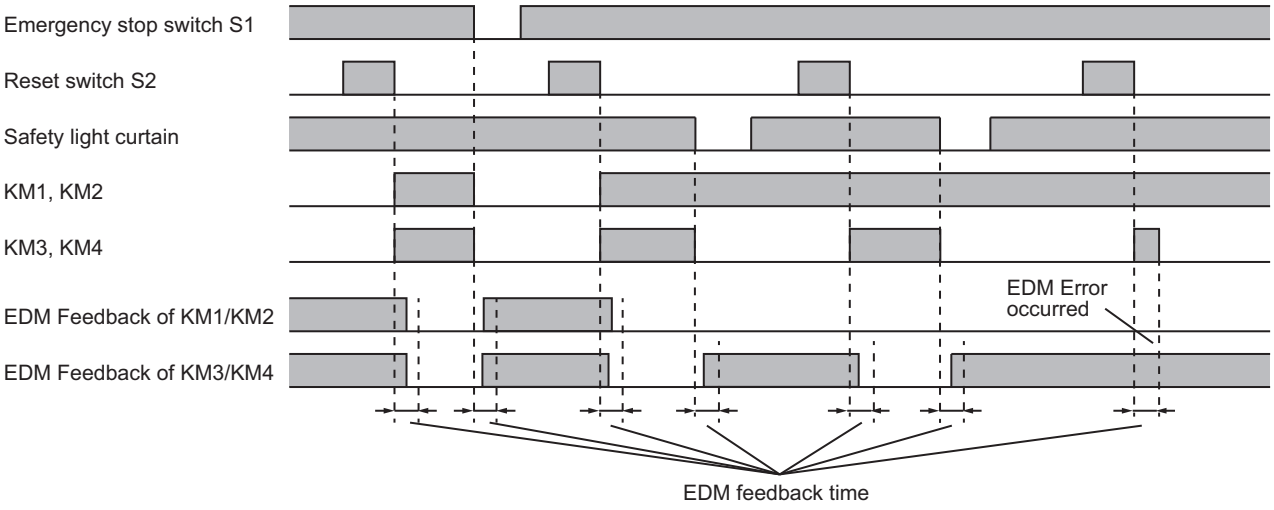
Safety category/PL/SIL	Specification
Safety category	Up to Cat.4
PL	Up to PLe
SIL	Up to SIL3

● Operation

The operation is the same as for *partial stop + entire stop application*.

● Timing Chart

The timing chart is shown below.



I/O Configuration Settings

The details of the I/O configuration settings are as follows.

Inputs

Input	Device	Test Output Mode	ON->OFF delay time	OFF->ON delay time	Discrepancy time
Si00/T00	Emergency stop switch (dual-channel equivalent input)	Test Output	0 ms	0 ms	500 ms
Si01/T01		Test Output	0 ms	0 ms	
Si02/T02	Safety light curtain	Power Supply Output	0 ms	0 ms	500 ms
Si03/T03		Standard Output	0 ms	0 ms	
Si04/T04	-	Not Used	-	-	-
Si05/T05	-	Not Used	-	-	-
Si06/T06	Reset switch	Test Output	0 ms	0 ms	-
Si07/T07	-	Not Used	-	-	-
Si08/T08	EDM feedback	Test Output	0 ms	0 ms	-
Si09/T09	-	Not Used	-	-	-
Si10/T10	EDM feedback	Test Output	0 ms	0 ms	-
Si11/T11	-	Not Used	-	-	-

Input error latch signal: 1,000 ms

Outputs

Output	Device	EDM feedback setting	ON->OFF delay time	OFF->ON delay time
So00/So01	Dual-channel equivalent output (with test pulse)	Si08	0 × 100 ms	0 × 100 ms
So02/So03	Dual-channel equivalent output (with test pulse)	Si10	0 × 100 ms	0 × 100 ms

Output error latch signal: 1,000 ms

Logic

Inputs	Device	Input type	Reset type	So00/So01	So02/So03
Si00/Si01	Emergency stop switch (dual-channel equivalent input)	-	Manual(Si06)	0	0
Si02/Si03	Safety light curtain	-	Manual(Si06)	1	0

Reset signal	Minimum ON pulse width [ms]	Maximum ON pulse width [ms]
Si06	350	2,000

Power-on mode Executing

Signature

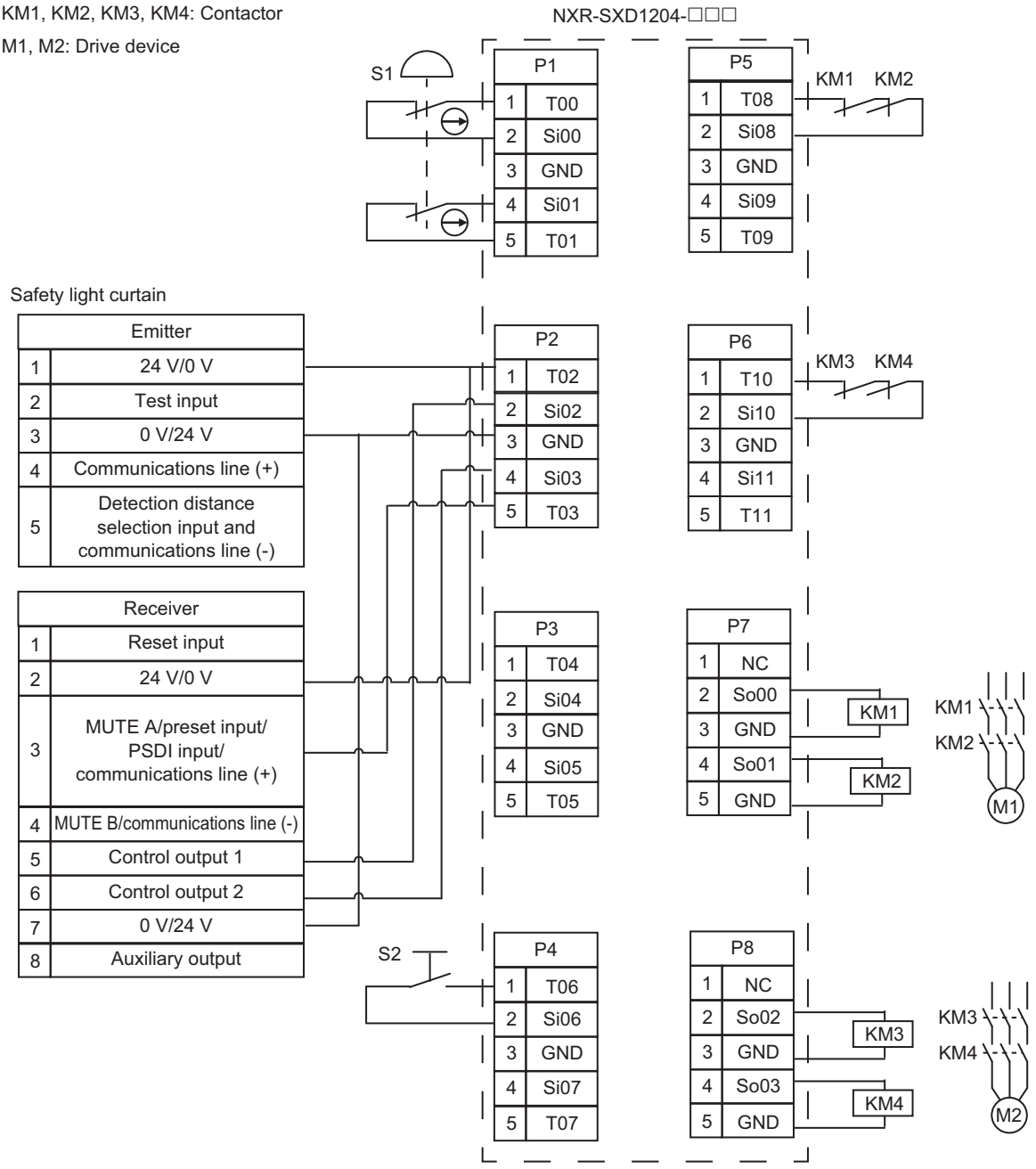
Safety Configuration CRC (SCCRC): C54E34C8

Safety Configuration Time Stamp (SCTS): 4D0C00000000

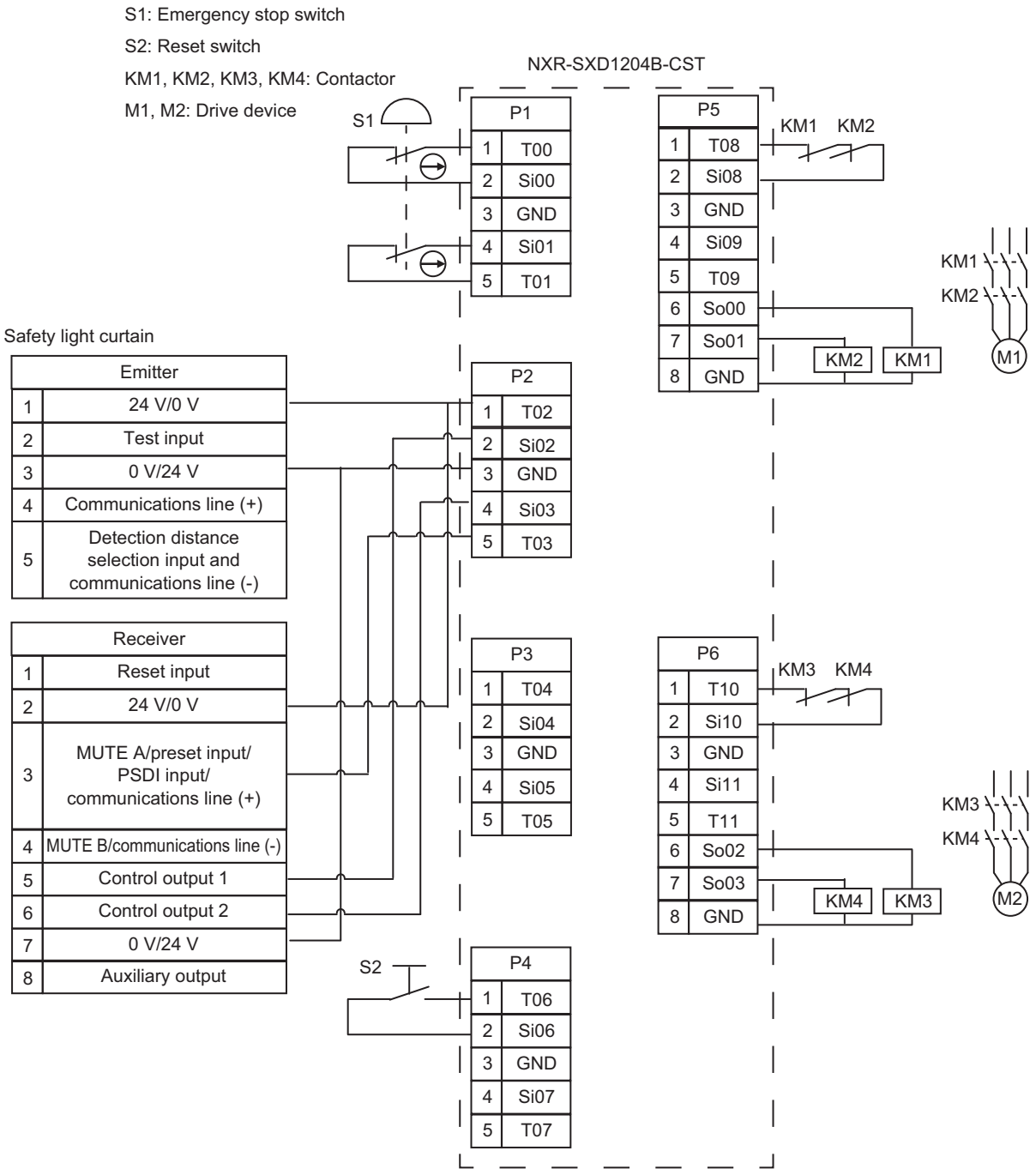
● Connecting Line Diagrams

The connecting line diagram for the NXR-SXD1204-□□□ is shown below.

S1: Emergency stop switch
S2: Reset switch
KM1, KM2, KM3, KM4: Contactor
M1, M2: Drive device



The connecting line diagram for the NXR-SXD1204B-CST is shown below.



● Precautions

Precautions for Correct Use

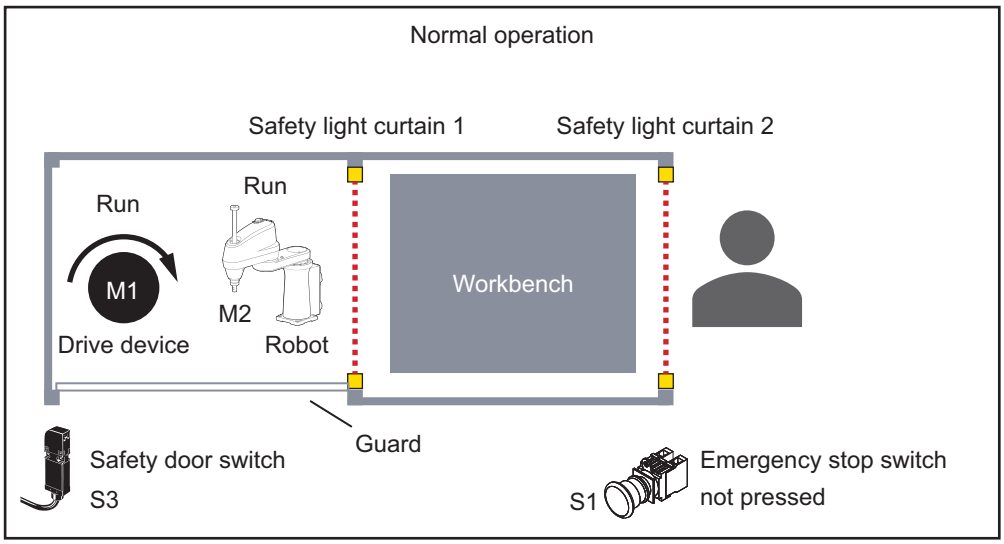
- Select the safety light curtains and emergency stop switches according to the safety request level of the system.
- Test the functionality every month to detect welded contactor contacts.
- The customer is responsible for attaining conformance of the entire system to standards.
- To detect electrical and mechanical failures, use a combination of redundant semiconductor output contacts and redundant mechanical output devices.

No. 3 Worker and Robot Automatic Switching Application

Worker and robot automatic switching application is an application to perform automatic switching of the worker and robot and perform an entire stop using an emergency stop switch and guard. It stops the robot as necessary to prevent contact between the worker and robot.

● Overview of the Application

At the production site, one drive device and one robot are running.
There is a workbench beside the robot. When the robot places a product on the workbench, a worker picks up that workpiece from the opposite side.
Safety light curtains are installed on both sides of the workbench. It is dangerous if both the robot and worker access the workbench at the same time, so the robot stops if both of the two pairs of safety light curtains are interrupted. When that happens, the drive device at the back of the robot does not stop.
There is a guard for maintenance in the space where the drive device and robot are installed, and a safety door switch is installed. If the worker opens the door, both the drive device and robot stop entirely.
If an abnormality has occurred, the worker presses an emergency stop switch. Both the drive device and robot stop entirely in that case as well.



Safety category/PL/SIL	Specifications
Safety category	Up to Cat.3
PL	Up to PLe
SIL	Up to SIL3

Operation

The specifications for operation using an input signal from each device is as follows.

When emergency stop switch S1 is pressed

- If emergency stop switch S1 is pressed, the power supply to drive device M1 and robot M2 is shut off immediately.
- The power supply to robot M2 is retained in the shut-off state until the guard is closed, the light beam of safety light curtain 1 or safety light curtain 2 enters, emergency stop switch S1 is released, and reset switch S2 is pressed.
- The power supply to drive device M1 is retained in the shut-off state until the guard is closed, the emergency stop switch S1 is released, and reset switch S2 is pressed.

When the guard is opened (emergency stop switch S1 is not pressed)

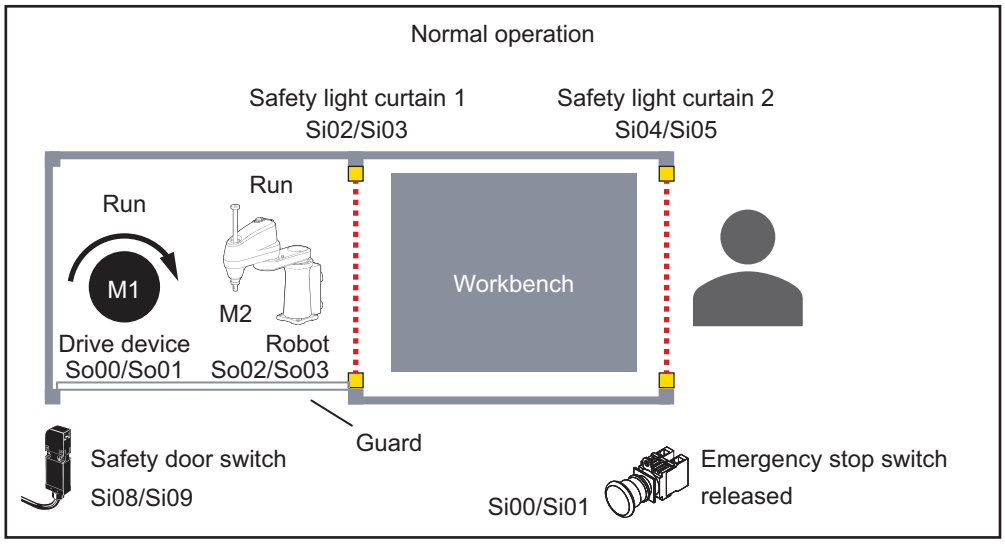
- The fact that the guard was opened is detected by safety door switch S3, and the power supply to drive device M1 and robot M2 is shut off immediately.
- The power supply to robot M2 is retained in the shut-off state until the guard is closed, the light beam of safety light curtain 1 or safety light curtain 2 enters, and reset switch S2 is pressed.
- The power supply to drive device M1 is retained in the shut-off state until the guard is closed and reset switch S2 is pressed.

When the safety light curtain is interrupted (emergency stop switch S1 is not pressed and guard is closed)

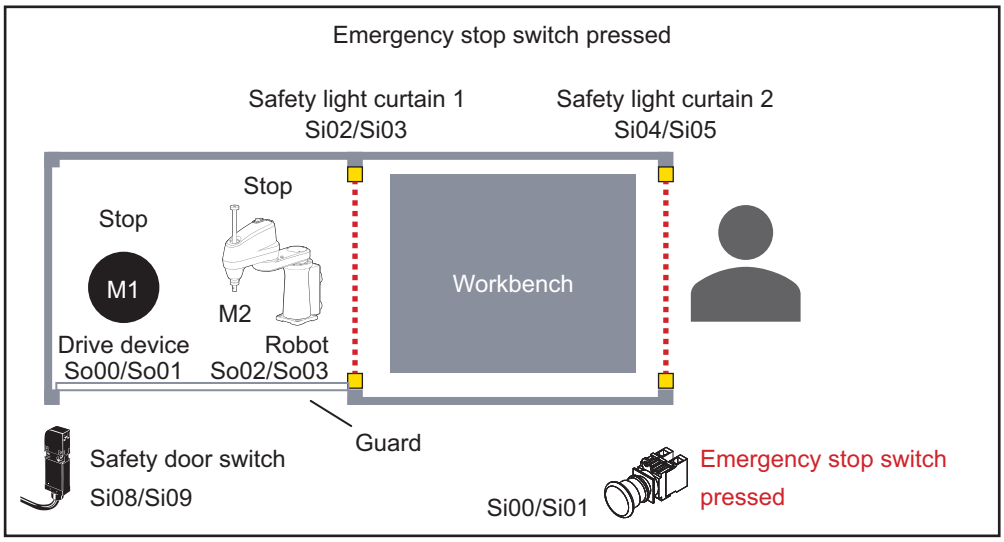
- When both safety light curtain 1 and safety light curtain 2 are interrupted, the power supply to robot M2 is shut off immediately. Power continues to be supplied to drive device M1.
- The power supply to robot M2 is retained in the shut-off state until the light beam of safety light curtain 1 or safety light curtain 2 enters.

The operation in each situation is illustrated in the figures.

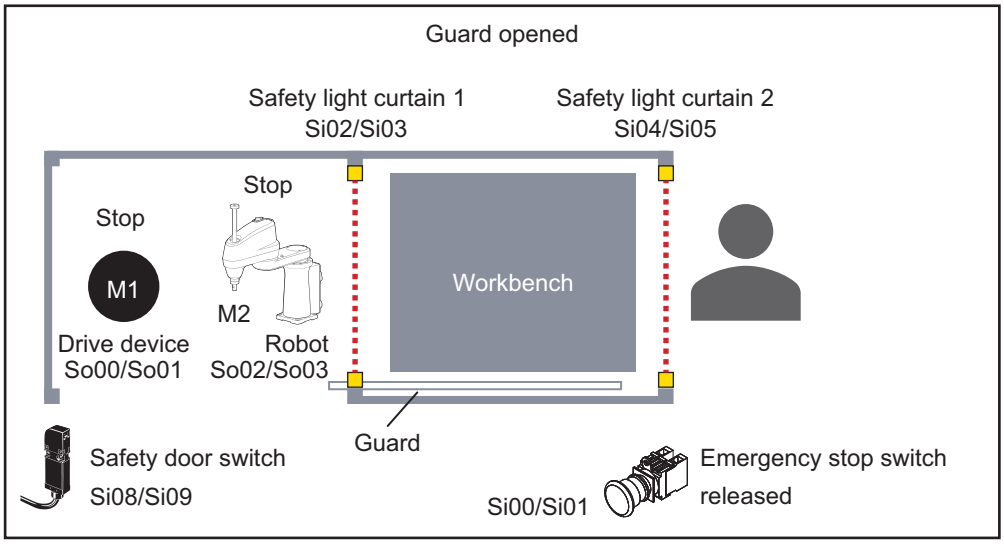
In normal operation, one drive device M1 and one robot M2 are running.



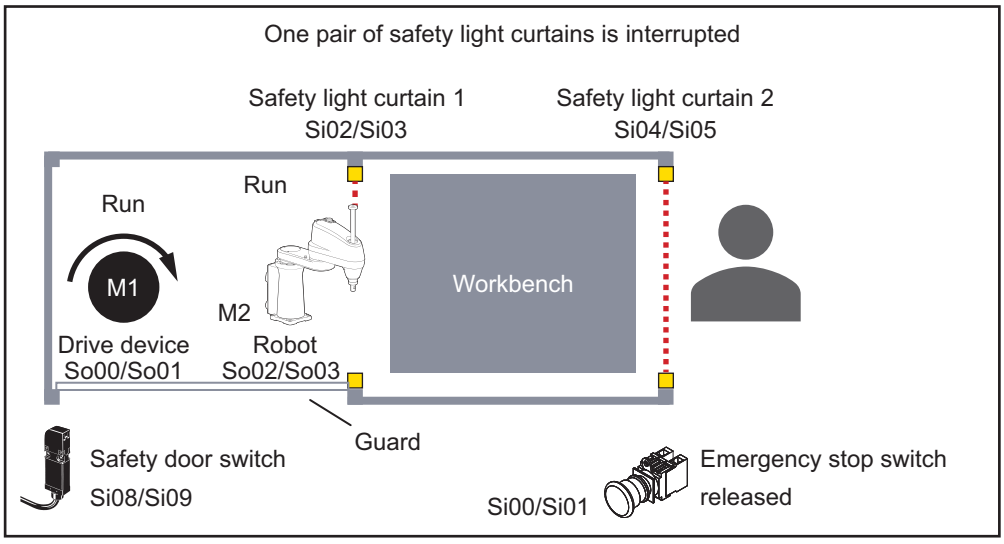
When emergency stop switch S1 is pressed, both drive device M1 and robot M2 stop.

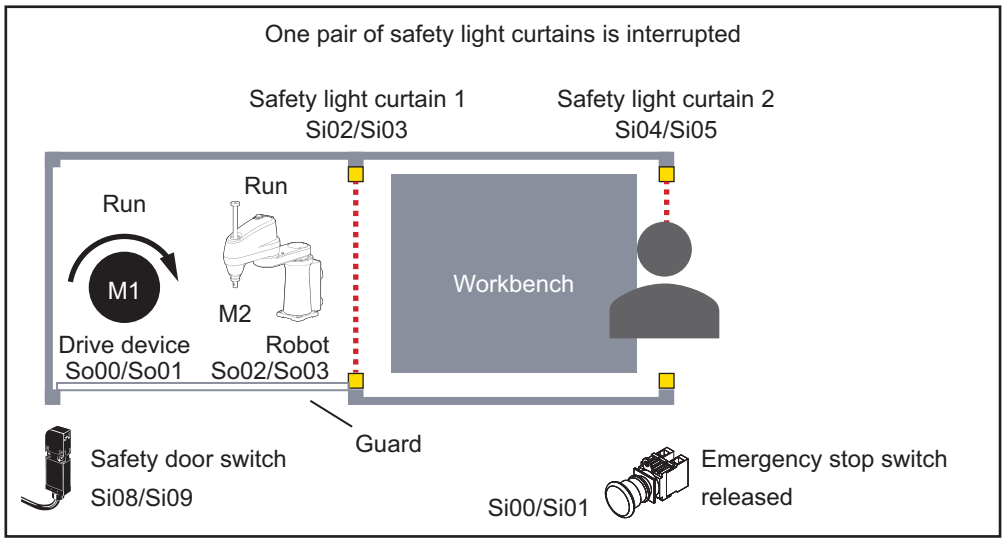


If the guard is opened, both drive device M1 and robot M2 stop.

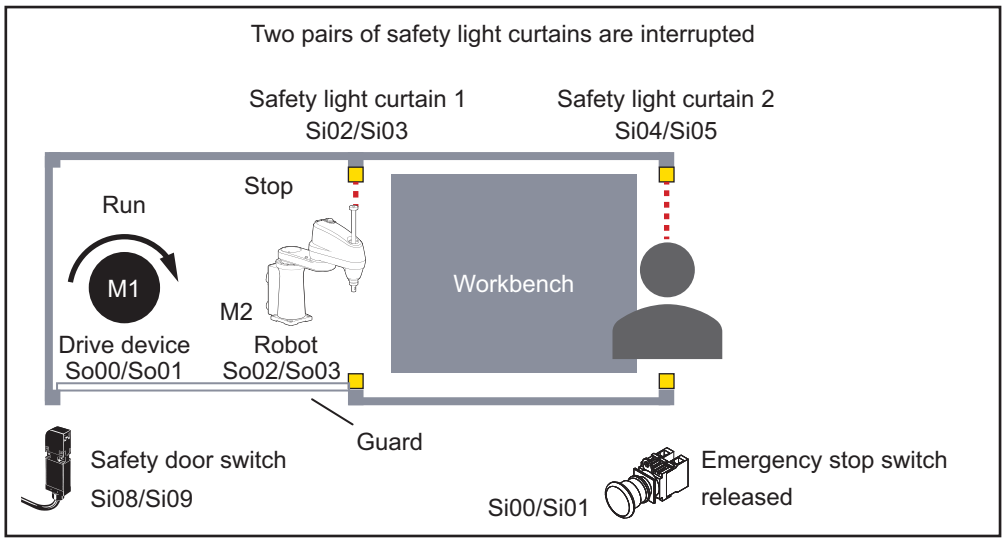


Drive device M1 and robot M2 both continue running even if one of the two pairs of safety light curtains is interrupted.



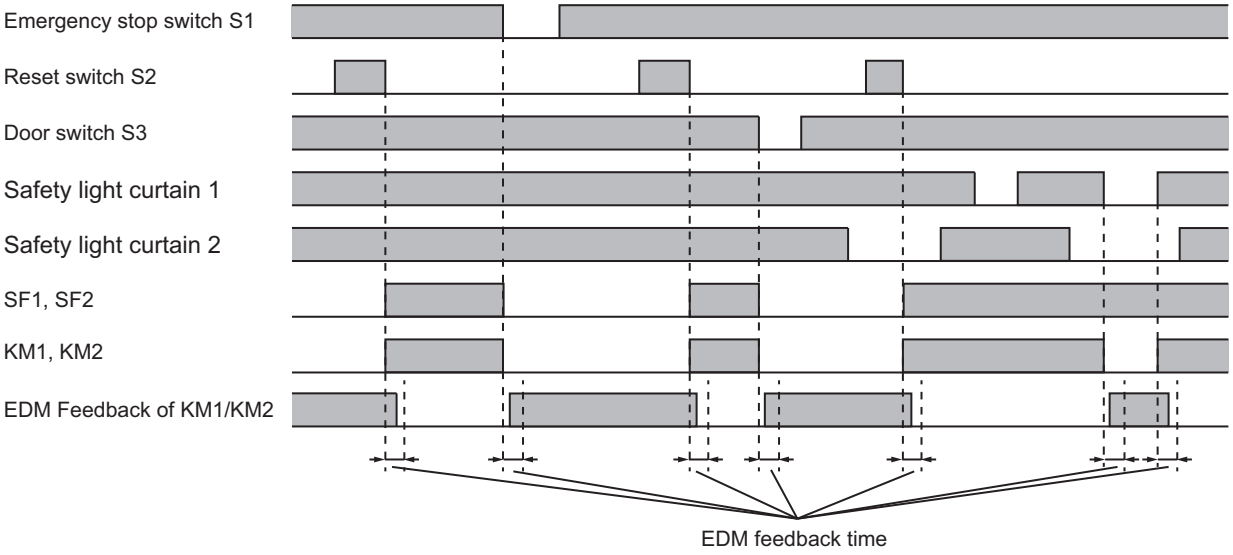


If both of the two pairs of safety light curtains are interrupted, robot M2 stops because there is the risk of contact between the worker and robot M2. Drive device M1 continues running.



● Timing Chart

The timing chart is shown below.



● I/O Configuration Settings

The details of the I/O configuration settings are as follows.

Inputs

Input	Device	Test Output Mode	ON->OFF delay time	OFF->ON delay time	Discrepancy time
Si00/T00	Emergency stop switch (dual-channel equivalent input)	Test Output	0 ms	0 ms	500 ms
Si01/T01		Test Output	0 ms	0 ms	
Si02/T02	Safety light curtain	Power Supply Output	0 ms	0 ms	500 ms
Si03/T03		Standard Output	0 ms	0 ms	
Si04/T04	Safety light curtain	Power Supply Output	0 ms	0 ms	500 ms
Si05/T05		Standard Output	0 ms	0 ms	
Si06/T06	Reset switch	Test Output	0 ms	0 ms	-
Si07/T07	-	Standard Output	-	-	-
Si08/T08	Safety door switch (dual-channel equivalent input)	Test Output	0 ms	0 ms	500 ms
Si09/T09		Test Output	0 ms	0 ms	
Si10/T10	EDM feedback	Test Output	0 ms	0 ms	-
Si11/T11	-	Not Used	-	-	-

Input error latch signal: 1,000 ms

Outputs

Output	Device	EDM feedback setting	ON->OFF delay time	OFF->ON delay time
So00/So01	Dual-channel equivalent output (with test pulse)	Unused	0 × 100 ms	0 × 100 ms
So02/So03	Dual-channel equivalent output (with test pulse)	Si10	0 × 100 ms	0 × 100 ms

Output error latch signal: 1,000 ms

Logic

Inputs	Device	Input type	Reset type	So00/So01	So02/So03
Si00/Si01	Emergency stop switch (dual-channel equivalent input)	-	Manual(Si06)	0	0
Si08/Si09	Safety door switch (dual-channel equivalent input)	-	Manual(Si06)	0	0
Si02/Si03	Safety light curtain	2 Input(OR)	Auto	1	0
Si04/Si05	Safety light curtain				

Reset signal	Minimum ON pulse width [ms]	Maximum ON pulse width [ms]
Si06	350	2,000

Power-on mode Executing

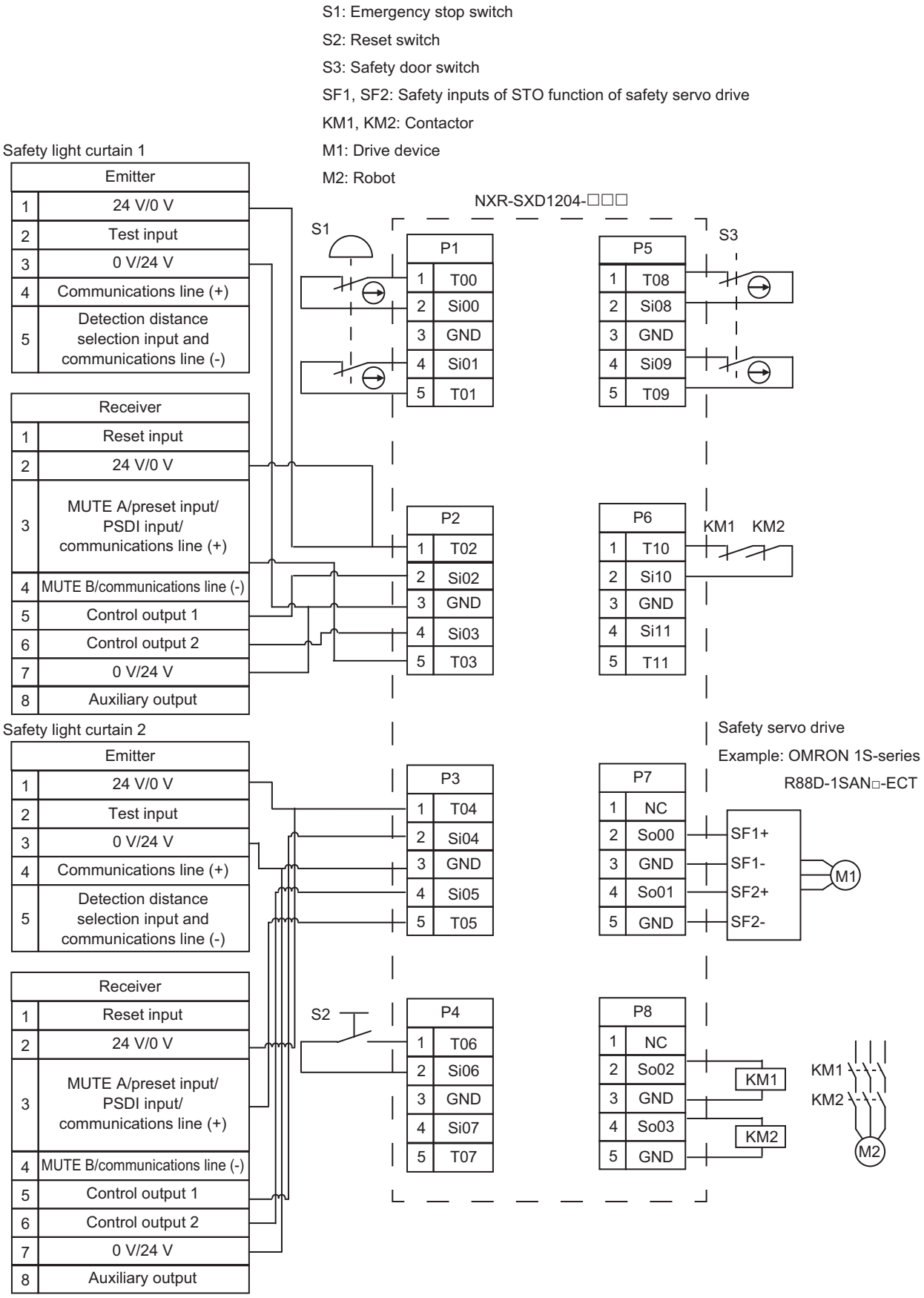
Signature

Safety Configuration CRC (SCCRC): F63EF4B6

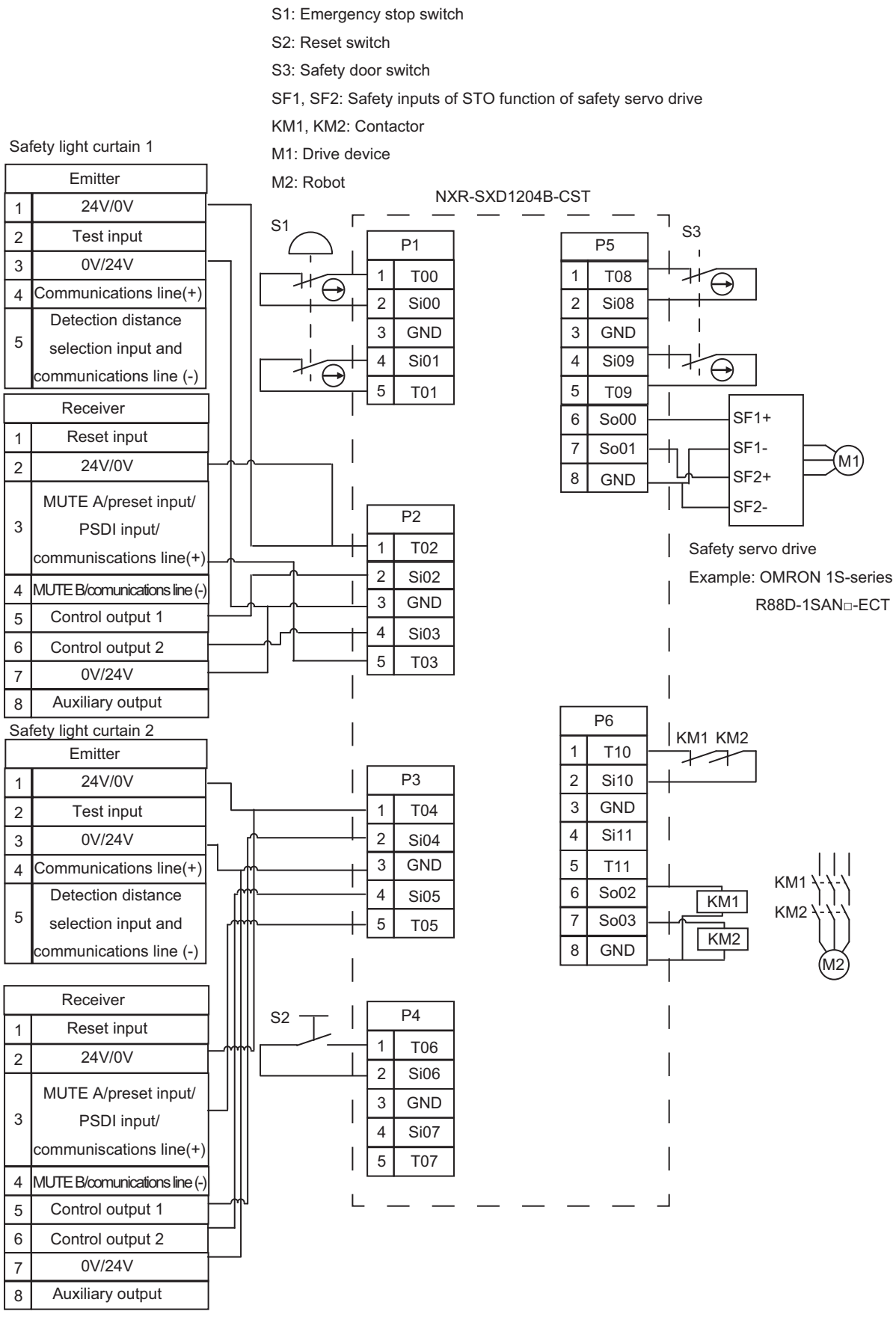
Safety Configuration Time Stamp (SCTS): 4D0C00000000

● Connecting Line Diagrams

The connecting line diagram for the NXR-SXD1204-□□□ is shown below.



The connecting line diagram for the NXR-SXD1204B-CST is shown below.



Precautions

Precautions for Correct Use

- Select the devices to connect according to the safety request level of the system.
- For the safety servo drives, select devices that can achieve the safety requirement level of the system without using EDM.
- Test the functionality every month to detect welded contactor contacts.
- Test the functionality every six months to detect faults in the safety input circuits of the servo drives.
- 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.

6-8 Operating Modes

This section describes the operating modes of the Safety I/O Block.

6-8-1 Operating Mode Types

The Safety I/O Block has the following operating modes.
The operating mode can be confirmed from the MS indicator or operating status monitor of the Web UI.

Operating mode	Display in the Web UI	MS indicator status	Operations in remote I/O mode	Operations in simple logic mode
Operating status (Executing)	Executing	Lit green	Status while Safety I/O Block is operating All functions are operating, and normal operation is being performed. The statuses of the main safety functions in this status are as follows. • Logic function: Disabled • CIP Safety communications: Connection established • Safety input: Enabled • Safety output: Enabled If a CIP Safety connection is opened in the operation standby status (idle), the status transitions to this status.	Status while Safety I/O Block is operating All functions are operating, and normal operation is being performed. The statuses of the main safety functions in this status are as follows. • Logic function: Executing • CIP Safety communications: Communications are possible • Safety input: Enabled • Safety output: Enabled Transitions to this status if the operating status is instructed from the operating mode change function in the operation standby status (idle).
Operation standby status (Idle)	Idle	Flashing green	Status where the safety configuration is completed, and waiting to transition to the operating status (executing). The statuses of the main safety functions in this status are as follows. • Logic function: Disabled • CIP Safety communications: Waiting to establish connection • Safety input: Enabled • Safety output: Clear If the CIP Safety connections are all disconnected in the operating status (executing), the status transitions to this status.	Status where the safety configuration is completed, and waiting to transition to the operating status (executing). The statuses of the main safety functions in this status are as follows. • Logic function: Stopped • CIP Safety communications: Communications are possible • Safety input: Enabled • Safety output: Clear Transitions to this status if the operation standby status is instructed from the operating mode change function in the operating status (executing).
TUNID setting wait status (Waiting for TUNID)	Waiting for TUNID	Flashing green and red	Status where the TUNID is not set The software settings of the IP address can be configured in this status.	
Configuration wait status (Configuring)	Configuring	Flashing green and red	Status where the TUNID settings are completed, and the safety configuration is not configured	
Operation aborted error (Abort)	Abort	Flashing red	Nonfatal error is occurring	

Operating mode	Display in the Web UI	MS indicator status	Operations in remote I/O mode	Operations in simple logic mode
Critical fault (Critical Fault)	Critical Fault	Lit red	A critical fault is occurring All functions stop, and transitions to a safe state.	
Initializing (Self-Testing)	Self-Testing	Flashing green and red	Status where executing the self-diagnosis required to guarantee the safety functions	-
IP address indication (IP Address Display)	Web UI access is not possible	Not lit	Status where executing IP address indication function	-
I/O wiring checking (I/O Wiring Checking)	Reading is not possible Web UI access is not possible	Not lit	Status where executing I/O wiring checking function	-

6-8-2 Functions Executable in Each Operating Mode

The possibility of executing each function in each operating mode is as follows.

Function	Normal operating modes							Special modes	
	Initializing (Self-Testing)	TUNID setting wait status (Waiting for TUNID)	Configuration wait status (Configuring)	Operation standby status (Idle)	Operating status (Executing)	Operation aborted error (Abort)	Critical fault (Critical Fault)	IP address indication (IP Address Display)	I/O wiring checking (I/O Wiring Checking)
CIP Safety communications	Not possible	Not possible	Not possible	Possible	Possible	Not possible	Not possible	Not possible	Not possible
EtherNet/IP communications	Not possible	Not possible	Not possible	Possible	Possible	Not possible	Not possible	Not possible	Not possible
CIP message communications	Not possible	Possible	Possible	Possible	Possible	Possible	Not possible	Not possible	Not possible
Access from the Web UI	Not possible	Possible	Possible	Possible	Possible	Possible	Not possible	Not possible	Not possible
Safety input function	Not possible	Not possible	Not possible	Possible	Possible	Possible	Not possible	Not possible	Possible*1
Test output function	Not possible	Not possible	Not possible	Possible	Possible	Possible	Not possible	Not possible	Possible*1

Function	Normal operating modes							Special modes	
	Initializing (Self-Testing)	TUNID setting wait status (Waiting for TUNID)	Configuration wait status (Configuring)	Operation standby status (Idle)	Operating status (Executing)	Operation aborted error (Abort)	Critical fault (Critical Fault)	IP address indication (IP Address Display)	I/O wiring checking (I/O Wiring Checking)
Safety output function	Not possible	Not possible	Not possible	Not possible	Possible	Possible	Not possible	Not possible	Possible*1
IP address setting function	Not possible	Possible	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible
Power OFF function for through-wiring output	Not possible	Possible	Possible	Possible	Possible	Possible	Not possible	Not possible	Not possible
Simple logic function	Not possible	Not possible	Not possible	Not possible	Possible*2	Not possible	Not possible	Not possible	Possible*1
I/O wiring checking function	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible	Possible
IP address indication function	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible	Possible	Not possible
Backup of backup function	Not possible	Not possible	Not possible	Possible	Possible	Not possible	Not possible	Not possible	Not possible
Verification of backup function	Not possible	Possible	Possible	Possible	Possible	Possible	Not possible	Not possible	Not possible
Restoration of backup function	Not possible	Possible	Possible	Possible*3	Possible*3	Possible	Not possible	Not possible	Not possible
Firmware update function	Not possible	Possible	Possible	Possible*3	Possible*3	Possible	Not possible	Not possible	Not possible
Changing the safety password	Not possible	Possible	Possible	Possible	Possible	Possible	Not possible	Not possible	Not possible
Operating mode change function	Not possible	Not possible	Not possible	Possible	Possible	Not possible	Not possible	Not possible	Not possible
Configuration lock function	Not possible	Not possible	Not possible	Possible	Possible	Possible*4	Not possible	Not possible	Not possible
Restart function	Not possible	Possible	Possible	Possible*3	Possible*3	Possible	Not possible	Not possible	Not possible

Function	Normal operating modes							Special modes	
	Initializing (Self-Testing)	TUNID setting wait status (Waiting for TUNID)	Configuration wait status (Configuring)	Operation standby status (Idle)	Operating status (Executing)	Operation aborted error (Abort)	Critical fault (Critical Fault)	IP address indication (IP Address Display)	I/O wiring checking (I/O Wiring Checking)
Clear all memory function	Not possible	Possible	Possible	Possible*3	Possible*3	Possible	Not possible	Not possible	Not possible

***1.** Operates with I/O wiring checking dedicated settings.
***2.** In remote I/O mode, the simple logical processing functions do not operate.
***3.** Not possible while the CIP Safety communications connection is established.
***4.** Unlocking of the configuration only is possible.

6-8-3 Web UI Functions Executable in Each Operating Mode

The possibility of executing each Web UI function in each operating mode is as follows.

Screen	Function	Operating mode				
		TUNID setting wait status (Waiting for TUNID)	Configuration wait status (Configuring)	Operation standby status (Idle)	Operating status (Executing)	Operation aborted error (Abort)
Operating Status Monitor screen	Operating status monitor	Possible	Possible	Possible	Possible	Possible
I/O Monitor screen	I/O monitor	Possible	Possible	Possible	Possible	Possible
Current Error/Event Log screen	Display current error	Possible	Possible	Possible	Possible	Possible
	Event log display and file output	Possible	Possible	Possible	Possible	Possible
	Clear event log	Possible	Possible	Possible	Possible	Possible
Production Information screen	Display production information	Possible	Possible	Possible	Possible	Possible
TCP/IP Settings screen	Write TCP/IP settings	Possible	Not possible	Not possible	Not possible	Not possible
	Read TCP/IP settings	Possible	Possible	Possible	Possible	Possible
TUNID Settings screen	Write TUNID	Possible	Not possible	Not possible	Not possible	Not possible
	Read TUNID	Possible	Possible	Possible	Possible	Possible
Safety Application Settings screen	Display safety application settings	Possible	Possible	Possible	Possible	Possible
	Write and delete safety application settings	Possible	Possible	Possible	Possible	Possible
Automatic Clock Adjustment Settings screen	Write automatic clock adjustment settings	Possible	Possible	Possible	Possible	Possible
	Read automatic clock adjustment settings	Possible	Possible	Possible	Possible	Possible

Screen	Function	Operating mode				
		TUNID setting wait status (Waiting for TUNID)	Configuration wait status (Configuring)	Operation standby status (Idle)	Operating status (Executing)	Operation aborted error (Abort)
Change Operating Mode screen	Change operating mode	Not possible	Not possible	Possible	Possible	Not possible
Configuration Lock screen	Lock the configuration	Not possible	Not possible	Possible	Possible	Not possible
	Unlock the configuration	Not possible	Not possible	Possible	Possible	Possible
Restart screen	Restart	Possible	Possible	Possible*1	Possible*1	Possible
Memory All Clear screen	Clear all memory	Possible	Possible	Possible*1	Possible*1	Possible
Backup	Backup	Not possible	Not possible	Possible	Possible	Not possible
	Verify	Possible	Possible	Possible	Possible	Possible
	Restore	Possible	Possible	Possible*1	Possible*1	Possible
Send General CIP Command screen	Send general CIP command	Possible	Possible	Possible	Possible	Possible
Unit Identification screen	Identify Unit	Possible	Possible	Possible	Possible	Possible
Communications Cable Diagnosis screen	Diagnose communications cable	Possible	Possible	Possible	Possible	Possible
Safety Password Setting screen	Set safety password	Possible	Possible	Possible	Possible	Possible
Update Firmware screen	Update firmware	Possible	Possible	Possible*1	Possible*1	Possible

***1.** Not possible while the CIP Safety communications connection is established.

6-8-4 Operating Mode Changing and Power-on Mode

When the safety application to be used is a fixed application, user-defined application, or add-on application, you need to change the operating mode to switch between executing and stopping the logic function.
Refer to *7-16 Changing the Operating Mode* on page 7-95 for the procedure to change the operating mode using Sysmac Studio or the Web UI.
In addition, you can specify the operating mode at power-on in the settings of the safety application.
The differences in operation depending on the power-on mode are as follows:

Power-on mode	Operation
Executing	• The status becomes *Operating status* at power-on, and the logic function is executed automatically. • Since the power-on mode of a fixed application is set to *Executing*, startup is in the *Operating status* when the power is turned ON again while TUNID is set. • The status transitions to *Operating status* immediately after configured using Type1 Safety Open with the user-defined application.

Power-on mode	Operation
Idle	• The status becomes *Operating wait status* at power-on, and startup is with the logic function in the stopped state.

7

Safety I/O Block Settings

This chapter describes the various settings of the Safety I/O Block.

7-1 Setting Procedure 7-3
- 7-1-1 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open) 7-3
- 7-1-2 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI) 7-6
- 7-1-3 Setting Procedure of Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application 7-9
- 7-1-4 Setting Procedure of Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User 7-11
- 7-1-5 Setting Procedure of Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User 7-14

7-2 Overview of the Web UI 7-17
- 7-2-1 Various Specifications of the Web UI 7-17
- 7-2-2 Operation Authorities of the Web UI 7-17
- 7-2-3 Screen Configuration of Web UI 7-17
- 7-2-4 Main Menu List 7-18
- 7-2-5 Web UI Startup Procedure 7-21
- 7-2-6 Login 7-22
- 7-2-7 Logout 7-24
- 7-2-8 Precautions for Initial Login 7-24

7-3 CIP Safety Communications Settings 7-27
- 7-3-1 Connection Settings for CIP Safety Communications 7-27
- 7-3-2 Exporting and Importing the Settings of the Safety I/O Block 7-36

7-4 EtherNet/IP Communications Settings 7-38
- 7-4-1 Setting Tag Data Link Communications 7-38
- 7-4-2 LLDP Function 7-42

7-5 Safety Input Functions Settings 7-44
- 7-5-1 Setting Procedure for Safety Input Functions 7-44
- 7-5-2 Setting Procedure for Standard Output Functions 7-47

7-6 Setting Safety Output Functions 7-50
- 7-6-1 Safety Output Function Setting Procedure 7-50

7-7 Logic Function Settings 7-53
- 7-7-1 Logic Setting Procedure 7-53
- 7-7-2 Displaying the Parameter List 7-58

7-7-3 Examples of Abnormal Operations of Input Devices That Should Be Considered 7-59

7-8 Setting the Safety Signatures 7-63

7-9 Create the safety application file 7-65
7-9-1 Registration of Safety I/O Block 7-65
7-9-2 Safety Application Settings 7-66
7-9-3 Safety I/O Functions Settings 7-68
7-9-4 Logic Function Settings 7-68
7-9-5 Exporting a Safety Application File 7-68

7-10 Setting IP Addresses 7-71
7-10-1 IP Address Configuration 7-71
7-10-2 Selecting the Method to Set the IP Address Using the Rotary Switches 7-73
7-10-3 Setting by Sysmac Studio 7-74
7-10-4 Setting by Web UI 7-76

7-11 TUNID Settings 7-78
7-11-1 Purpose of TUNID 7-78
7-11-2 TUNID Setting Procedure 7-78

7-12 Selecting the Safety Application 7-83

7-13 Restart 7-84
7-13-1 Purpose of Restart 7-84
7-13-2 Procedure for Using Restart 7-84

7-14 Configuration 7-87
7-14-1 Configuring the Safety Controller 7-87
7-14-2 Configuration of Safety I/O Block 7-87

7-15 Setting the Automatic Clock Adjustment 7-91
7-15-1 Purpose of Automatic Clock Adjustment 7-91
7-15-2 Procedure for Using the Automatic Clock Adjustment 7-91
7-15-3 Details on Automatic Clock Adjustment 7-94

7-16 Changing the Operating Mode 7-95
7-16-1 Procedure for Using Change Operating Mode 7-95

7-17 Configuration Lock 7-99
7-17-1 Purpose of Configuration Lock 7-99
7-17-2 Procedure for Using the Configuration Lock 7-99
7-17-3 Details on Configuration Lock 7-103

7-18 Setting the Safety Password 7-104
7-18-1 Purpose of Safety Password 7-104
7-18-2 Procedure for Using Safety Password Setting 7-104
7-18-3 Details on Safety Password 7-106

7-19 Backup 7-108
7-19-1 Purpose of Backup 7-108
7-19-2 Procedure for Using Backup 7-108
7-19-3 Details on Backup 7-111

7-1 Setting Procedure

The setting procedure of the Safety I/O Block differs depending on the safety control system.
Refer to *1-3-1 Safety Control System* on page 1-4 for details on safety control system configurations.

Precautions for Correct Use

If the settings of the Safety I/O Block are changed in Sysmac Studio, execute a synchronization transfer to apply the setting information of Sysmac Studio to the Safety I/O Block. Refer to *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on synchronization transfer of Sysmac Studio.

7-1-1 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)

The following shows the setting procedure of the configuration for the safety controller to perform control (configuration using Type 1 Safety Open).
The procedure before installation and wiring is as follows:

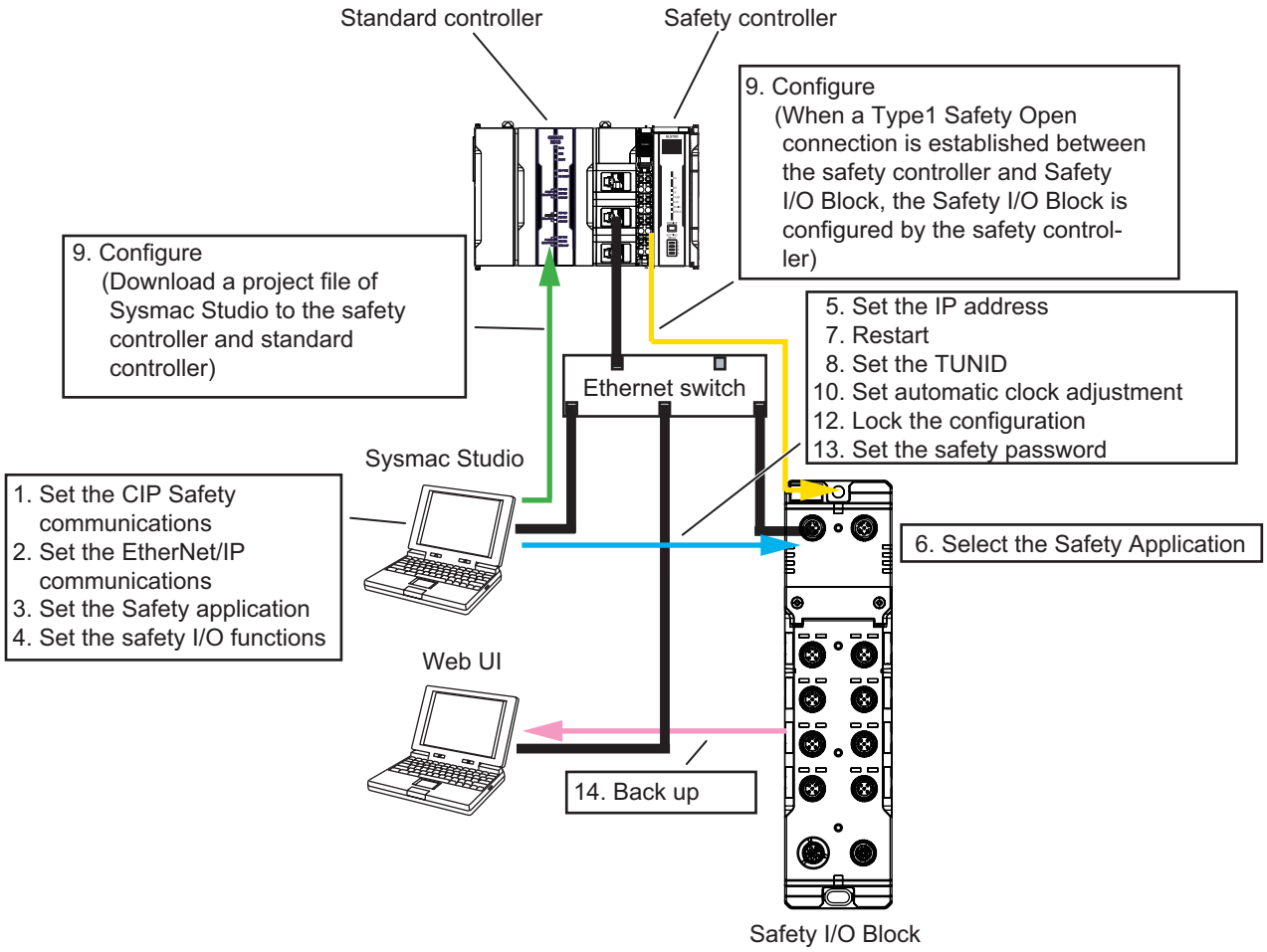
Step	Setting item	Support software to use	Description	Reference
1	Set the CIP Safety communications	Sysmac Studio	Configure the settings for CIP Safety communications between a safety controller and Safety I/O Block in a project file of Sysmac Studio. Select **Configure Target Device (Type1)** for the open type.	*7-3 CIP Safety Communications Settings* on page 7-27
2	Set the EtherNet/IP communications	Sysmac Studio	Configure the settings for EtherNet/IP communications between a standard controller and Safety I/O Block in a project file of Sysmac Studio.	*7-4 EtherNet/IP Communications Settings* on page 7-38
3	Set the safety application	Sysmac Studio	Configure the safety application settings in a project file of Sysmac Studio. Select 00: Remote I/O mode.	*7-9-2 Safety Application Settings* on page 7-66
4	Set the safety I/O functions	Sysmac Studio	Configure the I/O configuration settings for the Safety I/O Block in a project file of Sysmac Studio.	*7-5 Safety Input Functions Settings* on page 7-44 *7-6 Setting Safety Output Functions* on page 7-50

The procedure after installation and wiring is as follows:

Step	Setting item	Support software to use	Description	Reference
5	Set the IP address	Sysmac Studio*1	Configure the IP address settings of the Safety I/O Block.	*7-10 Setting IP Addresses* on page 7-71
6	Select the safety application	-	Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to *0*.	*7-12 Selecting the Safety Application* on page 7-83
7	Restart	Sysmac Studio*1	Restart the Safety I/O Block.	*7-13 Restart* on page 7-84
8	Set the TUNID	Sysmac Studio*1	Configure the TUNID settings of the Safety I/O Block.	*7-11 TUNID Settings* on page 7-78

Step	Setting item	Support software to use	Description	Reference
9	Configure	Sysmac Studio	Download a project file of Sysmac Studio and configure the safety controller and standard controller. The Safety I/O Block is configured by the safety controller when a Type1 Safety Open connection is established between the safety controller and the Safety I/O Block.	*7-14 Configuration* on page 7-87
10	Set automatic clock adjustment	Sysmac Studio*1	Configure the settings for automatic clock adjustment of the Safety I/O Block.	*7-15 Setting the Automatic Clock Adjustment* on page 7-91
11	Check the operation	-	Verify all I/O wiring and the operation of the program to check that the Safety I/O Block operates as intended.	-
12	Lock the configuration	Sysmac Studio*1	Execute safety validation of the safety control system to check that the setting values are correct. After the check, execute locking of the configuration. After executing locking of the configuration, setting values of the Safety I/O Block cannot be changed until the configuration is unlocked.	*7-17 Configuration Lock* on page 7-99
13	Set the safety password	Sysmac Studio*1	Configure the settings of the safety password for the Safety I/O Block.	*7-18 Setting the Safety Password* on page 7-104
14	Back up	Web UI	Create a backup file of the Safety I/O Block.	*7-19 Backup* on page 7-108

***1.** The settings can also be configured using the Web UI.


Standard controller
Safety controller
9. Configure
(When a Type1 Safety Open connection is established between the safety controller and Safety I/O Block, the Safety I/O Block is configured by the safety controller)
9. Configure
(Download a project file of Sysmac Studio to the safety controller and standard controller)
5. Set the IP address
7. Restart
8. Set the TUNID
10. Set automatic clock adjustment
12. Lock the configuration
13. Set the safety password
Ethernet switch
Sysmac Studio
1. Set the CIP Safety communications
2. Set the EtherNet/IP communications
3. Set the Safety application
4. Set the safety I/O functions
6. Select the Safety Application
Web UI
14. Back up
Safety I/O Block

7-1-2 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI)

The following shows the setting procedure of the configuration for the safety controller to perform control (configuration using the Web UI).
The procedure before installation and wiring is as follows:

Step	Setting item		Support software to use	Description	Reference
1	Create the remote I/O mode safety application[*1]	Create the safety application file	Sysmac Studio	Create a project file for exporting a safety application file. Execute exporting of the safety application file with this project file. For this safety application file, define only the I/O configuration settings.	*7-9 Create the safety application file* on page 7-65
2	Create a project file for a safety program of the safety controller[*1]	Set the CIP Safety communications	Sysmac Studio	Configure the settings for CIP Safety communications between a safety controller and Safety I/O Block in a project file of Sysmac Studio. For the open type, select **Check Safety Signature (Type2a)**.	*7-3 CIP Safety Communications Settings* on page 7-27
3		Set the EtherNet/IP communications	Sysmac Studio	Configure the settings for EtherNet/IP communications between a standard controller and Safety I/O Block in a project file of Sysmac Studio.	*7-4 EtherNet/IP Communications Settings* on page 7-38
4		Set the safety application	Sysmac Studio	Configure the safety application settings in a project file of Sysmac Studio. Select 00: Remote I/O mode.	*7-9-2 Safety Application Settings* on page 7-66
5		Set the safety signatures	Sysmac Studio	Configure the settings for the safety signatures in a project file of Sysmac Studio. Enter the SCCRC and SCTS recorded in *7-9-5 Exporting a Safety Application File* on page 7-68.	*7-8 Setting the Safety Signatures* on page 7-63

***1.** Create separate project files for the export of the safety application file and for the safety program of the safety controller.

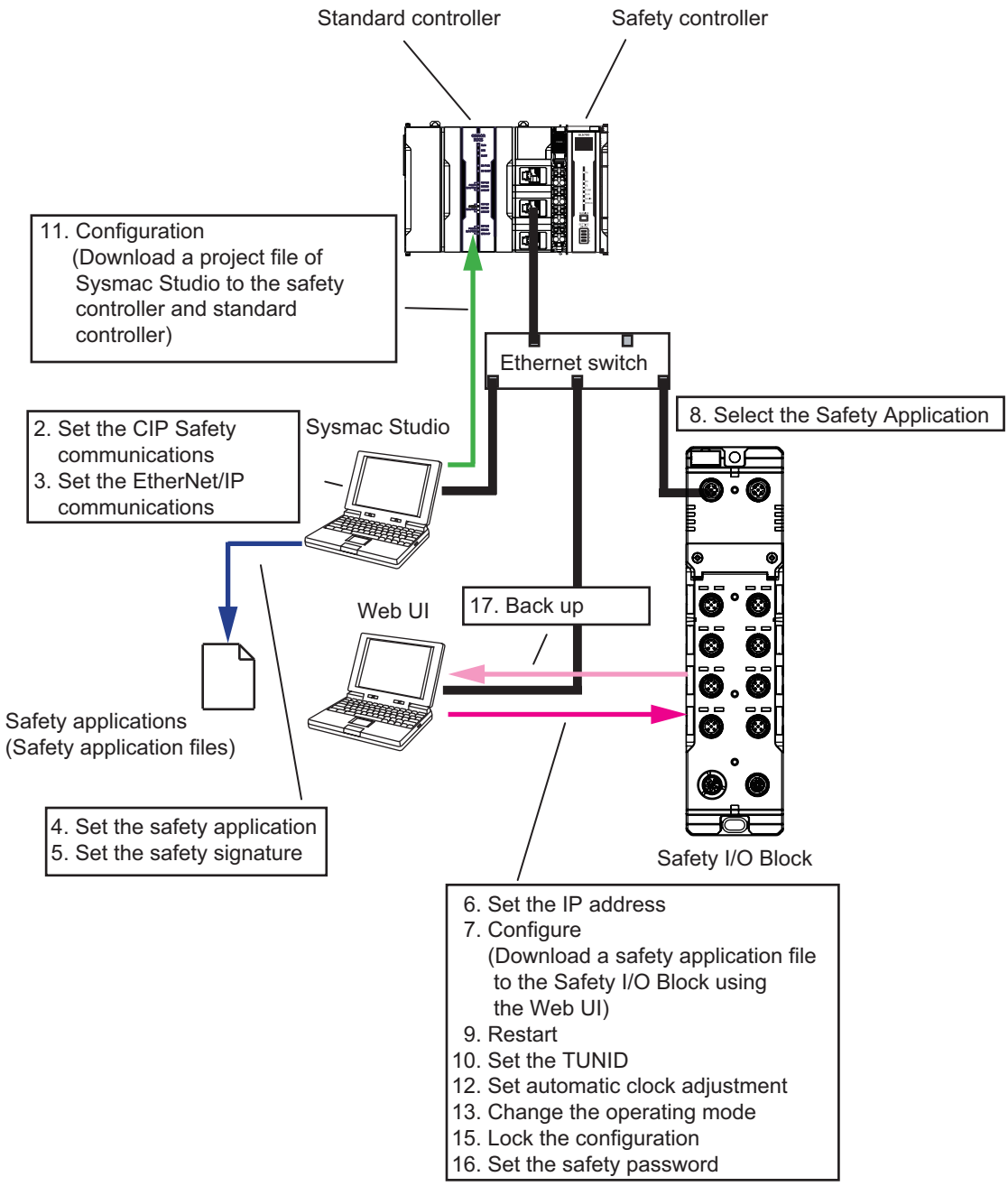
The procedure after installation and wiring is as follows:
To set the safety controller, use the project file for the safety program.

Step	Setting item	Support software to use	Description	Reference
6	Set IP address	Web UI[*1]	Configure the IP address settings of the Safety I/O Block.	*7-10 Setting IP Addresses* on page 7-71
7	Configure (Safety I/O Block side)	Web UI	Configure the Safety I/O Block by using the Web UI to download a safety application file to the Safety I/O Block. Use a safety application file for remote I/O mode. A safety application file for an add-on application cannot be used.	*7-14-2 Configuration of Safety I/O Block* on page 7-87
8	Select the safety application	-	Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to *0*.	*7-12 Selecting the Safety Application* on page 7-83

Step	Setting item	Support software to use	Description	Reference
9	Restart	Web UI*1	Restart the Safety I/O Block.	*7-13 Restart* on page 7-84
10	Set the TUNID	Web UI*1	Configure the TUNID settings of the Safety I/O Block.	*7-11 TUNID Settings* on page 7-78
11	Configure (safety controller and standard controller sides)	Sysmac Studio	Download a project file of Sysmac Studio and configure the safety controller and standard controller.	*7-14-1 Configuring the Safety Controller* on page 7-87
12	Set automatic clock adjustment	Web UI*1	Configure the settings for automatic clock adjustment of the Safety I/O Block.	*7-15 Setting the Automatic Clock Adjustment* on page 7-91
13	Change the operating mode*2	Web UI*1	Change the operating mode of the Safety I/O Block to *Executing*.	*7-16 Changing the Operating Mode* on page 7-95
14	Check the operation	-	Verify all I/O wiring and the operation of the program to check that the Safety I/O Block operates as intended.	-
15	Lock the configuration	Web UI*1	Execute safety validation of the safety control system to check that the setting values are correct. After the check, execute locking of the configuration. After executing locking of the configuration, setting values of the Safety I/O Block cannot be changed until the configuration is unlocked.	*7-17 Configuration Lock* on page 7-99
16	Set the safety password	Web UI*1	Configure the settings of the safety password for the Safety I/O Block.	*7-18 Setting the Safety Password* on page 7-104
17	Back up	Web UI	Create a backup file of the Safety I/O Block.	*7-19 Backup* on page 7-108

***1.** The settings can also be configured using Sysmac Studio.

***2.** This setting is required only when you set power-on mode to *Idle* in the settings of logic functions in step 4. This setting is not required when you set power-on mode to *Executing*.


Standard controller
Safety controller
11. Configuration
(Download a project file of Sysmac Studio to the safety controller and standard controller)
Ethernet switch
8. Select the Safety Application
2. Set the CIP Safety communications
3. Set the EtherNet/IP communications
Sysmac Studio
Web UI
17. Back up
Safety applications
(Safety application files)
4. Set the safety application
5. Set the safety signature
Safety I/O Block
6. Set the IP address
7. Configure
(Download a safety application file to the Safety I/O Block using the Web UI)
9. Restart
10. Set the TUNID
12. Set automatic clock adjustment
13. Change the operating mode
15. Lock the configuration
16. Set the safety password

7-1-3 Setting Procedure of Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application

The following shows the setting procedure of the configuration for the Safety I/O Block to perform control using a preset safety application.
The procedure before installation and wiring is as follows:

Step	Setting item	Support software to use	Description	Reference
1	Set the CIP Safety communications*1	Sysmac Studio	Configure the settings for CIP Safety communications between a safety controller and Safety I/O Block in a project file of Sysmac Studio. For the open type, select **Check Safety Signature (Type2a)**.	*7-3 CIP Safety Communications Settings* on page 7-27
2	Set the EtherNet/IP communications*2	Sysmac Studio	Configure the settings for EtherNet/IP communications between a standard controller and Safety I/O Block in a project file of Sysmac Studio.	*7-4 EtherNet/IP Communications Settings* on page 7-38
3	Set the safety application*1	Sysmac Studio	Configure the safety application settings in a project file of Sysmac Studio. Select the fixed application to use.	*7-9-2 Safety Application Settings* on page 7-66

***1.** When not using a safety controller, these settings are not required.
***2.** When not using a standard controller, these settings are not required.

The procedure after installation and wiring is as follows:

Step	Setting item	Support software to use	Description	Reference
4	Set the IP address*1	Web UI*2	Configure the IP address settings of the Safety I/O Block.	*7-10 Setting IP Addresses* on page 7-71
5	Set the TUNID	Web UI*2	Configure the TUNID settings of the Safety I/O Block.	*7-11 TUNID Settings* on page 7-78
6	Select the safety application	-	Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to one of the numbers *1-3* of the safety application (fixed application) to be used.	*7-12 Selecting the Safety Application* on page 7-83
7	Restart	Web UI*2	Restart the Safety I/O Block.	*7-13 Restart* on page 7-84
8	Configure*3	Sysmac Studio	Download a project file of Sysmac Studio and configure the safety controller and standard controller. Configuration of the Safety I/O Block is not required.	*7-14-1 Configuring the Safety Controller* on page 7-87
9	Set automatic clock adjustment	Web UI*2	Configure the settings for automatic clock adjustment of the Safety I/O Block.	*7-15 Setting the Automatic Clock Adjustment* on page 7-91
10	Check the operation	-	Verify all I/O wiring and the operation of the program to check that the Safety I/O Block operates as intended.	-
11	Lock the configuration	Web UI*2	Execute safety validation of the safety control system to check that the setting values are correct. After the check, execute locking of the configuration. After executing locking of the configuration, setting values of the Safety I/O Block cannot be changed until the configuration is unlocked.	*7-17 Configuration Lock* on page 7-99

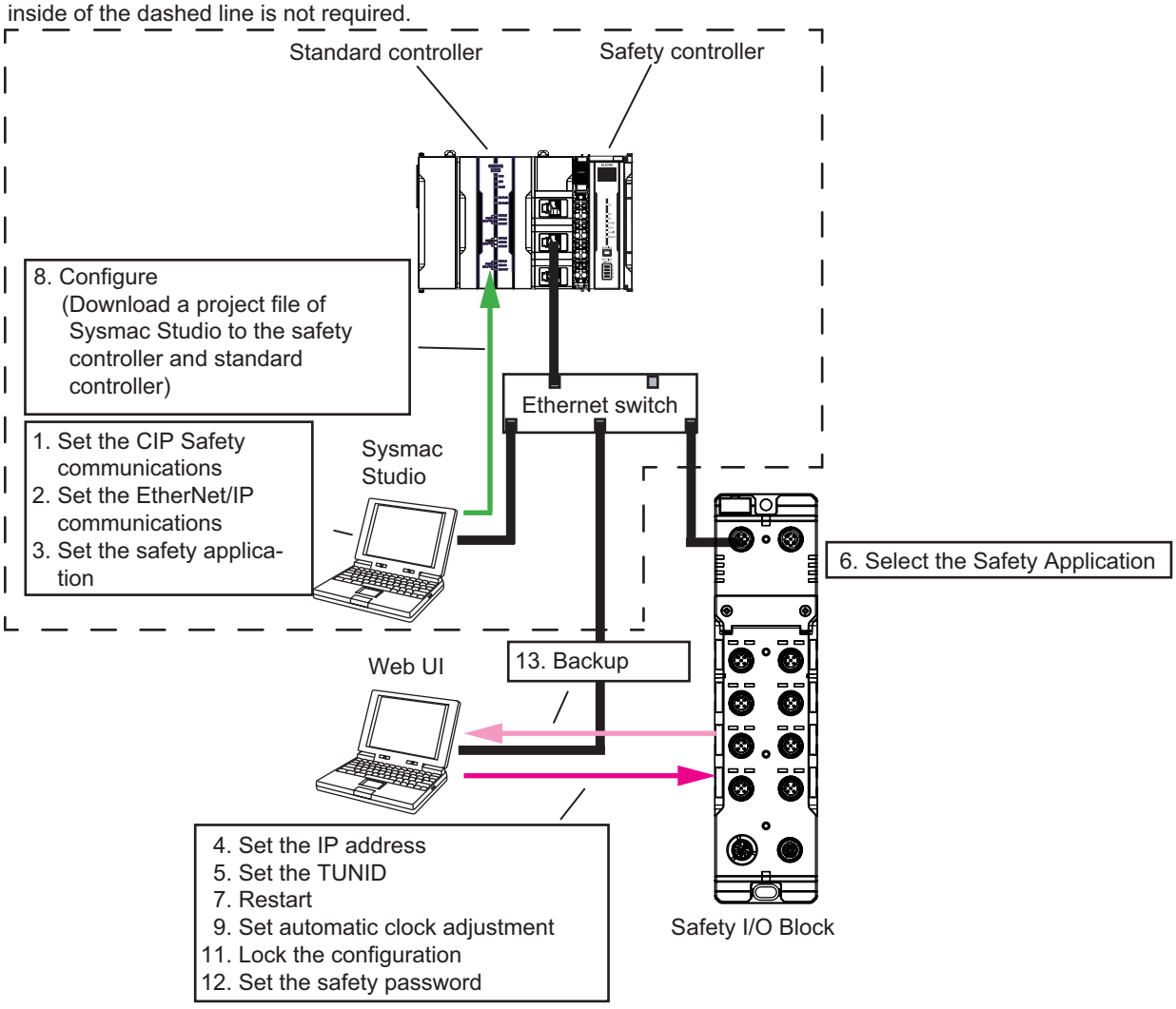
Step	Setting item	Support software to use	Description	Reference
12	Set the safety password	Web UI*2	Configure the settings of the safety password for the Safety I/O Block.	*7-18 Setting the Safety Password* on page 7-104
13	Backup	Web UI	Create a backup file of the Safety I/O Block.	*7-19 Backup* on page 7-108

***1.** When not using any of a safety controller and standard controller, these settings are not required. In this case, the Safety I/O Block will operate with the default IP address.

***2.** The settings can also be configured using Sysmac Studio.

***3.** When not using any of a safety controller and standard controller, these settings are not required.

When not using any of a safety controller and standard controller,
inside of the dashed line is not required.



7-1-4 Setting Procedure of Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User

The following shows the setting procedure of a configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user.
The procedure before installation and wiring is as follows:

Step	Setting item	Support software to use	Description	Reference
1	Set the CIP Safety communications	Sysmac Studio	Configure the settings for CIP Safety communications between a safety controller and Safety I/O Block in a project file of Sysmac Studio. For the open type, select **Configure Target Device (Type1)**.	*7-3 CIP Safety Communications Settings* on page 7-27
2	Set the EtherNet/IP communications*1	Sysmac Studio	Configure the settings for EtherNet/IP communications between a standard controller and Safety I/O Block in a project file of Sysmac Studio.	*7-4 EtherNet/IP Communications Settings* on page 7-38
3	Set the safety application	Sysmac Studio	Configure the safety application settings in a project file of Sysmac Studio. Select 15: User defined.	*7-9-2 Safety Application Settings* on page 7-66
4	Set the safety I/O functions	Sysmac Studio	Configure the I/O configuration settings for the Safety I/O Block in a project file of Sysmac Studio.	*7-5 Safety Input Functions Settings* on page 7-44 *7-6 Setting Safety Output Functions* on page 7-50
5	Set the logic functions	Sysmac Studio	Configure the settings for the logic and power-on mode of the Safety I/O Block in a project file of Sysmac Studio.	*7-7 Logic Function Settings* on page 7-53

***1.** When not using a standard controller, these settings are not required.

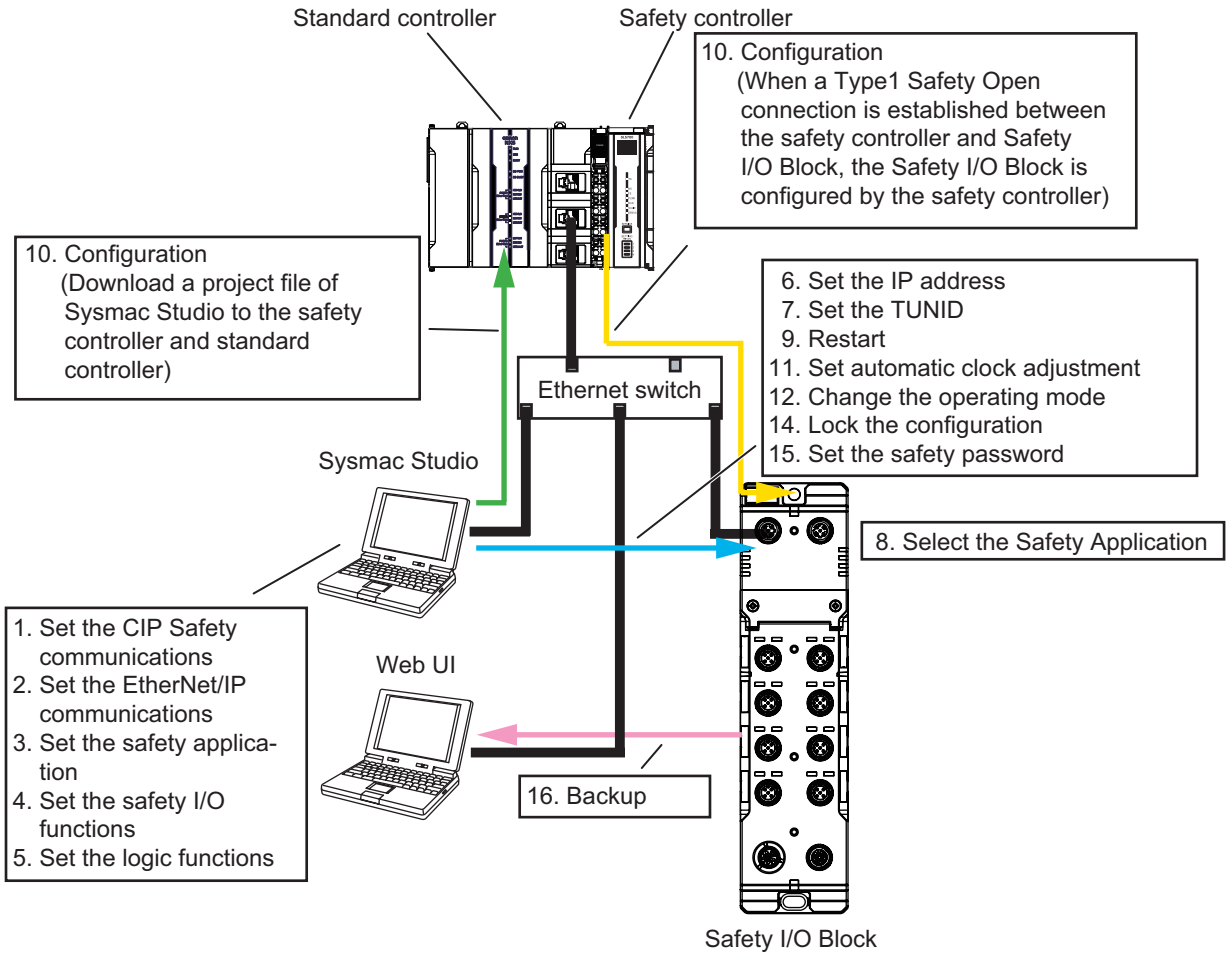
The procedure after installation and wiring is as follows:

Step	Setting item	Support software to use	Description	Reference
6	Set the IP address	Sysmac Studio*1	Configure the IP address settings of the Safety I/O Block.	*7-10 Setting IP Addresses* on page 7-71
7	Set the TUNID	Sysmac Studio*1	Configure the TUNID settings of the Safety I/O Block.	*7-11 TUNID Settings* on page 7-78
8	Select the safety application	-	Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to *F*.	*7-12 Selecting the Safety Application* on page 7-83
9	Restart	Sysmac Studio*1	Restart the Safety I/O Block.	*7-13 Restart* on page 7-84
10	Configuration	Sysmac Studio	Download a project file of Sysmac Studio and configure the safety controller and standard controller. The Safety I/O Block is configured by the safety controller when a Type1 Safety Open connection is established between the safety controller and the Safety I/O Block.	*7-14-1 Configuring the Safety Controller* on page 7-87

Step	Setting item	Support software to use	Description	Reference
11	Set automatic clock adjustment	Sysmac Studio*1	Configure the settings for automatic clock adjustment of the Safety I/O Block.	*7-15 Setting the Automatic Clock Adjustment* on page 7-91
12	Change the operating mode*2	Sysmac Studio*1	Change the operating mode of the Safety I/O Block to *Executing*.	*7-16 Changing the Operating Mode* on page 7-95
13	Check the operation	-	Verify all I/O wiring and the operation of the program to check that the Safety I/O Block operates as intended.	-
14	Lock the configuration	Sysmac Studio*1	Execute safety validation of the safety control system to check that the setting values are correct. After the check, execute locking of the configuration. After executing locking of the configuration, setting values of the Safety I/O Block cannot be changed until the configuration is unlocked.	*7-17 Configuration Lock* on page 7-99
15	Set the safety password	Sysmac Studio*1	Configure the settings of the safety password for the Safety I/O Block.	*7-18 Setting the Safety Password* on page 7-104
16	Backup	Web UI	Create a backup file of the Safety I/O Block.	*7-19 Backup* on page 7-108

***1.** The settings can also be configured using the Web UI.

***2.** This setting is required only when you set power-on mode to *Idle* in the settings of logic functions in step 4. This setting is not required when you set power-on mode to *Executing*.


Standard controller
Safety controller
10. Configuration
(When a Type1 Safety Open connection is established between the safety controller and Safety I/O Block, the Safety I/O Block is configured by the safety controller)
10. Configuration
(Download a project file of Sysmac Studio to the safety controller and standard controller)
6. Set the IP address
7. Set the TUNID
9. Restart
11. Set automatic clock adjustment
12. Change the operating mode
14. Lock the configuration
15. Set the safety password
Ethernet switch
Sysmac Studio
8. Select the Safety Application
1. Set the CIP Safety communications
2. Set the EtherNet/IP communications
3. Set the safety application
4. Set the safety I/O functions
5. Set the logic functions
Web UI
16. Backup
Safety I/O Block

7-1-5 Setting Procedure of Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User

The following shows the setting procedure of a configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user.
The procedure before installation and wiring is as follows:

Step	Setting item		Support software to use	Description	Reference
1	Create a safety application file for an add-on application*1	Export a safety application file	Sysmac Studio	Create a project file for exporting a safety application file. Execute exporting of the safety application with this project file. For this safety application file, define the logic settings and I/O configuration settings.	*7-9 Create the safety application file* on page 7-65
2	Create a project files for a safety program of the safety controller.*1	Set the CIP Safety communications*2	Sysmac Studio	Configure the settings for CIP Safety communications between a safety controller and Safety I/O Block in a project file of Sysmac Studio. For the open type, select **Check Safety Signature (Type2a)**.	*7-3 CIP Safety Communications Settings* on page 7-27
3		Set the EtherNet/IP communications*3	Sysmac Studio	Configure the settings for EtherNet/IP communications between a standard controller and Safety I/O Block in a project file of Sysmac Studio.	*7-4 EtherNet/IP Communications Settings* on page 7-38
4		Set the safety application*2	Sysmac Studio	Configure the safety application settings in a project file of Sysmac Studio. Select the add-on application to use.	*7-9-2 Safety Application Settings* on page 7-66
5		Set the safety signatures*2	Sysmac Studio	Configure the settings for the safety signatures in a project file of Sysmac Studio. Enter the SCCRC and SCTS recorded in “Export a safety application file.”	*7-8 Setting the Safety Signatures* on page 7-63

***1.** Create separate project files for the export of the safety application file and for the safety program of the safety controller.
***2.** When not using a safety controller, these settings are not required.
***3.** When not using a standard controller, these settings are not required.

The procedure after installation and wiring is as follows:
To set the safety controller, use the project file for the safety program.

Step	Setting item	Support software to use	Description	Reference
6	Set the IP address*1	Web UI*2	Configure the IP address settings of the Safety I/O Block.	*7-10 Setting IP Addresses* on page 7-71
7	Set the TUNID	Web UI*2	Configure the TUNID settings of the Safety I/O Block.	*7-11 TUNID Settings* on page 7-78

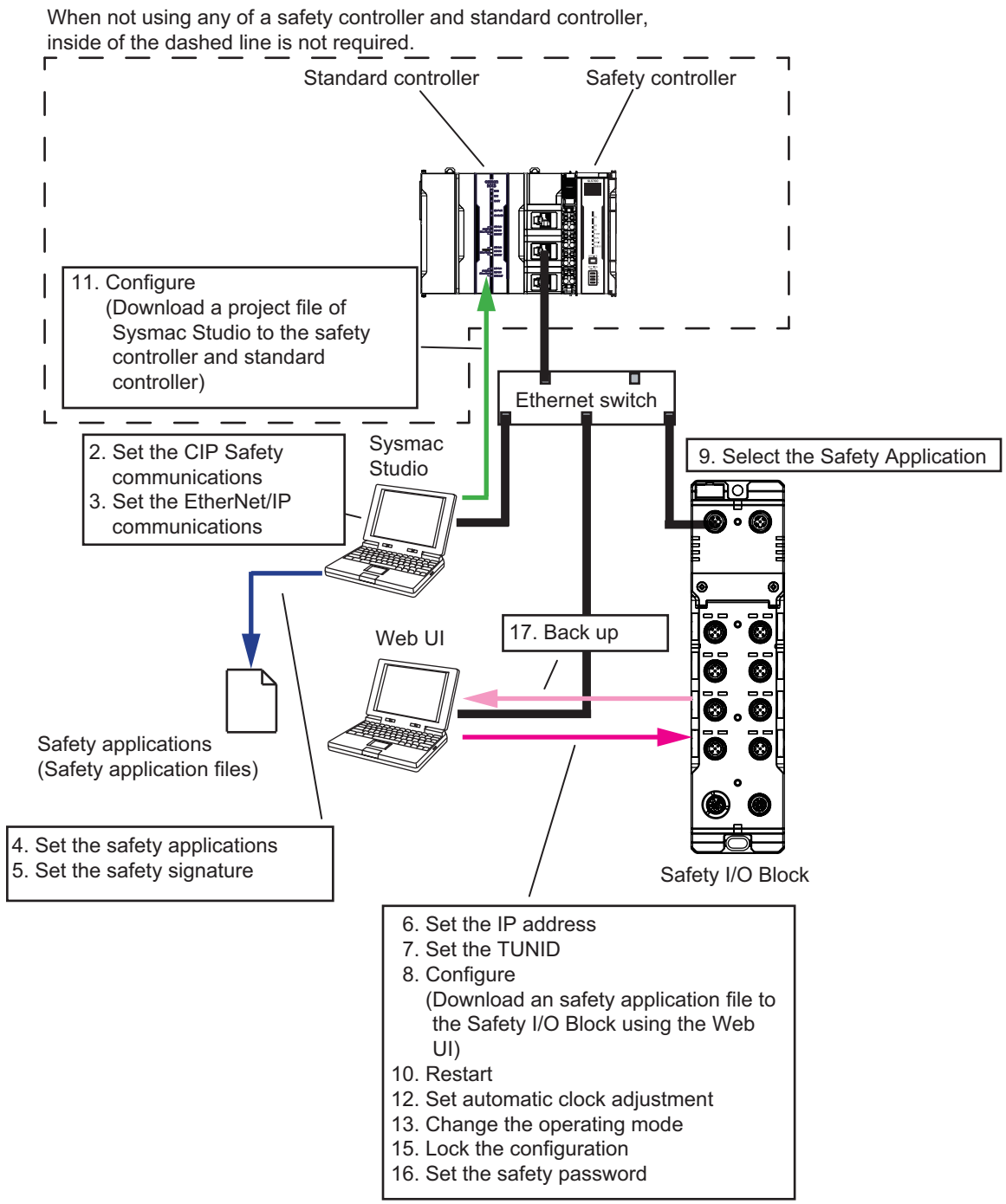
Step	Setting item	Support software to use	Description	Reference
8	Configure (Safety I/O Block side)	Web UI	Configure the Safety I/O Block by using the Web UI to download a safety application file to the Safety I/O Block. Use a safety application file for an add-on application. A safety application file for remote I/O mode cannot be used.	*7-14-2 Configuration of Safety I/O Block* on page 7-87
9	Select the safety application	-	Set both SETTING rotary switches SW1 and SW2 of the Safety I/O Block to number *9-D* of the safety application (add-on application) to be used.	*7-12 Selecting the Safety Application* on page 7-83
10	Restart	Web UI*2	Restart the Safety I/O Block.	*7-13 Restart* on page 7-84
11	Configure (safety controller and standard controller sides)*3	Sysmac Studio	Download a project file of Sysmac Studio and configure the safety controller and standard controller.	*7-14-1 Configuring the Safety Controller* on page 7-87
12	Set automatic clock adjustment	Web UI*2	Configure the settings for automatic clock adjustment of the .	*7-15 Setting the Automatic Clock Adjustment* on page 7-91
13	Change the operating mode*4	Web UI*2	Change the operating mode of the to *Executing*.	*7-16 Changing the Operating Mode* on page 7-95
14	Check the operation	-	Verify all I/O wiring and the operation of the program to check that the Safety I/O Block operates as intended.	-
15	Lock the configuration	Web UI*2	Execute safety validation of the safety control system to check that the setting values are correct. After the check, execute locking of the configuration. After executing locking of the configuration, setting values of the Safety I/O Block cannot be changed until the configuration is unlocked.	*7-17 Configuration Lock* on page 7-99
16	Set the safety password	Web UI*2	Configure the settings of the safety password for the Safety I/O Block.	*7-18 Setting the Safety Password* on page 7-104
17	Back up	Web UI	Create a backup file of the Safety I/O Block.	*7-19 Backup* on page 7-108

***1.** When not using any of a safety controller and standard controller, these settings are not required. In this case, the Safety I/O Block will operate with the default IP address.

***2.** The settings can also be configured using Sysmac Studio.

***3.** When not using any of a safety controller and standard controller, these settings are not required.

***4.** This setting is required only when you set power-on mode to *Idle* in the settings of logic functions in step 4. This setting is not required when you set power-on mode to *Executing*.


When not using any of a safety controller and standard controller, inside of the dashed line is not required.
Standard controller
Safety controller
11. Configure (Download a project file of Sysmac Studio to the safety controller and standard controller)
Ethernet switch
2. Set the CIP Safety communications
3. Set the EtherNet/IP communications
Sysmac Studio
9. Select the Safety Application
Web UI
17. Back up
Safety applications (Safety application files)
4. Set the safety applications
5. Set the safety signature
Safety I/O Block
6. Set the IP address
7. Set the TUNID
8. Configure (Download an safety application file to the Safety I/O Block using the Web UI)
10. Restart
12. Set automatic clock adjustment
13. Change the operating mode
15. Lock the configuration
16. Set the safety password

7-2 Overview of the Web UI

This section describes the overall content of the Web UI used for configuration, as well as the content common to each screen.

7-2-1 Various Specifications of the Web UI

The following table shows the various specifications of the Web UI.

Item	Specifications
Number of users who can log in simultaneously	Observers and administrators combined: 1
Local port number	443
Supported Languages	Japanese (ja) and English (en-US)
Supported character code	UTF-8
Authorities	Administrator and observer
Supported protocol	HTTPS
Supported browsers	Edge (PC version) and Chrome (PC version)
Session timeout time	10 minutes with no access
TLS version	TLS 1.2 is supported. TLS 1.0, TLS 1.1, and SSL are not supported.

7-2-2 Operation Authorities of the Web UI

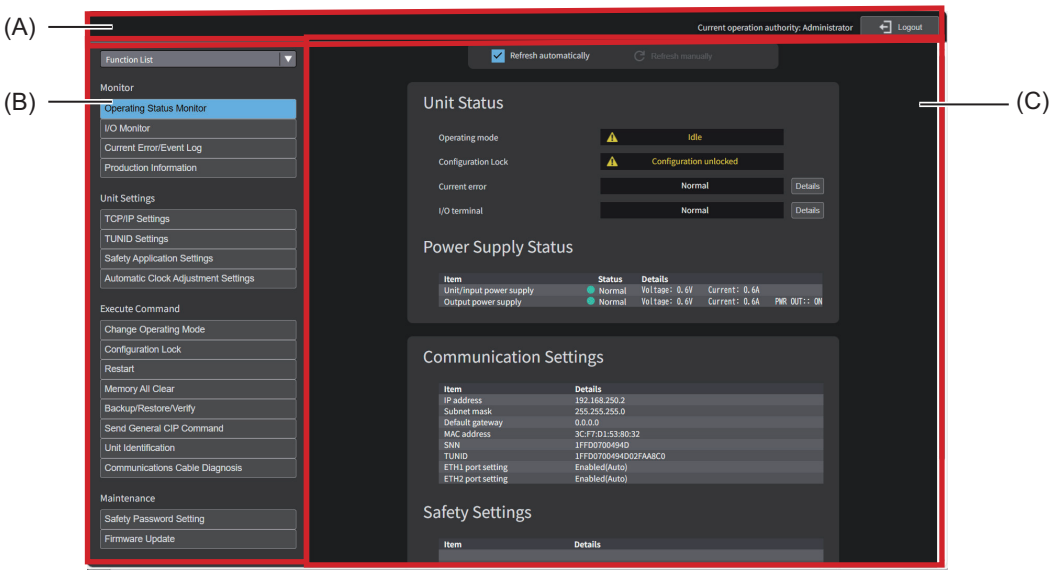
The Web UI has two operation authorities: *administrator* and *observer*.
The following table shows what each of the *administrator* and *observer* can do, and whether safety password authentication is required. The safety password is required to configure settings related to the safety of the Safety I/O Block. You can also use the Web UI to set the safety password.

Operation authority	What can do	Safety password authentication
Administrator	Reading, setting, and modifying various information and executing various commands	Required
Observer	Reading various information	Not required

Refer to *7-2-4 Main Menu List* on page 7-18 for the relationship between the various screens of the Web UI and whether use is possible as an *observer* or *administrator*.
To change the operation authority, log out from the Web UI and then log in again with the new operation authority.

7-2-3 Screen Configuration of Web UI

The following shows the screen configuration of the Web UI.



Letter	Name	Description
(A)	Common menu	Menu that is configured commonly across all main menus, regardless of the selected operation menu The **Current operation authority** field displays the authority of the logged in operator. Pressing the **Logout** button displays the Logout screen to enable you to log out.
(B)	Operation menus	Menus to select the main menu
(C)	Main menu	Menu to set the specific settings of the selected operation menu

There is a screen with the **Refresh automatically** check box and **Refresh manually** button at the top of the main menu. These controls allow you to set the timing to refresh the screen. They have the following meaning.

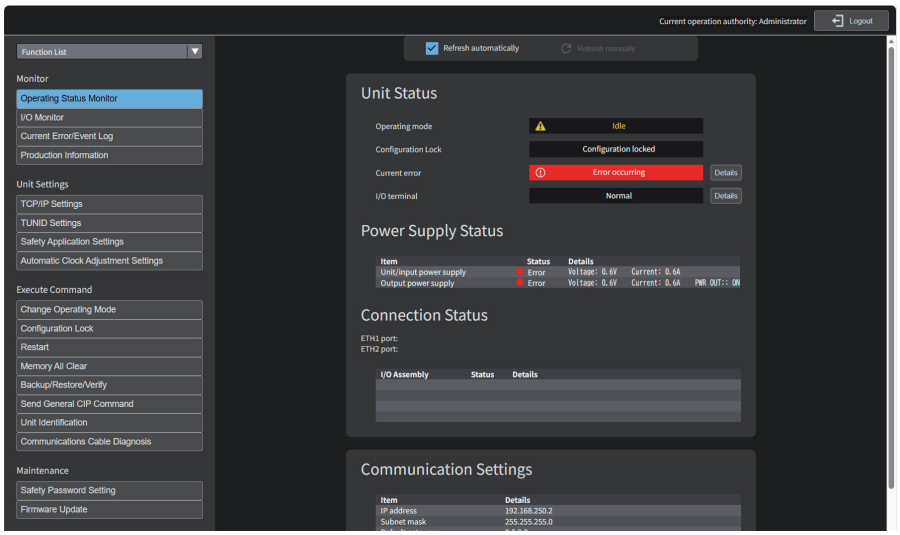
Item	Description
Refresh automatically	When this check box is selected, the screen is refreshed automatically at 1-second intervals. Default: Selected
Refresh manually	When this button is clicked, the screen is refreshed. This button is available only when the **Refresh automatically** check box is not selected.

7-2-4 Main Menu List

The main menu contains Function List and Replace Unit as shown below.
Switch between Function List and Replace Unit with the pull-down menu at the very top of the operation menu.

Menu command	Description
Function List	Used for various settings and monitoring of the Safety I/O Block.
Replace Unit	Used when replacing the Unit. This contains a collection of only the functions in Function List that are required for Unit replacement.

List of Functions

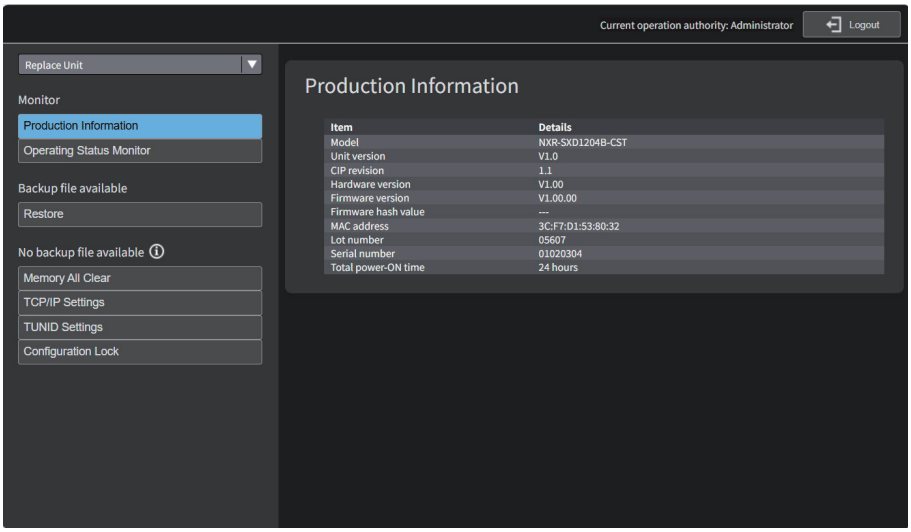


Function List includes the following items. The following table shows the overview, whether use is possible as an observer, and reference for each item.

Group of main menu	Screen name of main menu	Description	Whether use is possible as an observer	Reference
Monitor	Operating Status Monitor	Display the Unit status, power supply status, and other statuses of the corresponding Unit.	Possible	*11-1-3 Operating Status Monitor Function* on page 11-3
	I/O Monitor	Display the value of each I/O terminal of the corresponding Unit.	Possible	*8-11 I/O Monitor Function* on page 8-27
	Current Error/ Event Log	Display the current error and event logs of the corresponding Unit. Also, enable saving and clearing of the event log.	Possible	*11-2 Checking for Errors and Troubleshooting with the Event* on page 11-6
	Production information	Display the Unit version and other production information for the corresponding Unit.	Possible	*Production Information Screen* on page 33
Unit Settings	TCP/IP Settings	Configure the IP address, subnet mask, default gateway, and LINK settings of the corresponding Unit.	Not possible	*7-10 Setting IP Addresses* on page 7-71
	TUNID Settings	Set the TUNID of the corresponding Unit.	Not possible	*7-11 TUNID Settings* on page 7-78
	Safety Application Settings	Assign or remove the safety applications that run on the corresponding Unit to/from the rotary switch numbers.	Not possible	*7-14 Configuration* on page 7-87
	Automatic Clock Adjustment Settings	Adjust the time of the corresponding Unit.	Not possible	*7-15 Setting the Automatic Clock Adjustment* on page 7-91
Execute Command	Change Operating Mode	Set the operating mode to *Idle* or *Executing*.	Not possible	*7-16 Changing the Operating Mode* on page 7-95
	Configuration Lock	Execute locking and unlocking of the configuration.	Not possible	*7-17 Configuration Lock* on page 7-99
	Restart	Restart the corresponding Unit.	Not possible	*7-13 Restart* on page 7-84

Group of main menu	Screen name of main menu	Description	Whether use is possible as an observer	Reference
	Memory All Clear	Return all setting data of the corresponding Unit to the factory default settings.	Not possible	*8-2 Clear All Memory Function* on page 8-4
	Backup/Restore/Verify	Back up, restore, and verify the setting data of the corresponding Unit.	Not possible	*7-19 Backup* on page 7-108
	Send General CIP Command	Issue a CIP message command to the corresponding Unit without using a dedicated tool and display the execution results.	Not possible	*8-7 Send General CIP Command Function* on page 8-15
	Unit Identification	Light the Unit identification indicator of the corresponding Unit.	Not possible	*8-8 Unit Identification Function* on page 8-16
	Communications Cable Diagnosis	Check whether the communications cables are broken or short-circuited.	Not possible	*8-13 Communications Cable Diagnosis Function* on page 8-31
Maintenance	Safety Password Setting	Set the safety password for the Web UI of the corresponding Unit.	Not possible	*7-18 Setting the Safety Password* on page 7-104
	Update Firmware	Update the firmware of the corresponding Unit.	Not possible	*8-14 Firmware Update Function* on page 8-35

Replacing Units



Replace Unit includes the following items. The overview, whether use is possible as an observer, and reference for each item are the same as those in Function List.

Group of main menu	Screen name of main menu	Reference
Monitor	Production Information	*Production Information Screen* on page 33
	Operating Status Monitor	*11-1-3 Operating Status Monitor Function* on page 11-3
When there is a backup file	Restore*1	*7-19 Backup* on page 7-108
When there is no backup file	Memory All Clear	*8-2 Clear All Memory Function* on page 8-4
	TCP/IP Settings	*7-10 Setting IP Addresses* on page 7-71
	TUNID Settings	*7-11 TUNID Settings* on page 7-78
	Configuration Lock	*7-17 Configuration Lock* on page 7-99

***1.** From the Backup/Restore/Verify screen of Function List, only the restore function has been extracted.

7-2-5 Web UI Startup Procedure

There are two ways to start up the Web UI.

- Method to enter the IP address of the Safety I/O Block in the Web browser of the PC
- Method to enter the domain name with the IP address of the Safety I/O Block assigned in the Web browser of the PC

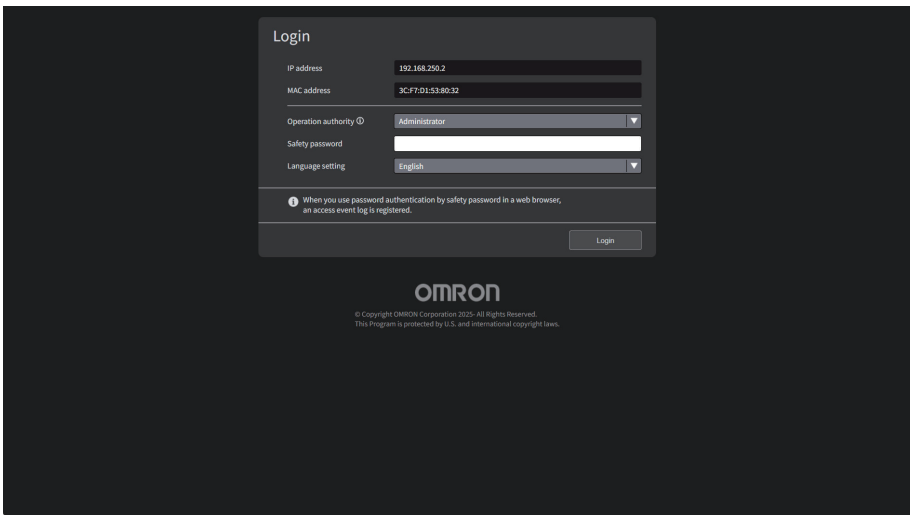
Method to Enter an IP Address

This section describes the procedure for the method to enter an IP address of the Safety I/O Block in the Web browser of the PC.

1 Use an Ethernet cable to connect the EtherNet/IP port of the Safety I/O Block and the Ethernet port of the PC.

2 Start the Web browser of the PC.

3 Enter the IP address of the Safety I/O Block in the Web browser. For example, if the IP address of Safety I/O Block is 192.168.250.1, enter *https://192.168.250.1/*.
The Web UI starts up and the following Login screen is displayed in the Web browser.



Precautions for Correct Use

When using the method to enter the IP address of the Safety I/O Block in the Web browser of the PC, there is the following security risk. If an unauthorized device intervenes between the PC and the Safety I/O Block on the network, information such as the safety password may be leaked by the unauthorized device. Therefore, take security measures such as the following:

- Use a firewall or similar measure to prevent access to the Safety I/O Block from outside the production area.
- Prevent entry by an unauthorized third party to the production area through access control or other means.
- Prevent an unauthorized device from intercepting communications between the PC and the Safety I/O Block by a method such as directly connecting the PC and the Safety I/O Block.

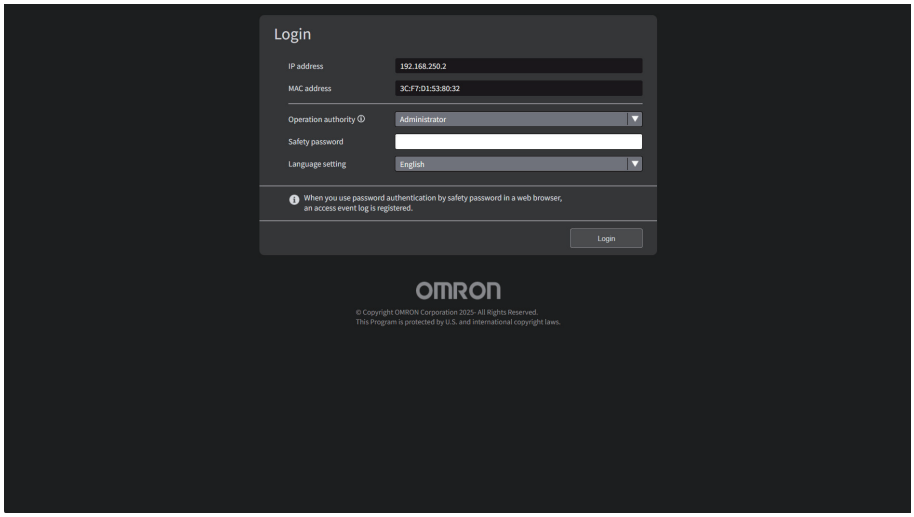
Method to Enter Domain Name

This section describes the procedure for the method to enter the domain name with the IP address of the Safety I/O Block assigned in the Web browser of the PC. Since encryption of the communications data and authentication by server certificate are performed, the security risk for this method is lower than that for the method to enter the IP address.
To use the method to enter the domain name, you need to configure the settings for using the HTTPS communications function on the PC in advance. Refer to *8-3 HTTPS Communications Function* on page 8-8 for details on the HTTPS communications function. The settings for using the HTTPS communications function need to be configured only once on each PC. This section describes the procedure to start up the Web UI using a PC that has the settings to use the HTTPS communications function already configured.

1. Use an Ethernet cable to connect the EtherNet/IP port of the Safety I/O Block and the Ethernet port of the PC.

2. Start the Web browser of the PC.

3. Enter the domain name assigned to the IP address of the Safety I/O Block in the Web browser. For example, if the domain name is *device1.NXR-SXD.local*, enter the following. *https://device1.NXR-SXD.local*
   The Web UI starts up and the following Login screen is displayed in the Web browser.

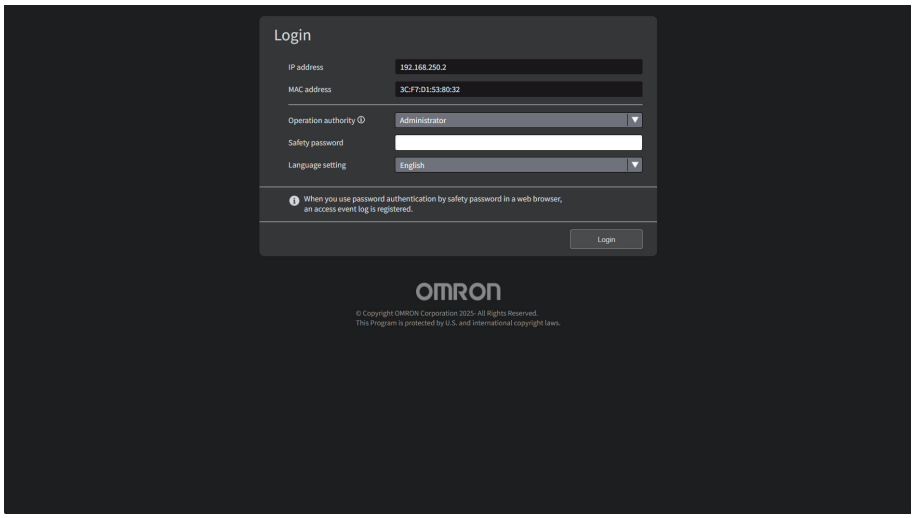


Precautions for Correct Use

When using the method to enter the domain name with the IP address of the Safety I/O Block assigned in the Web browser of the PC, observe the following precautions. If the IP address of the Safety I/O Block is changed without changing the settings of the domain name server, entering the domain name with the IP address assigned may result in accessing an unintended device. When changing the IP address of the Safety I/O Block, also change the settings of the domain name server. Furthermore, check that the MAC address displayed on the Login screen of the Web UI matches the MAC address of the intended Safety I/O Block.

7-2-6 Login

Enter the safety password to perform authority authentication and log in to the Web UI.



The safety password is not set at shipment from the factory.

If you enter the safety password 5 times incorrectly, you will be unable to log in for 10 minutes. The count for entering the safety password incorrectly is reset by any of a successful login, cycling of the power supply, or 10 minutes elapsing.

If there is no operation for at least 10 minutes after logging in, you will be required to re-enter the safety password to prevent unauthorized use by a third party without the administrator authority.

If a user exits the Web browser without logging out after login, the login state is retained for 10 minutes. Consequently, if the same user starts the Web browser from the same PC, the user can use the Web UI without performing the login operation. Another user cannot login during that period.

If a user turns OFF the power of the Safety I/O Block without logging out after login, the login state is discarded. Consequently, even if the same user starts the Web browser from the same PC, the user needs to log in to the Web UI again.

The **Safety password** field allows you to toggle between displaying and hiding the safety password.

Precautions for Correct Use

- Check that the MAC address displayed on the Login screen is the MAC address of the intended Unit before use. The MAC address of the Unit is written on the side of the Unit.
- To prevent unauthorized use by third parties, log out from the Safety I/O Block before interrupting operations via the Web UI and leaving your computer. In the Web UI, by selecting **Refresh automatically** on the Operating Status Monitor screen, I/O Monitor screen, Current Error screen and Event log screen, re-entry of the safety password is not required even after more than 10 minutes of inactivity.

Procedure for Using Login

The procedure to use login is as follows.

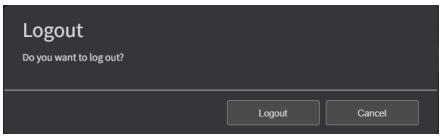
1. Check that the IP address of the corresponding Unit is displayed in the **IP address** field, and the MAC address of the corresponding Unit is displayed in the **MAC address** field.
2. Select **Administrator** or **Observer** in **Operation authority**.

3 Select **English** or **Japanese** in **Language settings**.
The language displayed in the Web UI is determined.

4 If you are an administrator, enter the safety password, and click the **Login** button. If you are an observer, you do not need to enter the safety password.
When you are logging in to the corresponding Unit for the first time as the administrator, the Change Initial Safety Password screen is displayed after login. Otherwise, the Operating Status Monitor screen is displayed after login.

7-2-7 Logout

Log out from the Web UI.
When you click the **Logout** button in the common menu, the Logout screen is displayed.



Procedure for Using Logout

Log out from the Web UI in the Logout screen. The setting procedure is as follows.

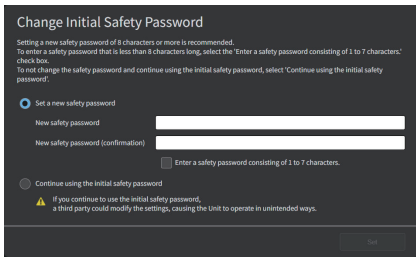
1 Click the **Logout** button.
Logging out is performed and the Login screen is displayed.

7-2-8 Precautions for Initial Login

The Change Initial Safety Password screen is displayed at initial login. To enhance security, be sure to change the safety password.

Change Initial Safety Password

The Change Initial Safety Password screen is used to change the safety password from the initial safety password at initial login. The screen is displayed immediately after the Login screen at initial login. If you set a new safety password or select the **Continue using the initial safety password** option, the screen is not displayed when logging in from the next time.
Refer to *7-18 Setting the Safety Password* on page 7-104 for details on the safety password authentication function.



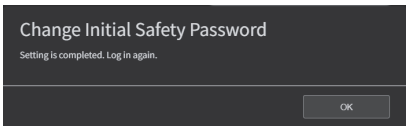
● Procedure for Using Change Initial Safety Password

The Change Initial Safety Password screen is used to change the safety password from the initial safety password. The usage procedure is as follows.

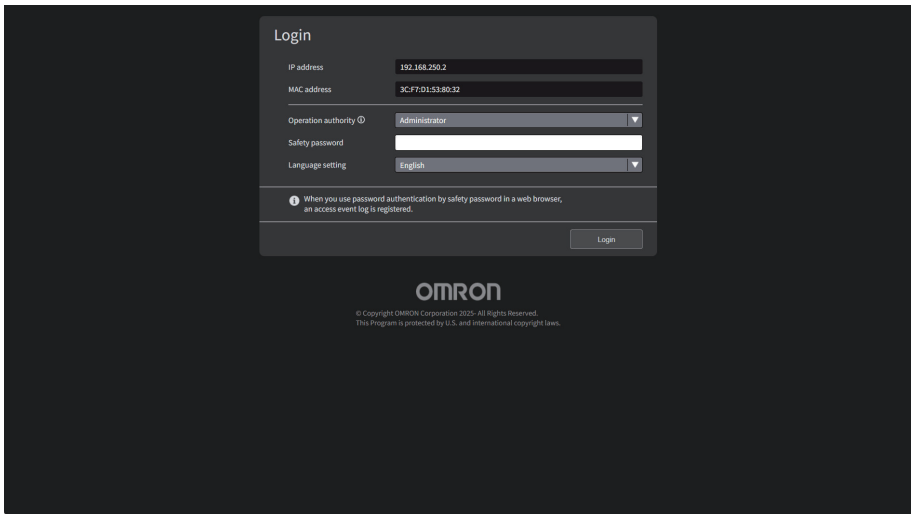
1 Select either the **Set a new safety password** or **Continue using the initial safety password** option.
If you select the **Continue using the initial safety password** option, the safety password cannot be changed. However, to improve the security, we recommend that you change the safety password.

2 If you select the **Set a new safety password** option, enter a new safety password in **New safety password** and **New safety password (confirmation)**.
To enhance the security, enter a safety password that is at least 8 characters long.
However, in special circumstances, such as when you wish to use the same password as another device, you can set a safety password that is 1 to 7 characters long if you select the **Enter a safety password consisting of 1 to 7 characters.** check box.

3 Click the **Set** button.
The safety password is set, and the following message is displayed.



4 Click the **OK** button.
The Login screen is displayed.



5 Enter the new safety password, and click the **Login** button.
The Operating Status Monitor screen is displayed.

7-3 CIP Safety Communications Settings

This section describes how to set the connection for CIP Safety communications using the Safety I/O Block of the CIP Safety originator and CIP Safety target.

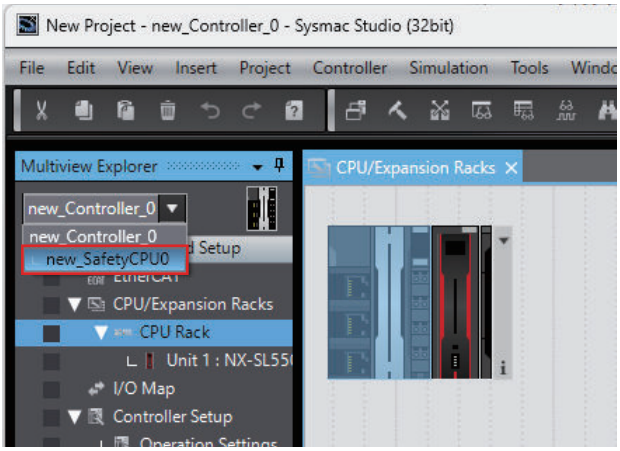
7-3-1 Connection Settings for CIP Safety Communications

This section describes how to configure the CIP Safety connection settings of the Safety I/O Block.

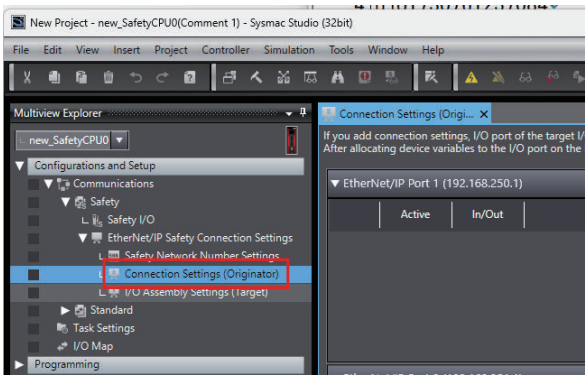
Connection Registration Procedure

This section describes the procedure to register a CIP Safety connection of the Safety I/O Block in Sysmac Studio using a Safety Network Controller as an example of a CIP Safety originator.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.



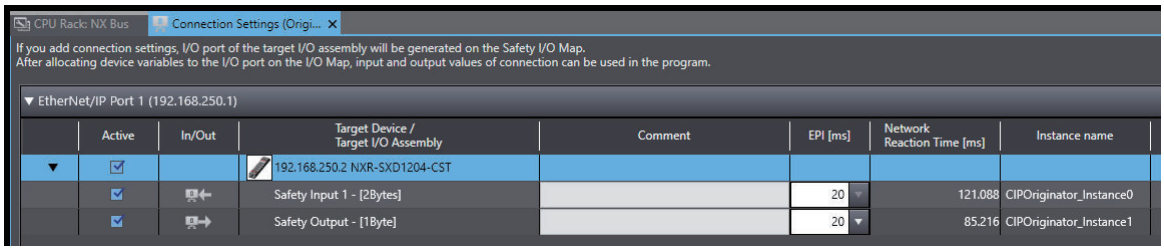
2 In Multiview Explorer, go to **Configurations and Setup** - **Communications** - **Safety** - **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**, or right-click it and select **Edit**.
The Connection Settings (Originator) Edit Pane is displayed on the Edit Pane.



3 Select **Safety I/O and Logic Device** from Toolbox, and select **NXR-SXD1204-CST** or **NXR-SXD1204B-CST**.



4 Drag the Safety I/O Block selected in Toolbox, and drop it on the Connection Settings (Originator) Edit Pane, or double-click the selected Safety I/O Block.



5 Set the IP address of the Safety I/O Block as necessary.
The IP address of the added connection is assigned automatically based on the IP addresses of the EtherNet/IP ports set on the Safety Network Controller. Edit the IP address according to the configuration of the network.
Refer to *Connection IP Address Setting Procedure* on page 7-28 for details on how to edit the IP address.

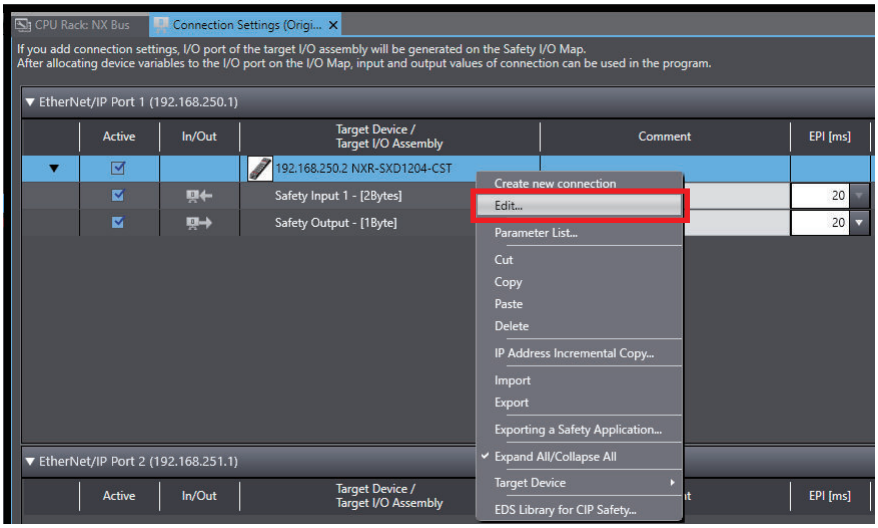
6 Change the I/O assemblies as necessary.
In the initial state, **Safety Input 1** and **Safety Output** are registered for the NXR-SXD1204-CST.
The same applies for the NXR-SXD1204B-CST.
Refer to *Procedure for Registering Additional Connections* on page 7-29 for how to change the I/O assemblies.

7 Edit the parameters of the registered connection.
Refer to *Connection Parameter Editing Procedure* on page 7-32 for how to edit the parameters of a connection.

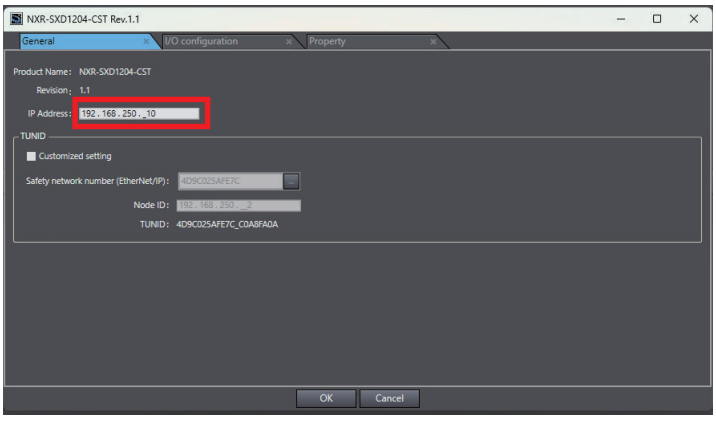
Connection IP Address Setting Procedure

This section describes the procedure to set the IP address of the Safety I/O Block as the IP address of the connection settings.

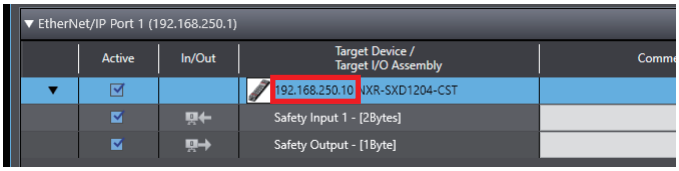
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane, then right-click it and select **Edit** from the menu.



2 Enter the IP address in the IP address field, and click the **OK** button.



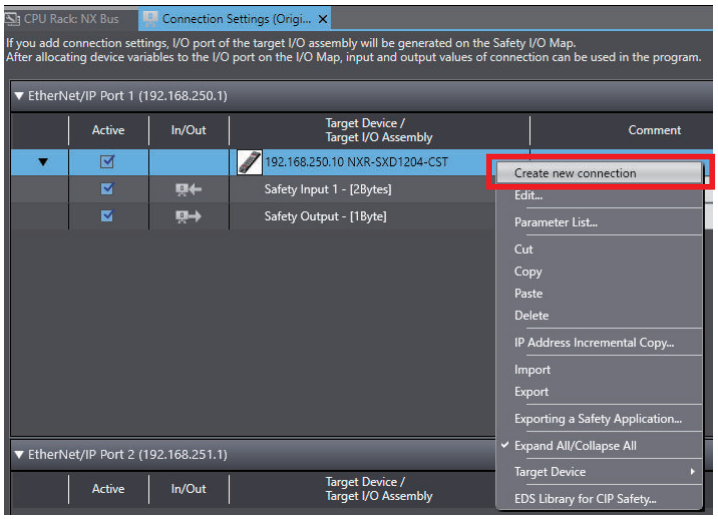
The entered IP address is reflected on the Connection Settings (Originator) Edit Pane.



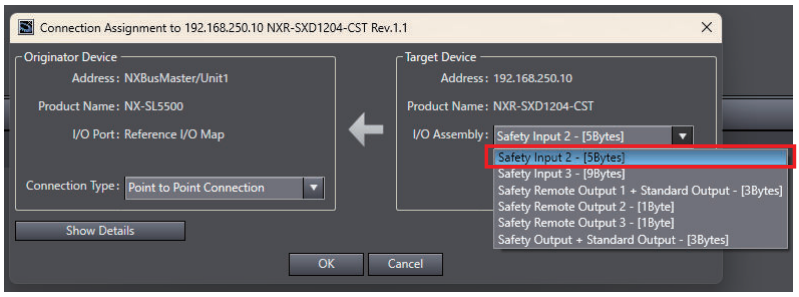
Procedure for Registering Additional Connections

The procedure to register an additional connection with the Safety I/O Block is described below.

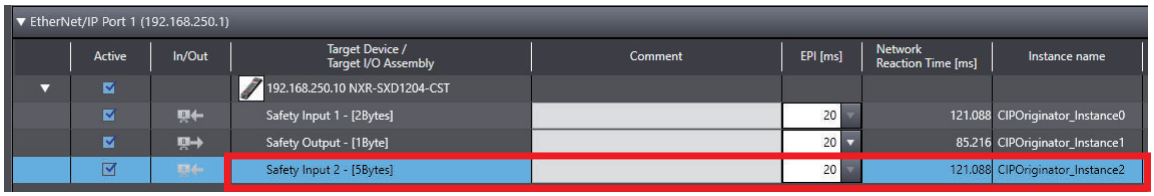
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane, and then right-click it and select **Create new connection**.



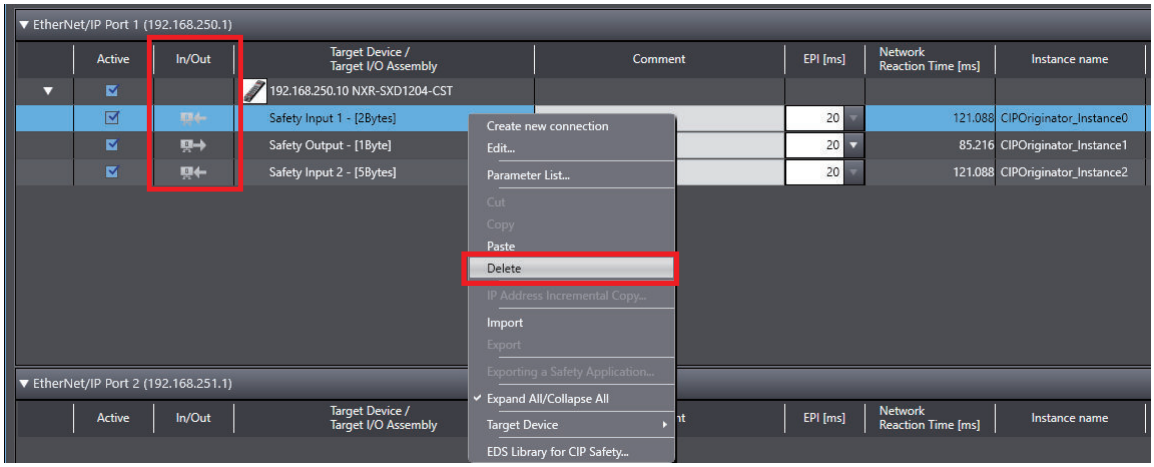
2 Select the item to add from the **I/O Assembly** pull-down list, and then click the **OK** button.

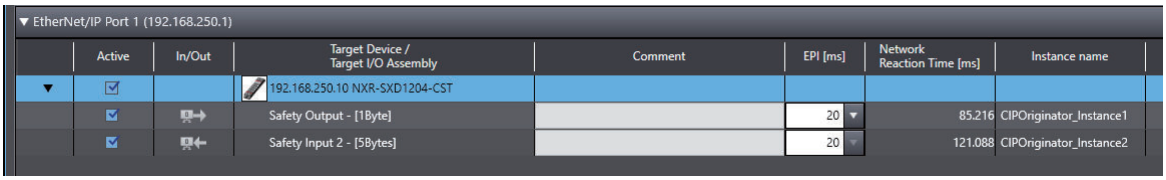


The added I/O assembly is displayed on the Connection Settings (Originator) Edit Pane.

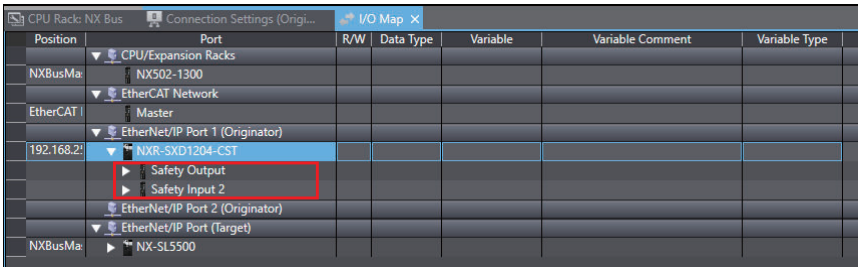


3 Select an I/O assembly you will not use, and then right-click it and select **Delete**.





The set I/O assemblies are reflected also on the I/O map automatically.



● Types and Restrictions of I/O Assemblies

The types and restrictions of registrable input assemblies and output assemblies for the Safety I/O Block are described below.

- Input assemblies

  An input assembly is data sent in the direction from Safety I/O Block to safety controller.

Assembly	Data size	Remarks
Safety Input 1	2byte	Value of safety input terminal + Status information of safety input terminals (aggregate) + Status information of safety output terminals (aggregate) + Output power supply error flag + Status information of connection
Safety Input 2	5byte	Value of safety input terminal + Status information of safety input terminal + Status information of safety input terminals (aggregate) + Status information of safety output terminals (aggregate) + Output power supply error flag + Status information of connection + Number of safety application
Safety Input 3	9byte	Value of safety input terminal + Status information of safety input terminal + Status information of safety output terminal + Value actually output to safety output terminal + Status information of test output terminal + Value of test output terminal + Status information of safety input terminals (aggregate) + Status information of safety output terminals (aggregate) + Output power supply error flag + Status information of connection + Number of safety application

- Output assemblies

  An output assembly is data sent in the direction from safety controller to Safety I/O Block.

Assembly	Data size	Remarks
Safety Output	1byte	ON/OFF to safety output terminal
Safety Output + Standard Output	3byte	ON/OFF to safety output terminal + ON/OFF of standby output to test output terminal
Safety Remote Output 1 + Standard Output	3byte	ON/OFF of remote output Ro 1 + ON/OFF of standby output to test output terminal
Safety Remote Output 2	1byte	ON/OFF of remote output Ro 2
Safety Remote Output 3	1byte	ON/OFF of remote output Ro 3

The settable output assemblies differ depending on the settings used for the safety application. The combinations of output assemblies are as follows.

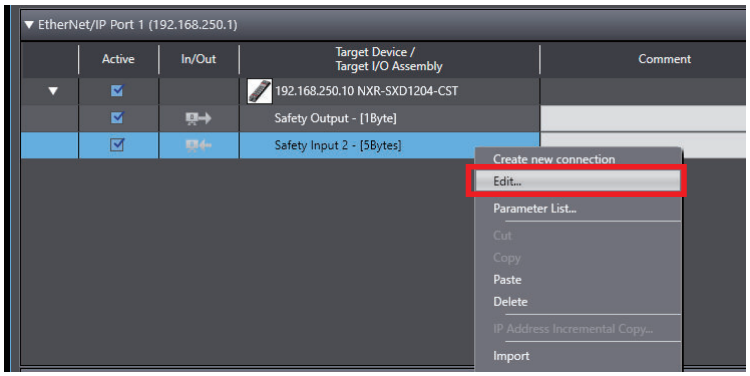
Sysmac Studio setting value of safety application and rotary switch settings	Combination of output assemblies
Safety application not used (When the setting value of the application is “00: Remote I/O mode” and rotary switches SW1 = SW2 = 0)	The following two types of assemblies can be used. • Safety Output • Safety Output + Standard Output However, it is not possible to establish connections for the two assemblies simultaneously.
Safety application used (When the setting value of the application is other than “00: Remote I/O mode” and rotary switches SW1 = SW2 = 1 to 3, 9 to 13, or 15)	The following three types of assemblies can be used. • Safety Remote Output 1 + Standard Output • Safety Remote Output 2 • Safety Remote Output 3

Refer to *A-3 I/O Assembly Ports and Corresponding Safety I/O Assembly Data Elements* on page A-14 for details on I/O assemblies.

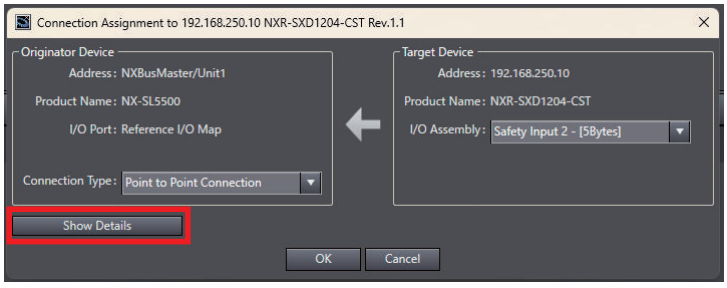
Connection Parameter Editing Procedure

Use the following procedure to edit the parameters for CIP Safety connections.

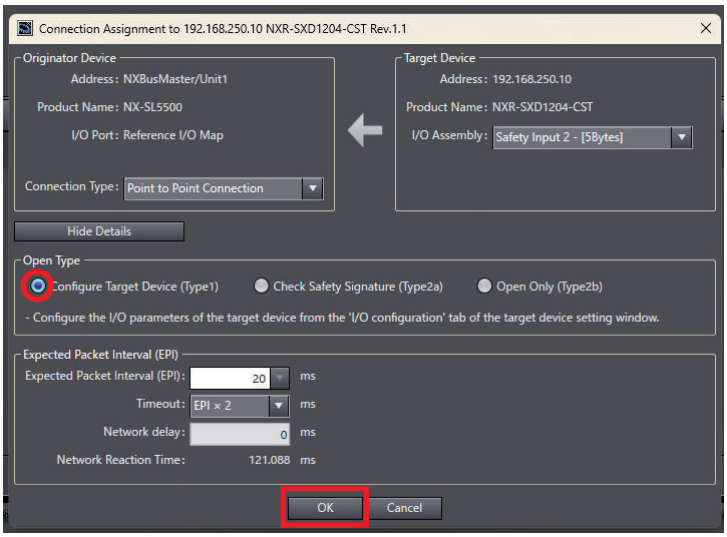
1 Select the connection of the Safety I/O Block on the Connection Settings (Originator) Edit Pane, then right-click it and select **Edit**.



2 Select **Detailed Display**.



3 Select **Configure Target Device** in the settings of **Open Type**, and click the **OK** button.



Item	Description
I/O Assembly	An I/O assembly is a unit of I/O data cyclically exchanged between a CIP Safety originator and CIP Safety target. Several I/O assemblies are defined and provided for the Safety I/O Block. Select from the defined I/O assemblies to register one I/O assembly per CIP Safety connection. I/O assemblies of target devices for which a CIP Safety connection can be opened are listed.
Connection Type	For the input connection (receiving from the target device), select either **Point to Point Connection** or **Multicast Connection**. The default setting is **Point to Point Connection**.
Open Type	Select a type for connection opening. • Configure Target Device (Type1) Configure the target devices after a connection is established. • Check Safety Signature (Type2a) Use the safety signature to check if the target devices are configured properly when establishing the connection. The safety signature consists of the Safety Configuration CRC and the Safety Configuration Time Stamp. • Open Only (Type2b) Configuration check of the target devices is not performed when establishing the connection. The default setting is **Configure Target Device (Type1)**.
Expected Packet Interval (EPI)	Set an interval for communications of safety process data between the originator and the target. The default setting is 20 (ms). Refer to *2-1-2 Communications Specifications* on page 2-3 for the setting range.
Timeout	Specify a timeout period for determining a communications error as a multiple of the EPI. The default setting is EPI x 2 (ms) (timeout is allowed just once). The setting range of the multiple is from 1 to 4.
Network Delay	Set the transmission delay time on the network. The default setting is 0 (ms).
Network Reaction Time	The value of connection response performance is displayed in ms. This is used in calculating the safety reaction time.

⚠ WARNING

If you set the open type to **Open Only**, make sure to verify that the originator and target have the correct configurations before use.
Serious injury may possibly occur due to loss of required safety functions.

Additional Information

The following provides a guideline for the minimum value of EPI in respect to number of registered connections. Note that when the connection type of the input is multicast, it is assumed that 8 originators are connected.

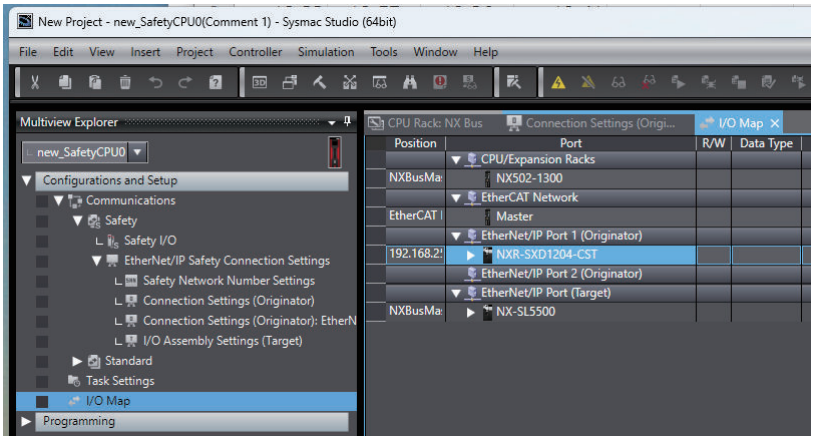
Number of connections	Minimum value of EPI
1 (1 input or 1 output)	5 ms
5 (2 inputs and 3 outputs)	20 ms

4 When setting is complete, click the **OK** button.

Registration Procedure for Device Variables

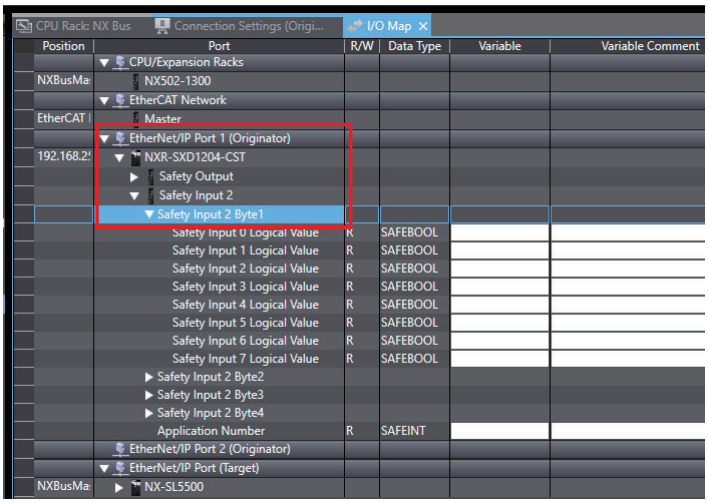
Device variables are used to access data in devices (Slaves, Units, and Safety I/O Block).
The Safety CPU Unit exchanges signals with external devices through logical interfaces that are called "I/O ports".
The following describes the procedure to register device variables for the I/O ports on the devices to make the values of the I/O on the devices available in the safety program in the Safety CPU Unit.
This is an example using the NXR-SXD1204-CST Safety I/O Block.

1 Select **Configurations and Setup** - **I/O Map** in the Multiview Explorer.

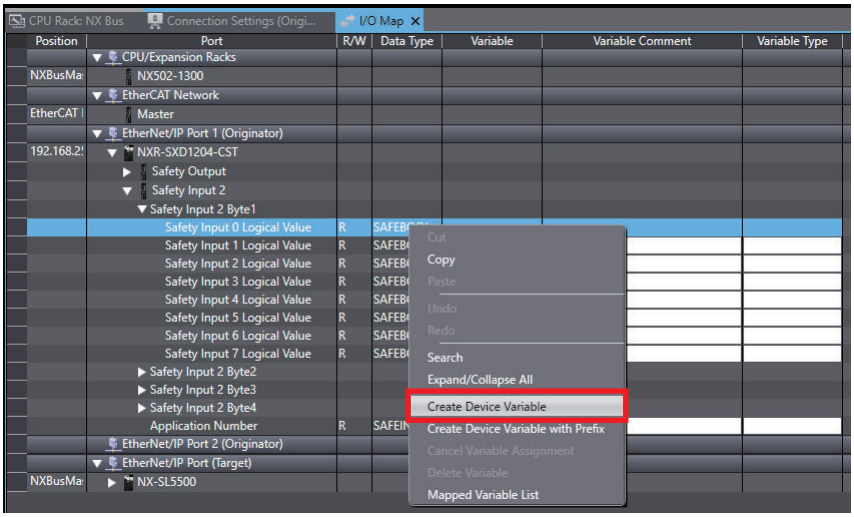


The I/O Map Edit Pane is displayed in the Edit Pane.

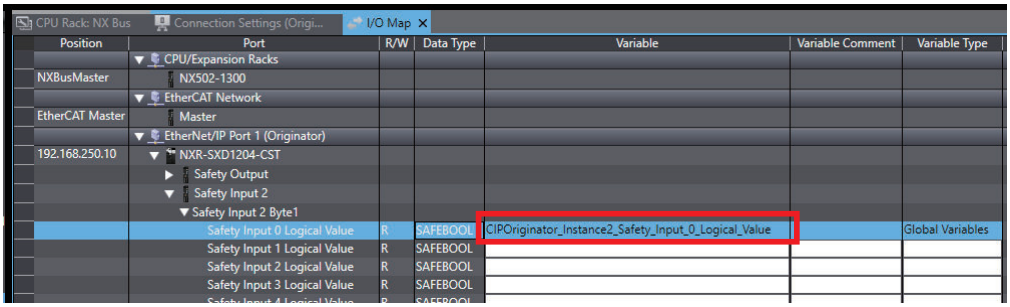
2 Open **EtherNet/IP Port 1 (Originator)** - **NXR-SXD1204-CST**–**Safety Input 2**–**Safety Input 2 Byte1** on the I/O Map Edit Pane.



3 Select an I/O port and directly enter a variable in the **Variable** column. Or, select the Safety I/O Block name or I/O port (multiple selectable), then right-click it and select **Create Device Variable**.
If you select **Create Device Variable**, the device variables are automatically named with the device name and port name.



The device variable is registered.



The device variables that you enter or automatically create are registered in the global variable table.

Additional Information

When registering a variable in advance, select the variable to assign to the I/O port from the pull-down list.

7-3-2 Exporting and Importing the Settings of the Safety I/O Block

You can export and import the settings of the Safety I/O Block as a single file (extension .tds) to reuse them.

This following data is processed:

- CPU Unit and connection settings
- IP address of the Safety I/O Block set with Sysmac Studio
- Settings of I/O functions of the Safety I/O Block

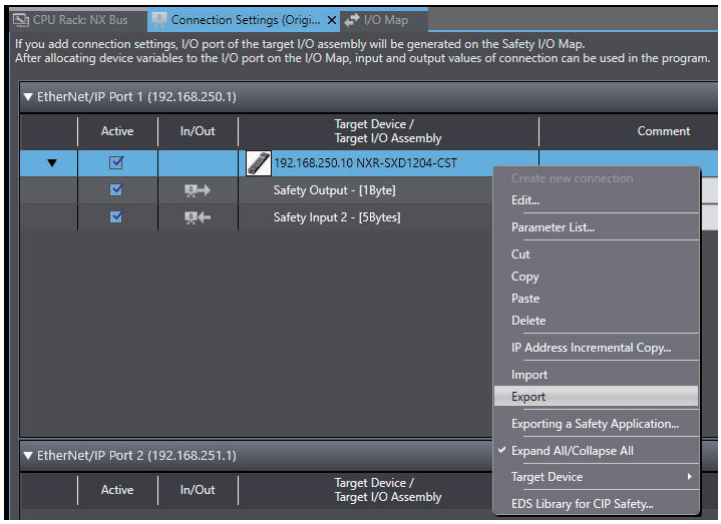
Additional Information

Refer to *7-19 Backup* on page 7-108 for backing up, verifying, and restoring using the Web UI.

How to Export Settings

The procedure to export the settings of the Safety I/O Block is as follows.

1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane, then right-click it and select **Export** from the menu.



The **Export** dialog box is displayed.

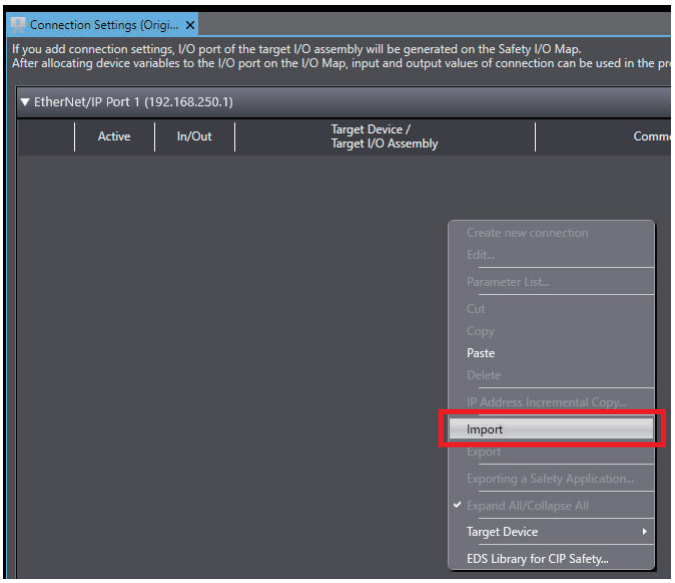
2 Select the save location, enter a file name, and click the **Save** button.

The configuration file of the Safety I/O Block is saved with the .tds extension in the specified save location.
The default file name is IP address␣Target device name.tds.

Procedure for Importing Settings

The procedure to import the settings of the Safety I/O Block is as follows.

1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane, then right-click it and select **Import** from the menu.



The **Import** dialog box is displayed.

2 Select the desired Safety I/O Block configuration file with the .tds extension, and click the **Open** button.

Precautions for Correct Use

The data integrity of the target device configuration file is not checked by CRC when it is imported.
It is your responsibility to verify that the settings are correct after the import, and sufficiently check the operation before switching to actual operation.

7-4 EtherNet/IP Communications Settings

This section describes how to set the connection for tag data link communications using the Safety I/O Block of the EtherNet/IP originator and EtherNet/IP target and how to set the LLDP function.

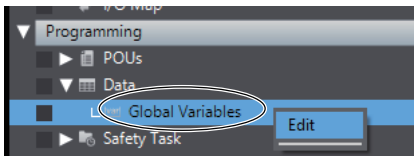
7-4-1 Setting Tag Data Link Communications

Set the connection for tag data link communications between the Safety I/O Block and originator.

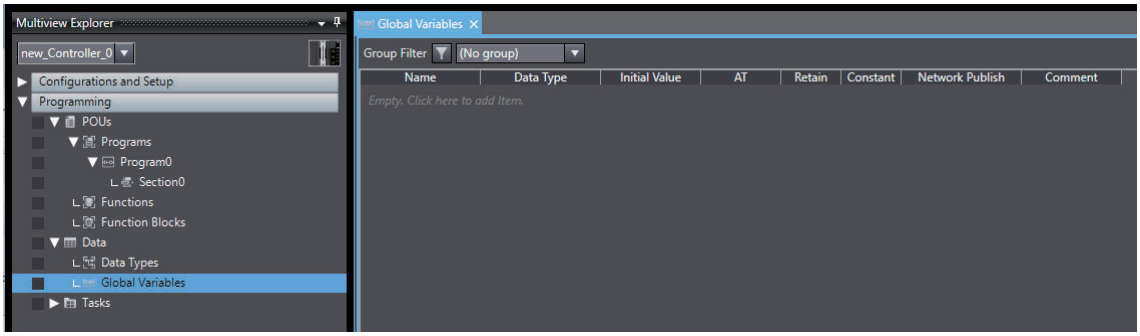
Setting Procedure for Tag Data Link Communications

This section describes the procedure to set the tag data link communications of the Safety I/O Block using Sysmac Studio.
The following procedure is an example of using the EtherNet/IP port built into the Standard Controller as the originator to set the input data (Assembly 960 to 3C0 hex) and size: 5 bytes in the I/O assembly data of the tag data link.

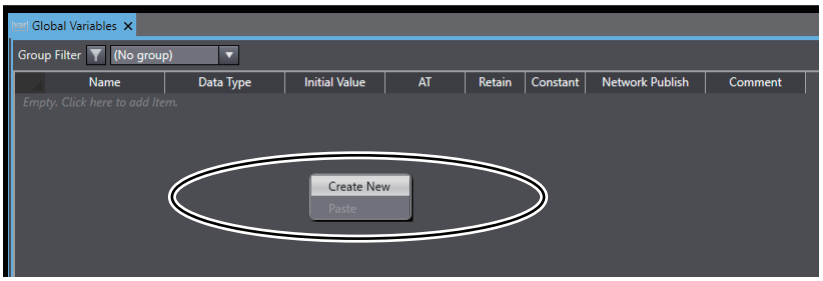
1 Double-click **Global Variables** under **Programming** - **Data** in the Multiview Explorer.
Or, right-click **Global Variables** under **Programming** - **Data** and select **Edit** from the menu.



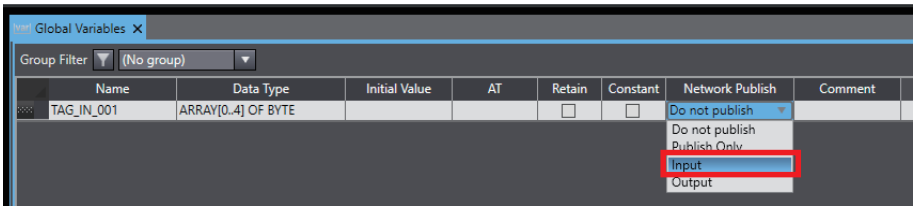
The global variable registration table is displayed.



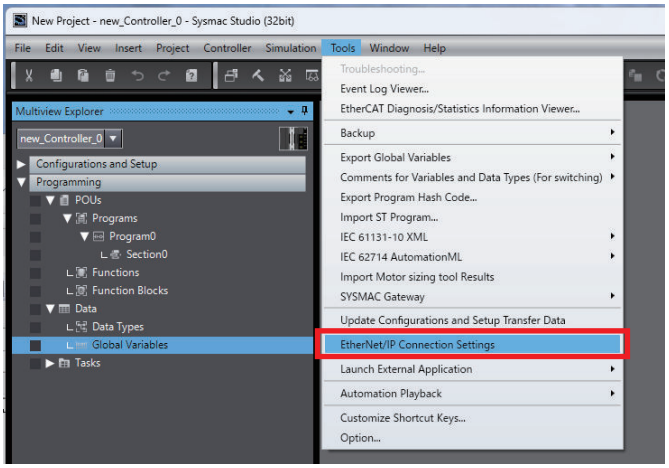
2 Press the **Insert** Key in the global variable table, or right-click in the global variable table and select **Create New** from the menu.



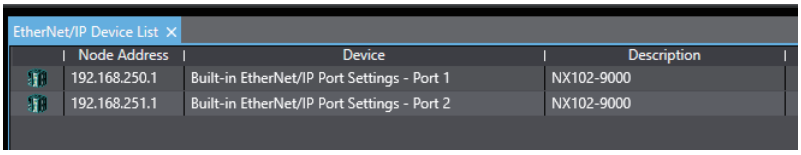
3 Register a variable of 5 bytes for the global variable, and set **Network Publish** to **Input**.



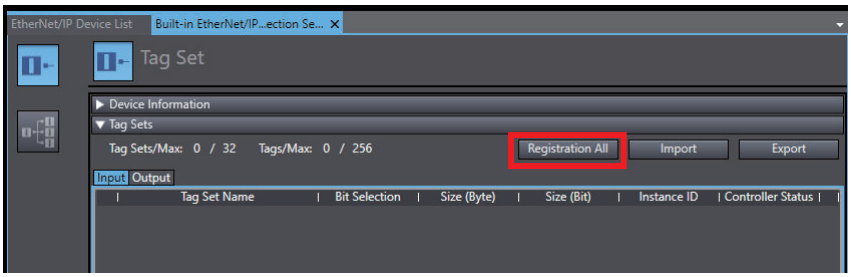
4 Select Standard PLC (Initial display new_Controller_0) in the Multiview Explorer, and select **EtherNet/IP Connection Settings** in the **Tools** menu from the menu bar at the top of the screen.



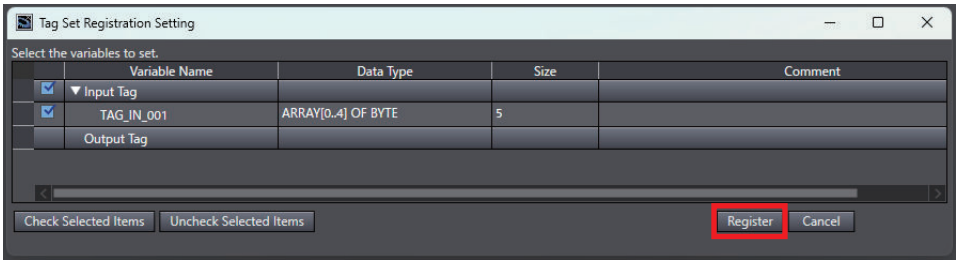
5 Double-click the network for which to set the tag data link, or right-click it then select **Edit**.



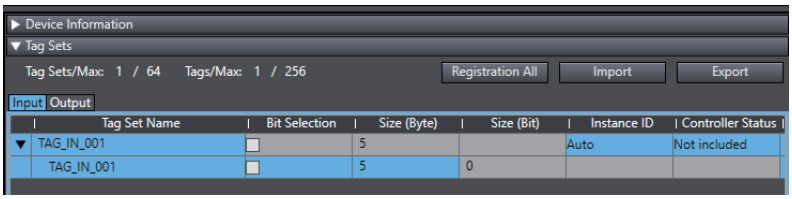
6 Check that the **Input** tab is selected, and then click **Registration All**.



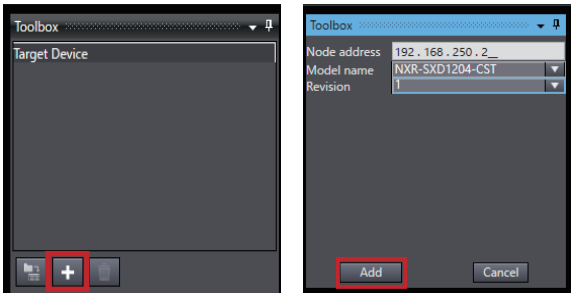
7 Check that the variable registered in step 3 is displayed, and then click **Register**.



The tag set is registered.

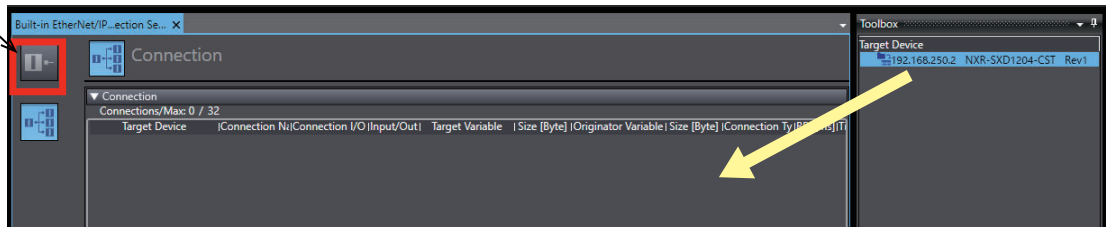


8 Click the **+** button of the Target Device field, enter the IP address, model name, and revision of the target, and click the **Add** button.

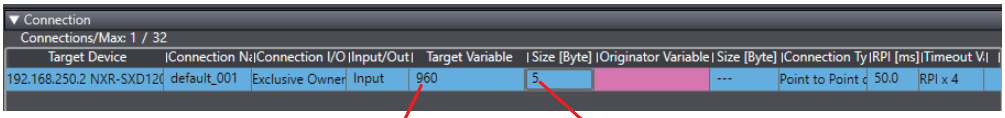


9 Click the **Connection** button to open the Connection Settings screen. The information of the target you just added is displayed in the Target Device field. Drag and drop it onto the Connection window.

Connection button



10 The target device is added to the Connection window. Enter the target variables.



Input Data (Assembly 960 to 3C0 Hex), Size 5 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input 3 Status	Safety Input 2 Status	Safety Input 1 Status	Safety Input 0 Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8
2	Safety Input 11 Status	Safety Input 10 Status	Safety Input 9 Status	Safety Input 8 Status	Safety Input 7 Status	Safety Input 6 Status	Safety Input 5 Status	Safety Input 4 Status
3	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	Reserved	Reserved	Reserved	Reserved
4	Application Number							

Enter the values of Assembly and Size shown in the table of *A-2 Safety I/O Assembly Data* on page A-4 for the target variable and size.

Set **Connection I/O Type**, **Connection Type**, **RPI**, and **Timeout Value** as necessary.

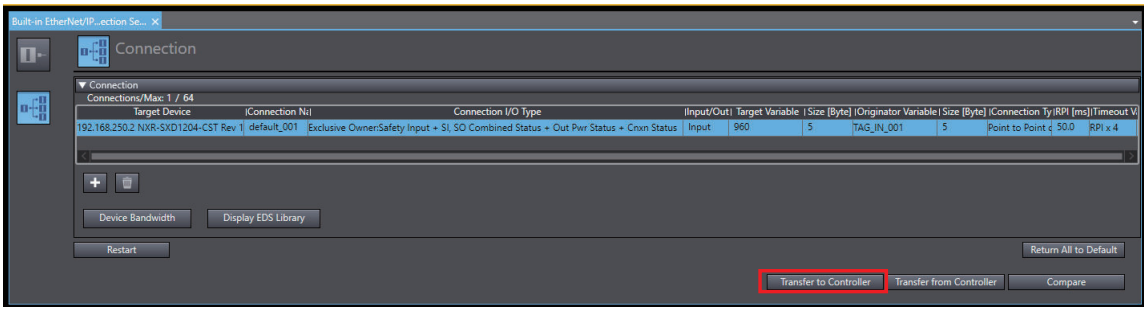
11 Enter the originator variables in the same way.

For the originator variables, select the tag set name set in step 7 from the pull-down list.

12 Go online and write the tag set and connection settings to the device.

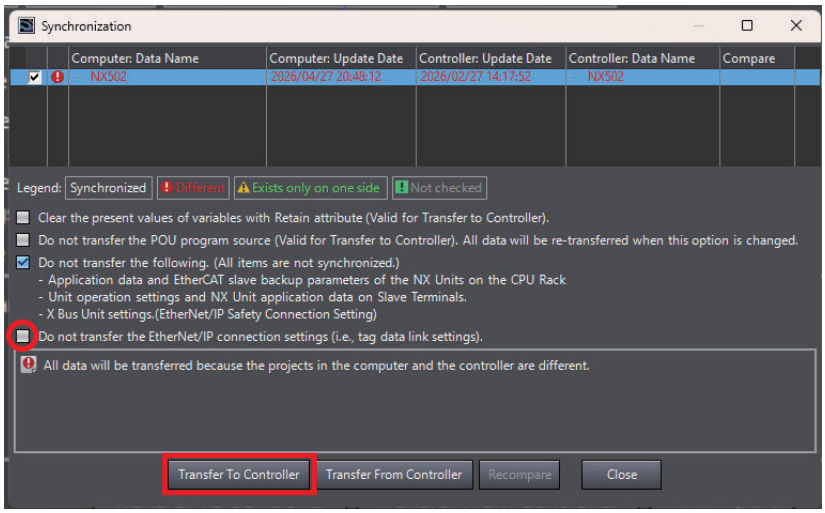
- When transferring only the tag data link settings

  Click **Transfer to Controller** on the connection settings screen.



- When synchronizing all data including programs

Select **Synchronization** from the **Controller** menu to display the Synchronization window.
Clear the **Do not transfer the EtherNet/IP connection settings (i.e., the tag data link settings)** check box, and click **Transfer to Controller**.



7-4-2 LLDP Function

The Link Layer Discovery Protocol (LLDP) function is used to exchange information between the Safety I/O Block and other network devices connected within a physically communicable range on the network.

Purpose of LLDP Function

The purpose of the LLDP function is to enable quick network configuration changes and error cause identification by gathering information on adjacent network devices.
For example, by using this function, you can detect which devices are connected to the network and what functions are currently enabled on those devices. This provides benefits such as being able to identify that the cause of a communications error is a network device configuration mistake.

Procedure for Using the LLDP Function

The LLDP function enable/disable setting is configured using explicit message communications.
The CIP objects related to the LLDP function are the *LLDP Management object* and *LLDP Data Table object*.
Refer to *A-4-12 LLDP Management Object (Class ID: 109 Hex)* on page A-51 and *A-4-13 LLDP Data Table Object (Class ID: 10A Hex)* on page A-53 for details on each of them.
Refer to *Explicit Message Server Function* on page 6-7 for the method to access CIP objects through an explicit message.

LLDP Function Details

The network device information that can be acquired using the LLDP function includes the following.

- MAC address
- Interface label

- Time that acquired information is valid
- Supported functions
- Management address
- CIP Identity
- Ethernet Preemption function status
- Time information when the information was last updated

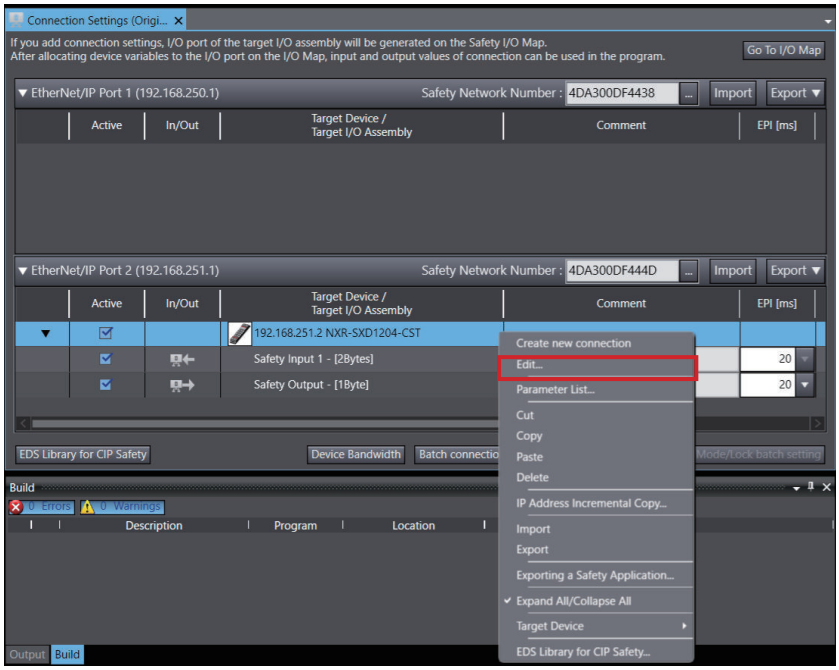
7-5 Safety Input Functions Settings

Configuring the settings of the safety input functions requires setting the parameters according to the connected devices.
This section explains the process using Sysmac Studio as an example.

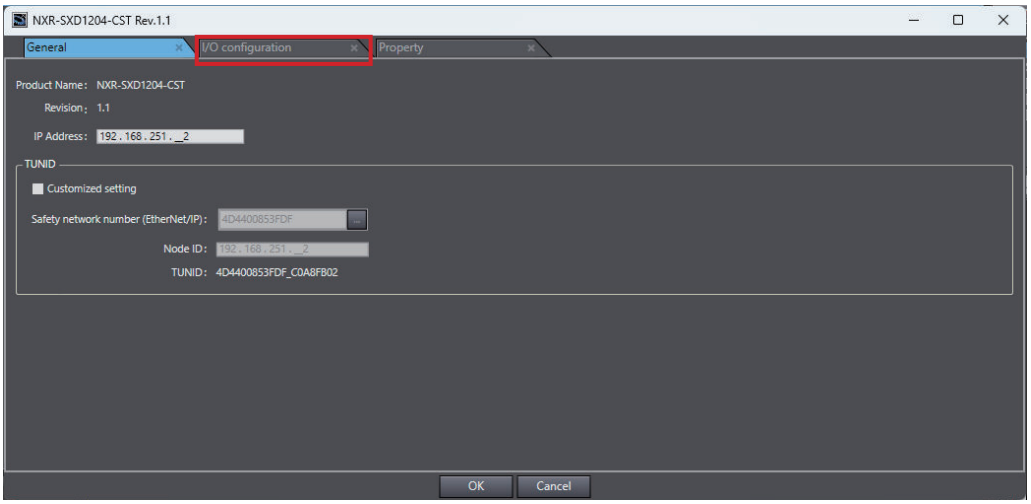
7-5-1 Setting Procedure for Safety Input Functions

Set the safety input functions of the Safety I/O Block by assigning input devices to the Safety I/O Block.
In addition, to capture signals from connected input devices, you need to configure the I/O configuration settings for each input terminal of the Safety I/O Block.
In Sysmac Studio, these settings are located in the Connection Settings (Originator) Edit Pane, so the explanation begins from that pane.
Refer to *7-3-1 Connection Settings for CIP Safety Communications* on page 7-27 for details on the CIP Safety connection settings.
Also refer to *6-4 Safety Input Functions* on page 6-8 for details on the safety input functions.
The following describes the procedure to configure the I/O configuration settings for devices registered in the Connection Settings (Originator) Edit Pane.

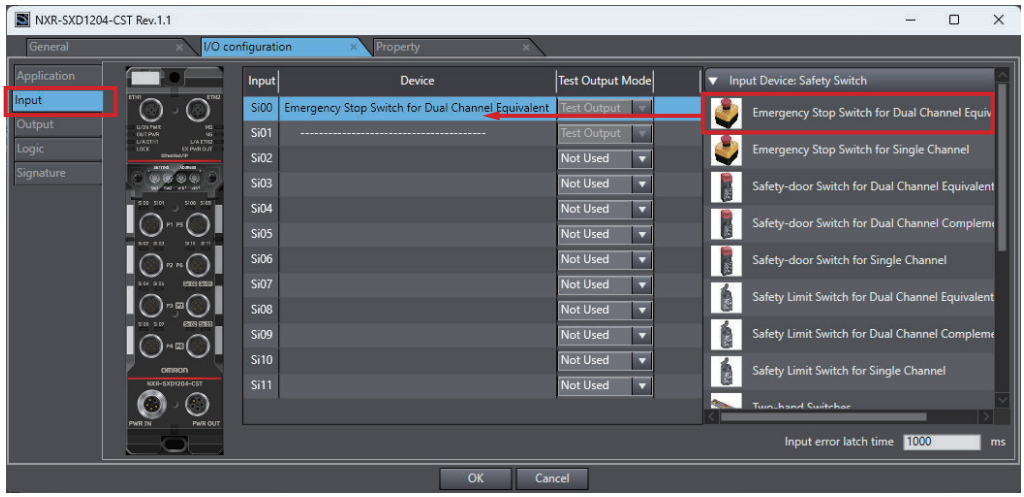
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane and double-click it, or right-click it and select **Edit** from the menu.



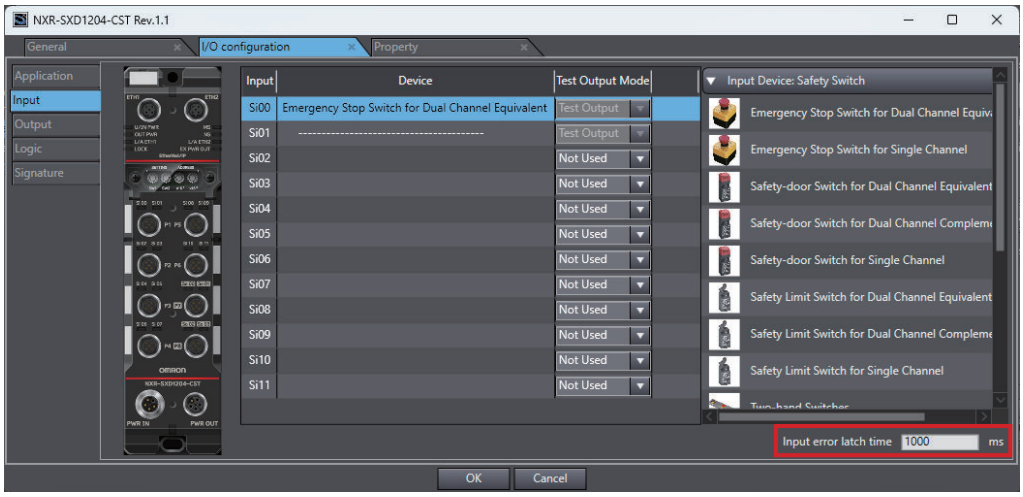
2 Select the **I/O configuration** tab.



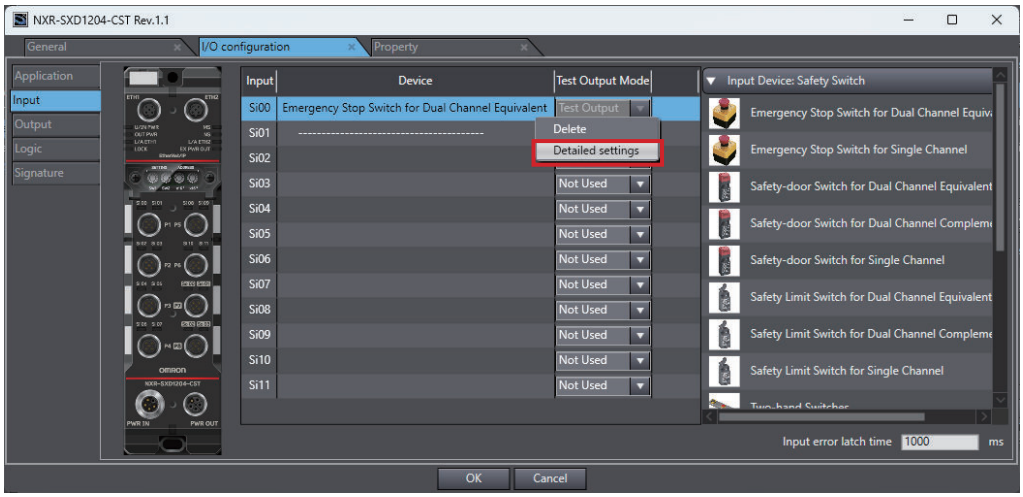
3 Register the input devices on the I/O Configuration Pane. The following register are possible only when the safety application is a remote I/O mode or user-defined application.
Select the **Input** tab on the left side to display the registration screen for input devices. Register an input device by expanding the toolbox on the right side and dragging and dropping any device onto the specified terminal.



4 Set **Input error latch time** at the bottom right of the screen as necessary.

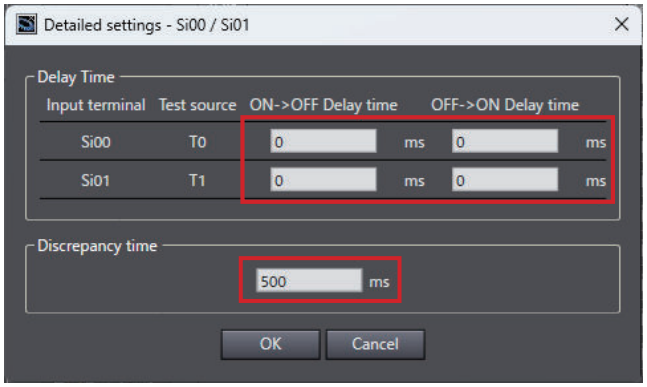


5 Select the registered input device and double-click it or select **Detailed settings** from the context menu of the registered input device to display the **Detailed settings** screen.



6 Set the following items as necessary.

- **ON->OFF Delay time**
- **OFF->ON Delay time**
- Discrepancy Time (dual channel input device only)



7 When setting is complete, click the **OK** button.

7-5-2 Setting Procedure for Standard Output Functions

When the safety input device is a device with semiconductor outputs, you can also select **Standard Output** for the Test Output Mode setting of the test output terminal.
Standard output from the Controller is possible by using a test output terminal.
Use it as a non-safety digital signal output terminal. For example, you can use it for monitor output by connecting it to the input of an indicator light or PLC.
The standard output function has a method that uses Sysmac Studio and a method that uses explicit message communications.

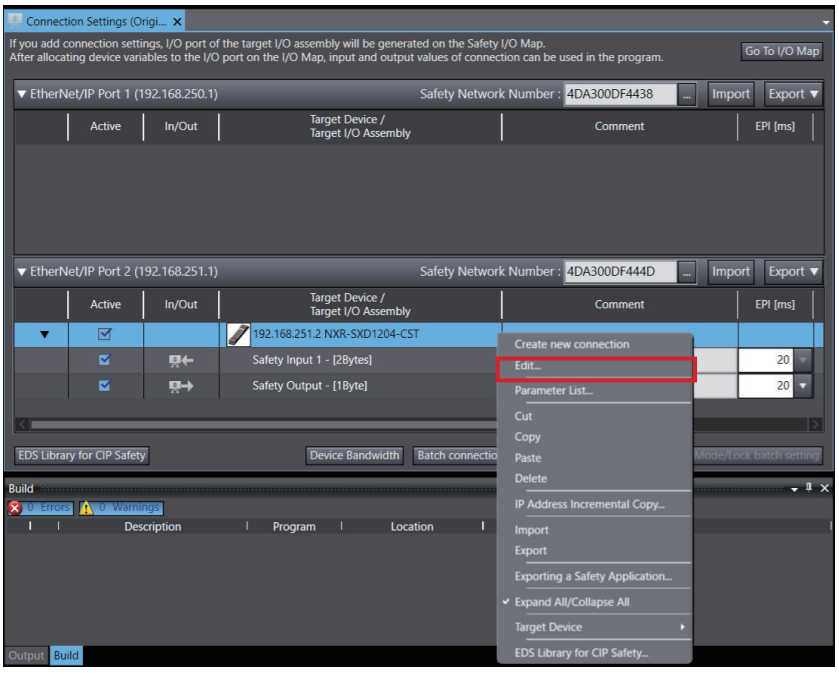
Additional Information

This function is not a safety function.

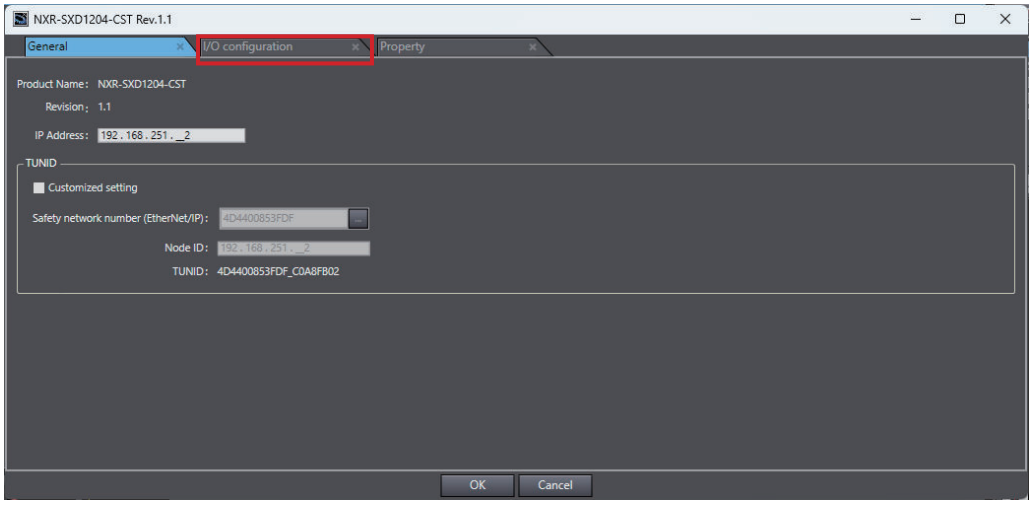
Setting Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.
In Sysmac Studio, these settings are located in the Connection Settings (Originator) Edit Pane, so the explanation begins from that pane.
Refer to *7-3-1 Connection Settings for CIP Safety Communications* on page 7-27 for details on the CIP Safety connection settings.
Also refer to *6-4 Safety Input Functions* on page 6-8 for details on the safety input functions.
The following describes the procedure to configure the I/O configuration settings for devices registered in the Connection Settings (Originator) Edit Pane.

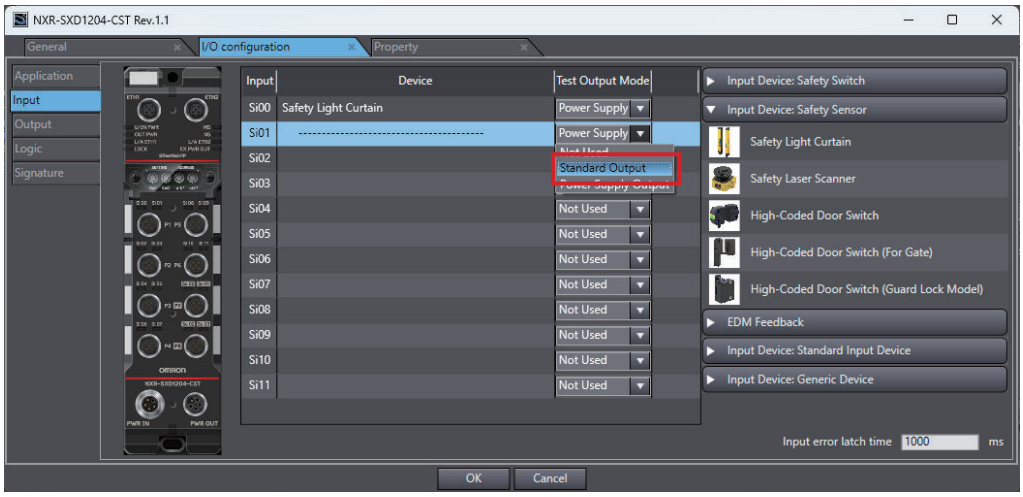
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane and double-click it, or right-click it and select **Edit** from the menu.



2 Select the **I/O configuration** tab.



3 Select **Standard Output** in the **Test Output Mode** setting for a terminal of an input device that is a device with semiconductor outputs. Settings are possible only when the safety application is a remote I/O mode or user-defined application.



4 When setting is complete, click the **OK** button.

Setting Procedure Using Explicit Message Communications

Set the usage method of the test output mode to **Standard Output**. Furthermore, set the output value of the test output terminal.
The commands to send are as follows.

Implementation details	Send command item	Send command value
Set the output value of the test output terminal*1	Service code	10 hex (Set_Attribute_Single)
	Class ID	09 hex (Discrete Output Point (DOP) object)
	Instance ID	01 hex to 0C hex (Specify the instance of each test output terminal.)
	Attribute ID	3 (Value)
	Service data	TRUE: Test output terminal is ON FALSE: Test output terminal is OFF

***1.** Writing of the value is possible only when Test Output Mode is **Standard Output**. Otherwise, the output value of the test output terminal is fixed to TRUE.

Refer to *Explicit Message Server Function* on page 6-7 for the method to access CIP objects through an explicit message.

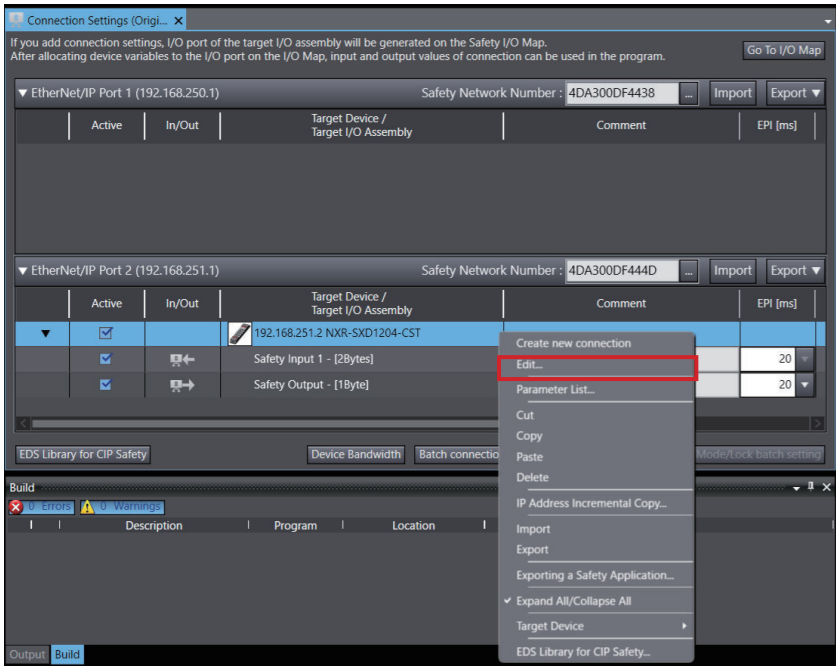
7-6 Setting Safety Output Functions

Configuring the settings of the safety output functions requires setting the parameters according to the connected devices.
This section explains the process using Sysmac Studio as an example.

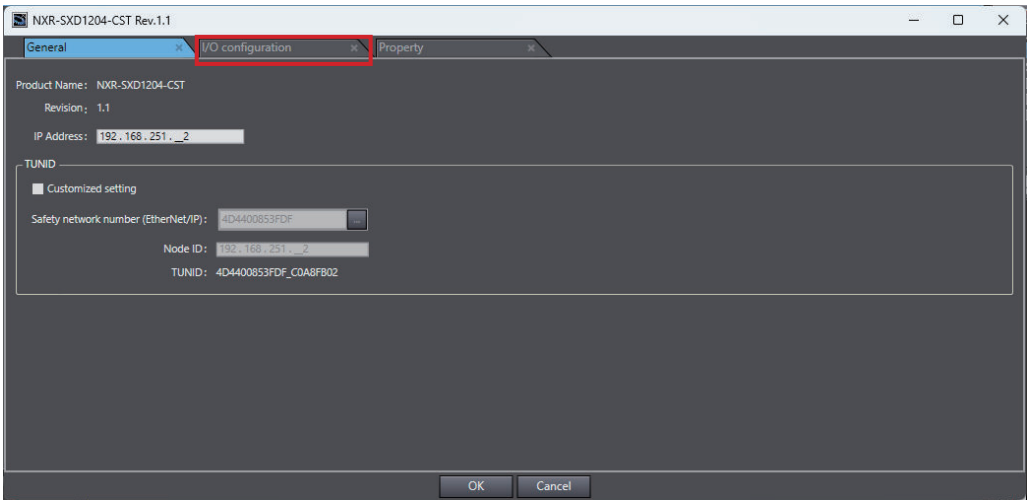
7-6-1 Safety Output Function Setting Procedure

Set the safety output functions of the Safety I/O Block by assigning output devices to the Safety I/O Block. Furthermore, to output signals to connected output devices, you need to configure the I/O configuration settings for each output terminal of the Safety I/O Block.
In Sysmac Studio, these settings are located in the Connection Settings (Originator) Edit Pane, so the explanation begins from that pane.
Refer to *7-3-1 Connection Settings for CIP Safety Communications* on page 7-27 for details on CIP Safety connection settings.
Also refer to *6-5 Safety Output Functions* on page 6-16 for details on the safety output functions.
The following describes the procedure to configure the I/O configuration settings for devices registered in the Connection Settings (Originator) Edit Pane.

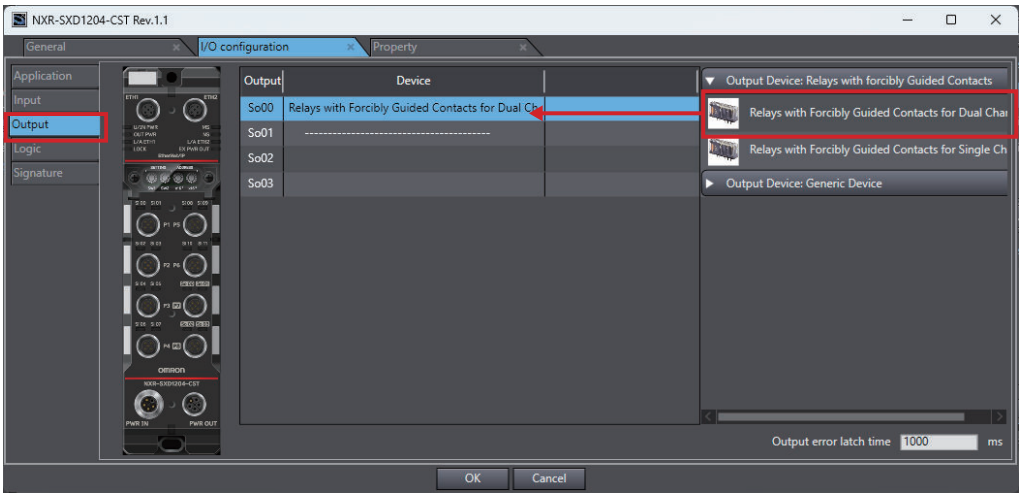
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane and double-click it, or right-click it and select **Edit** from the menu.



2 Select the **I/O configuration** tab.

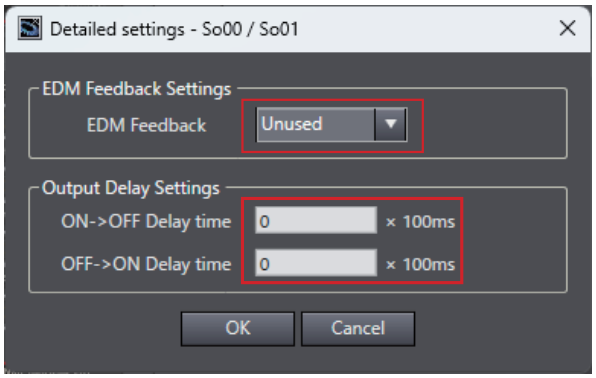


3 Register the output devices on the I/O Configuration Pane. The following register are possible only when the safety application is a remote I/O mode or user-defined application.
Select the **Output** tab on the left side to display the registration screen for output devices. Register an output device by expanding the toolbox on the right side and dragging and dropping any device onto the specified terminal.

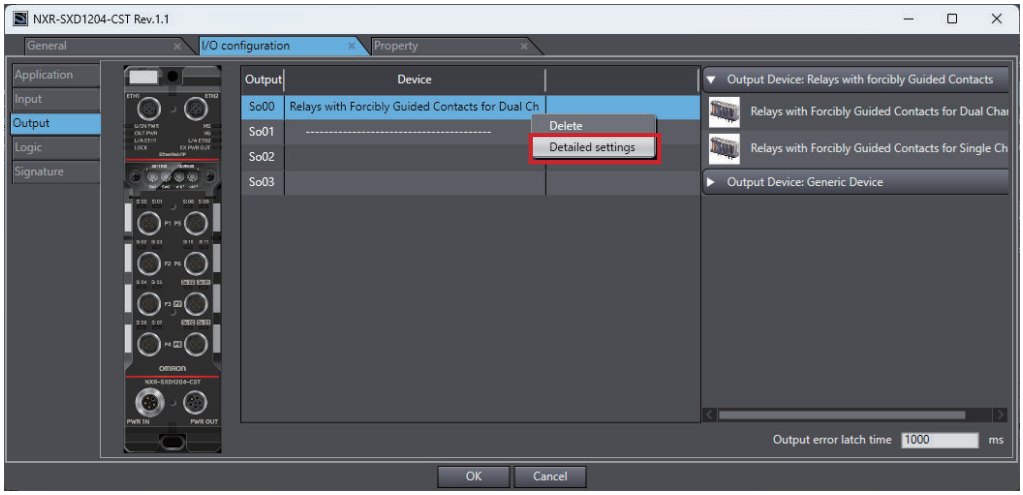


4 If the security application is a user-defined application, dragging and dropping it will display the **Detailed settings** screen, where you can configure the following items.

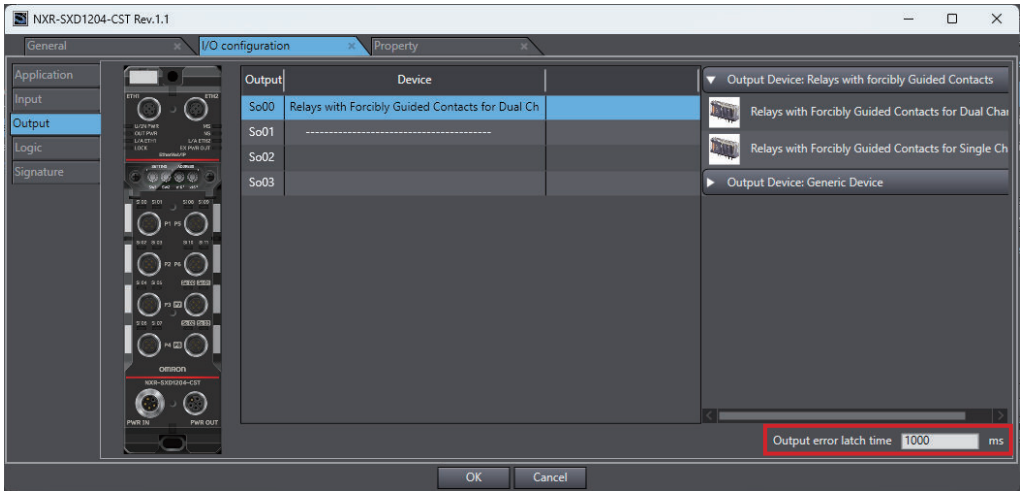
- EDM feedback (displayed only for terminals with **EDM feedback** registered on the safety input device)
- **ON->OFF Delay time**
- **OFF->ON Delay time**



5 If the safety application is a user-defined application, you can also display the **Detailed settings** screen by selecting the registered output device and double-clicking it, or by selecting **Detailed settings** from the context menu of the registered output device.



6 Set **Output error latch time** at the bottom right of the screen as necessary.



7 When setting is complete, click the **OK** button.

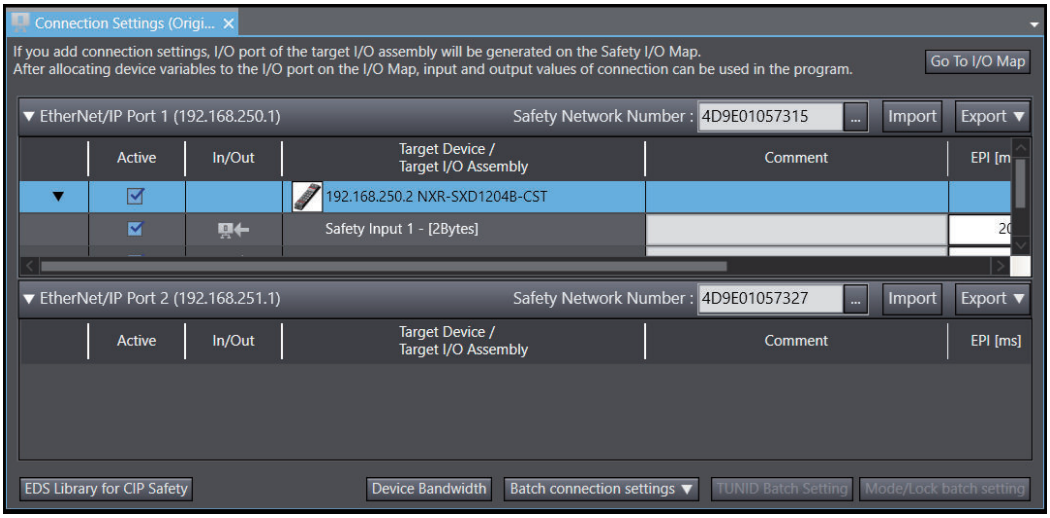
7-7 Logic Function Settings

With user-defined applications and add-on applications, you can design your own custom logic. Use Sysmac Studio to configure the logic.

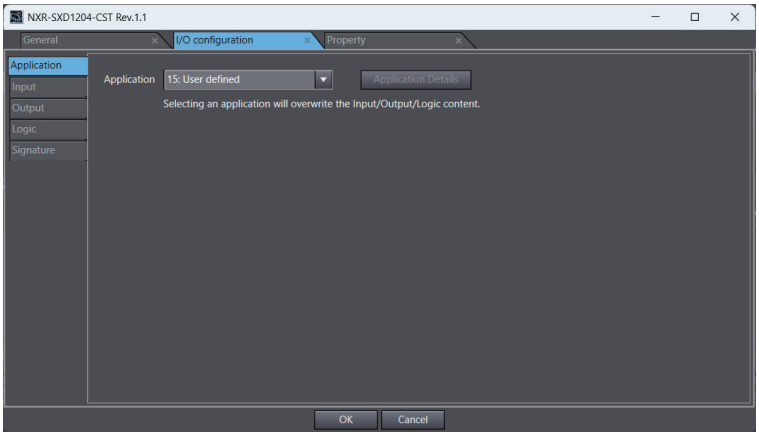
7-7-1 Logic Setting Procedure

Configure the logic settings after configuring the EtherNet/IP safety connection settings of each target device and target I/O assembly to be connected to the Safety I/O Block. Here, the explanation assumes that the safety input device settings are already completed.
Refer to *7-5-1 Setting Procedure for Safety Input Functions* on page 7-44 for details on the safety input device setting procedure.
The logic setting procedure is as follows.

1 In Sysmac Studio, go to **Configurations and Setup** - **Communications** - **Safety** - **EtherNet/IP Safety Connection Settings** of the Safety CPU Unit, and select **Connection Settings (Originator)**.
The **Connection Settings (Originator)** tab page is displayed.

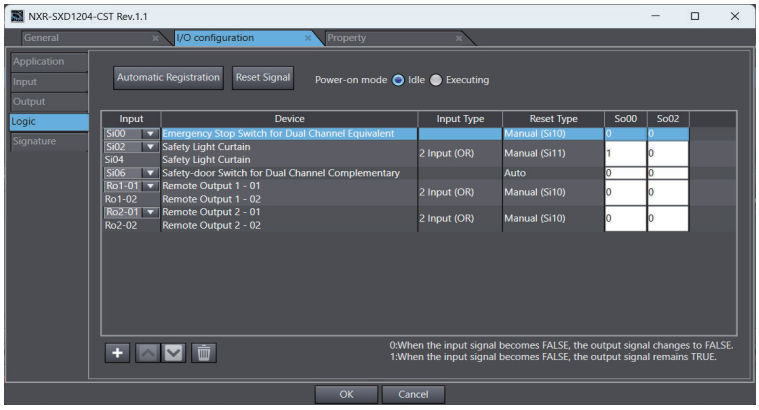


2 Select the **Application** tab of **I/O configuration** tab and set the application to**15: User defined**.



3 Select **Logic** tab of **I/O configuration** tab.

The following logic setting screen is displayed.



4 Click the **Automatic Registration** button.
Device rows are added. Furthermore, reset type, input type, and input signal settings are registered automatically on each row. The rules for automatic registration are as follows.

Item	Automatic registration rules
Device	The devices set on the **Input** tab that are neither reset switches nor EDM feedback are added.
Reset type	If reset switches are set on the **Input** tab: Manual reset of the minimum input terminal number with a reset switch set If reset switches are not set on the **Input** tab: Auto
Input type	All unset
So00 to So03	A column is created in the logic setting screen according to the settings on the **Output** tab. The values are all 0.

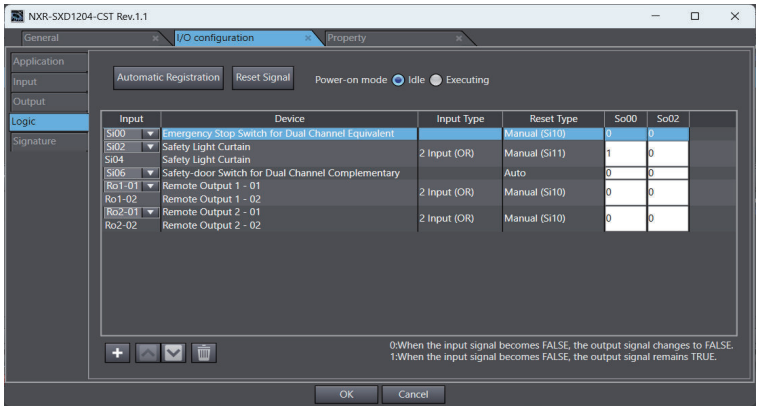
Furthermore, the input terminal numbers of the reset switches set on the **Input** tab are registered automatically in the reset signal.

5 Next, change the reset signal settings, change the logic settings, and configure the remote output settings.

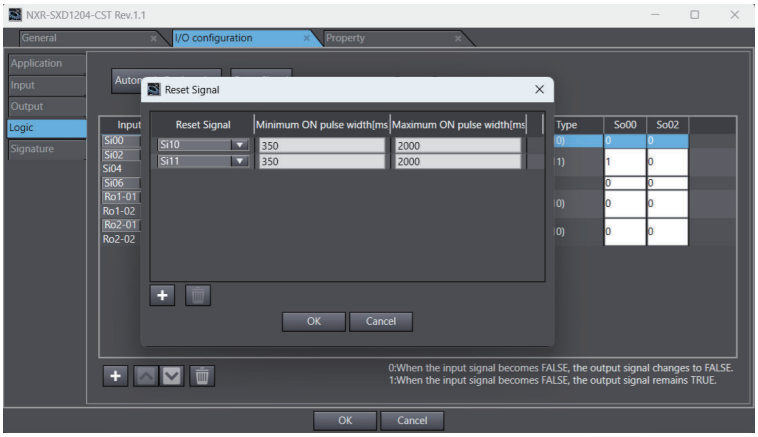
Changing the Reset Signal Settings

Change the automatically registered reset signal settings as necessary.

1 Click the **Reset signal** button on the **I/O configuration** tab and **Logic** tab.



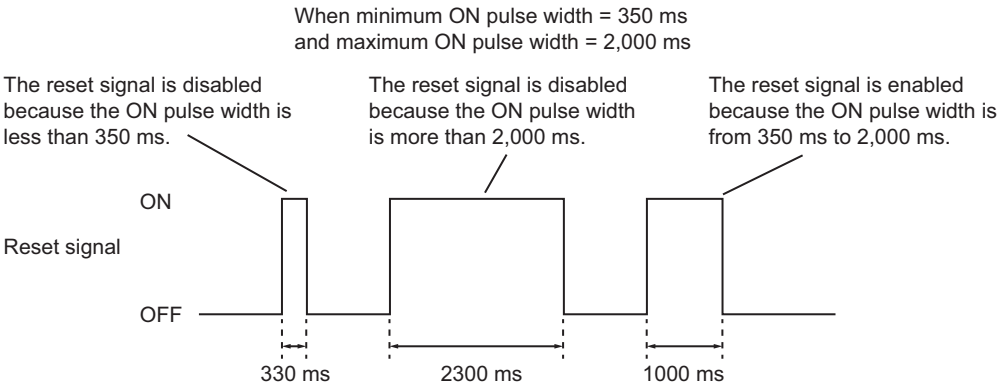
The **Reset signal** screen is displayed.



2 Set one of safety input terminals Si00 to Si11 or one of remote outputs Ro1-01, Ro1-02, Ro2-01, Ro2-02, Ro3-01, and Ro3-02 to the reset signal.

3 Set the minimum ON pulse width and maximum ON pulse width of the reset signal.
If the time that the reset signal is ON is the minimum ON pulse width or higher and the maximum ON pulse width or lower, the logic is reset. The initial value and settable range of each setting item are as follows.

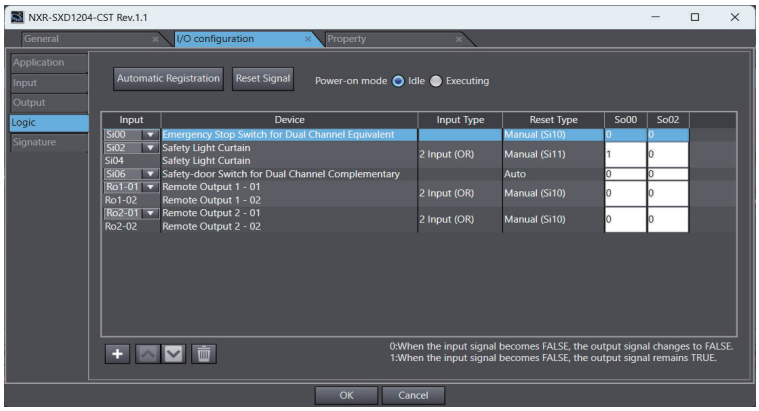
Setting item	Initial value [ms]	Settable range [ms]
Minimum ON pulse width	350	100 to 1,000 50 ms increments
Maximum ON pulse width	2,000	1,000 to 30,000 50 ms increments



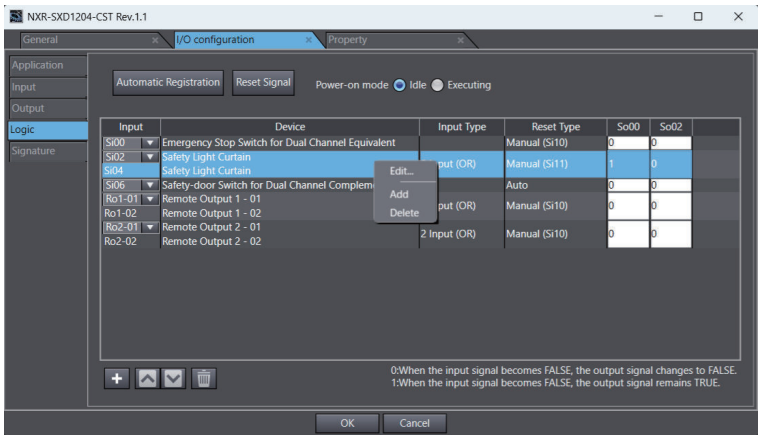
Changing the Logic Settings

Change the logic settings of each device as necessary.

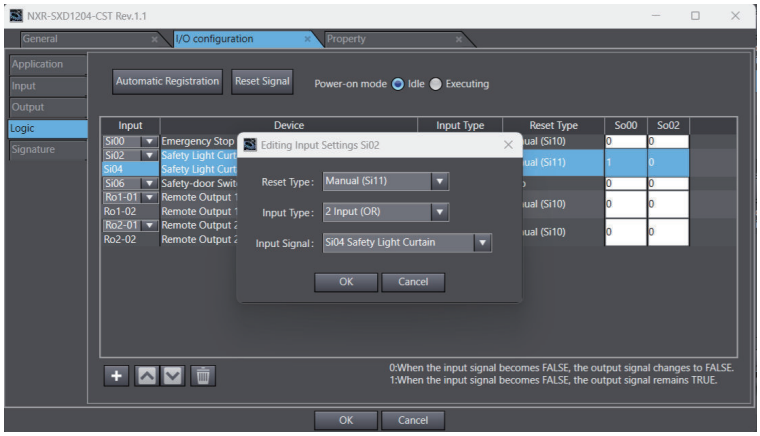
1 Select the **I/O configuration** tab and **Logic** tab, move the cursor to the row of the device for which you want to change the settings, and right-click.



A submenu like the following is displayed.



2 Select **Edit**.
The following edit screen is displayed.



3 Set **Reset type**, **Input type**, and **Input signal**.

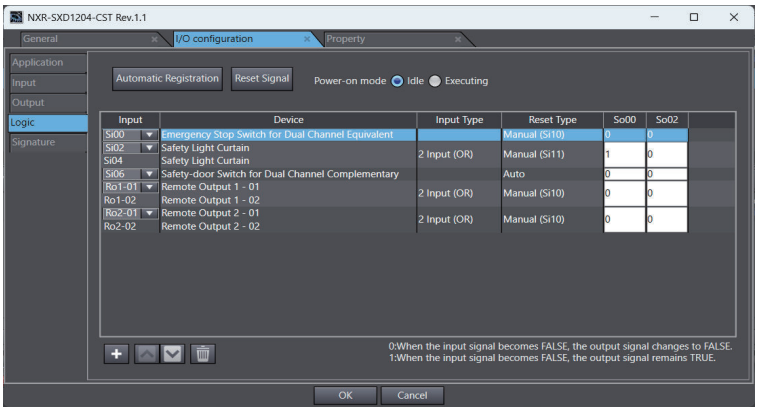
4 Directly enter **0** or **1** in the fields of safety output terminals So00 to So03.

5 To add a row, select **Add** in the submenu. To remove a row, select **Remove**.

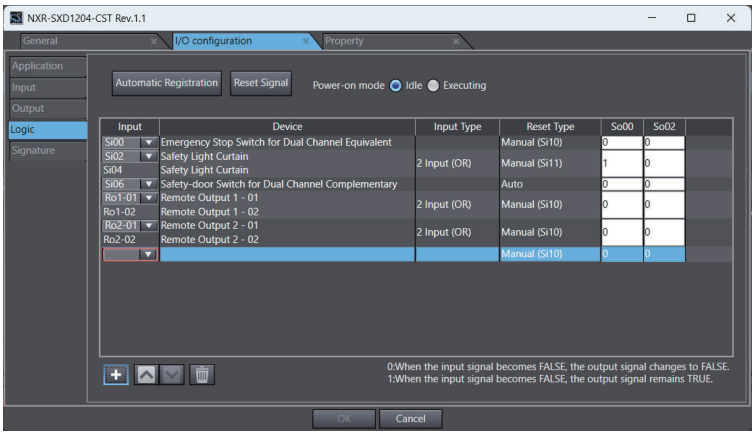
Remote Outputs Settings

Add and configure remote outputs as necessary.

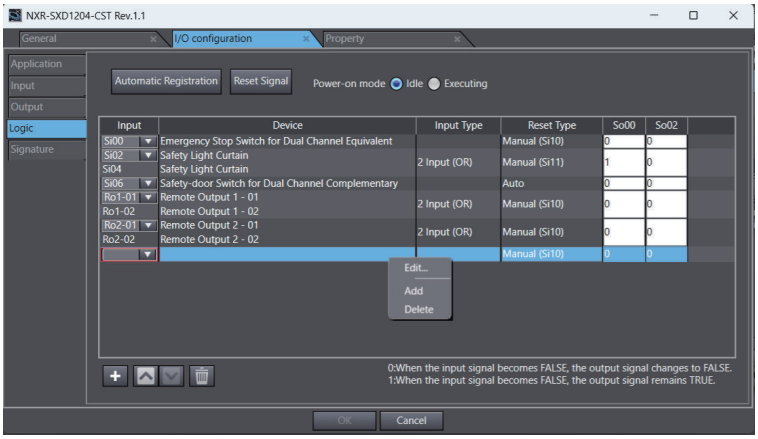
1 Click the **+** button on the **I/O configuration** tab and **Logic** tab.



A new row is added.

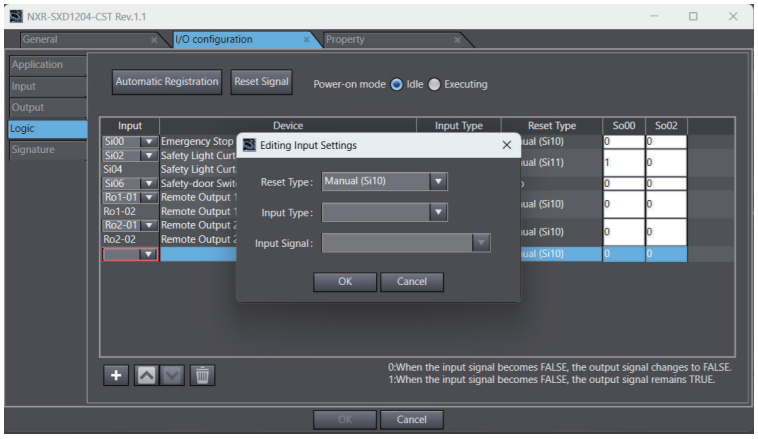


2 Move the cursor to the added row, and then right-click.
A submenu like the following is displayed.



3 Select **Edit**.

The following edit screen is displayed.

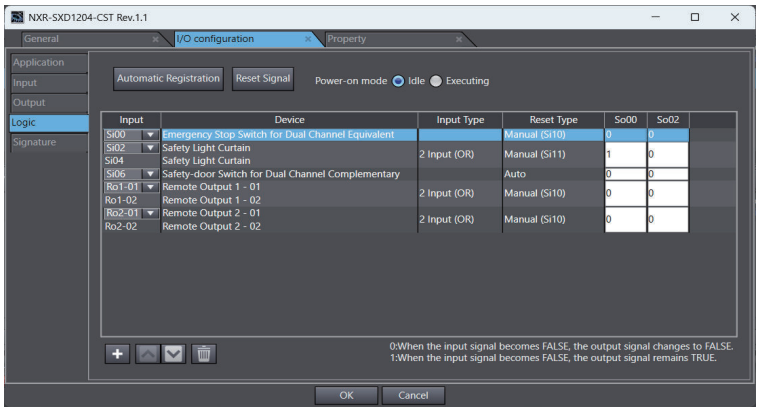


4 Set **Reset Type**, **Input Type**, and **Input Signal**. Set one of **Ro1-01**, **Ro1-02**, **Ro2-01**, **Ro2-02**, **Ro3-01**, and **Ro3-02** in **Input Signal**.

Setting the Power-on Mode

Set the operating mode to enter when the power is turned ON. If the operating mode when the power is turned ON is **Executing**, the safety application executes immediately after the power is turned ON.

1 Set **Power-on mode** to **Idle** or **Executing** on the **I/O configuration** tab and **Logic** tab.



2 Click the **OK** button.

Precautions for Correct Use

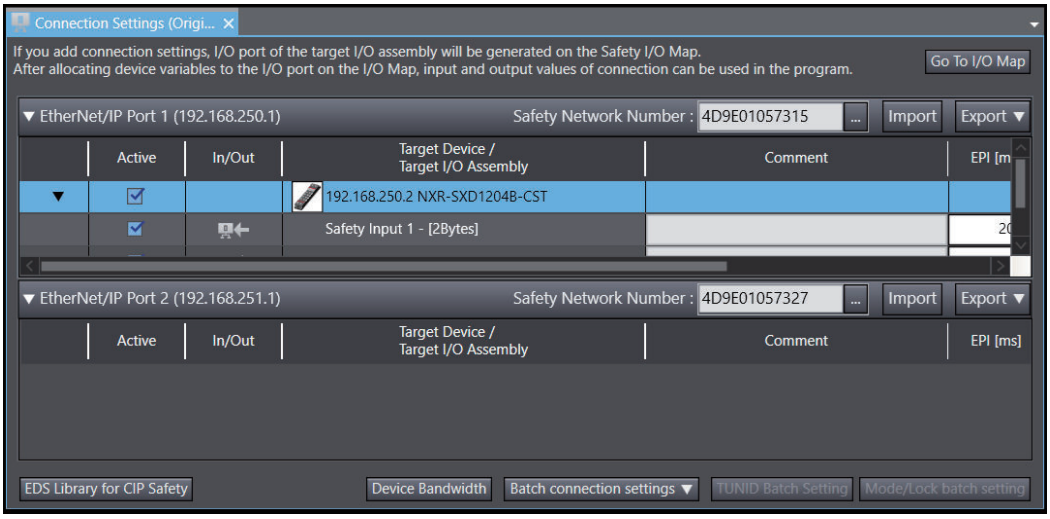
If the operating mode when the power is turned ON is **Idle**, safety output turns OFF because the safety application does not execute when the power is turned ON. To execute the safety application, change the operating mode for the Safety I/O Block. Set it to **Executing**.

7-7-2 Displaying the Parameter List

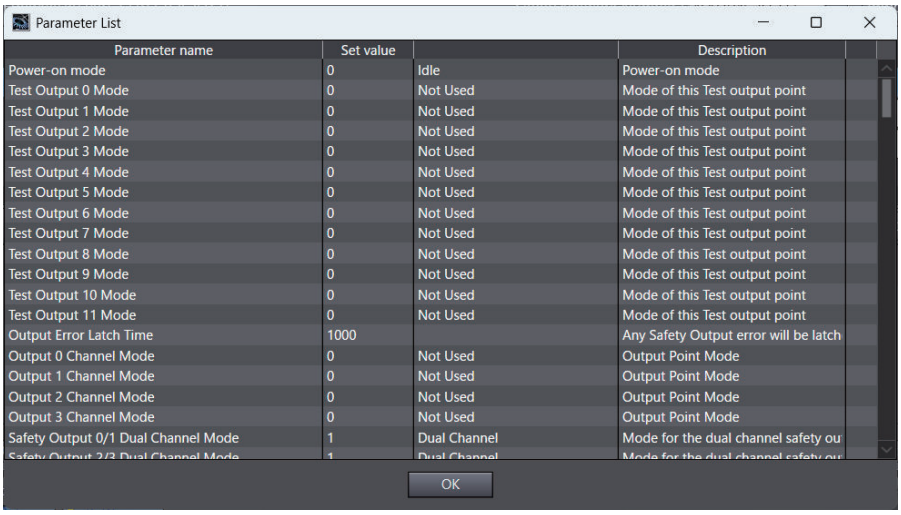
A list of the set parameters is displayed. Check that each parameter is set as intended.
The displayed items are as follows.

Item	Description
Parameter name	Setting parameter name
Setting value	Set value
Setting value (enum value)	Meaning of setting value
Description	Meaning of parameter name

1 In Sysmac Studio, go to **Configurations and Setup** - **Communications** - **Safety** - **EtherNet/IP Safety Connection Settings** of the Safety CPU Unit, and select **Connection Settings (Originator)**.
The **Connection Settings (Originator)** tab page is displayed.



2 Double-click Safety I/O Block, or right-click it and select **Parameter List**.
The parameter list is displayed.

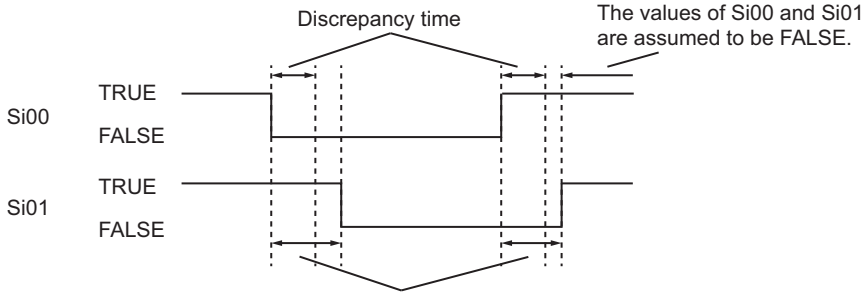


7-7-3 Examples of Abnormal Operations of Input Devices That Should Be Considered

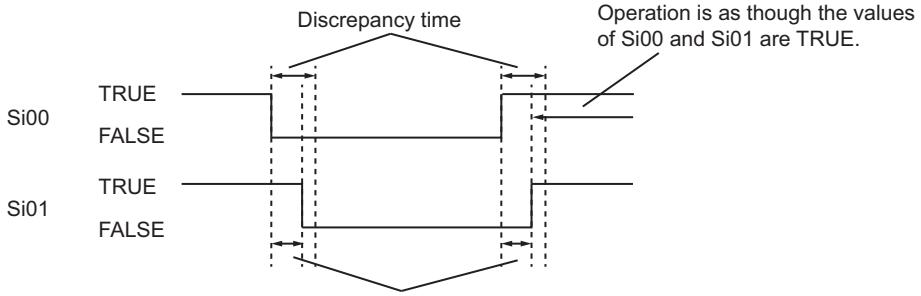
When configuring a logic function, to ensure that the equipment always operates safely, you should consider the possibilities of input devices unexpectedly operating abnormally. This section presents examples of abnormal operations of input devices.

Discrepancy Error at Safety Input

Of two inputs of a dual-channel input device, if the time from one value changing to the other value changing exceeds the preset discrepancy time, the *Discrepancy Error at Safety Input (65230000 hex)* event occurs because the change of input values cannot be detected normally. When the *Discrepancy Error at Safety Input (65230000 hex)* event occurs, operation is performed as if the value of the safety input data is FALSE.
Refer to *6-4-4 Dual Channel Evaluation* on page 6-11 for details on the discrepancy time.
Refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details on events.



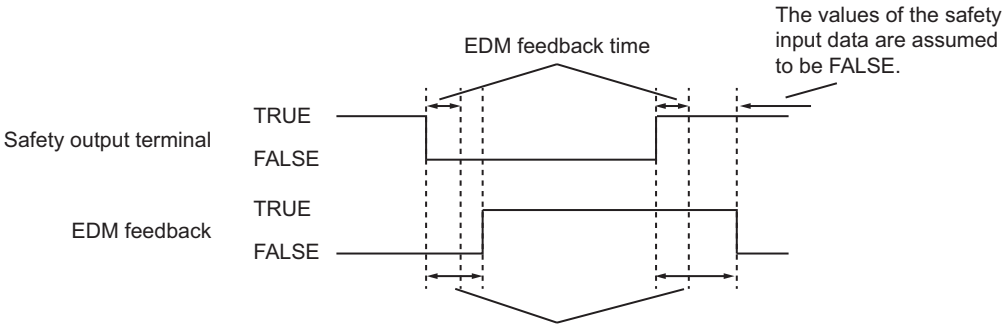
The time from the Si00 changing to the Si01 changing exceeds the discrepancy time, so operation is as though the values of Si00 and Si01 are FALSE also after the values of Si00 and Si01 become TRUE.



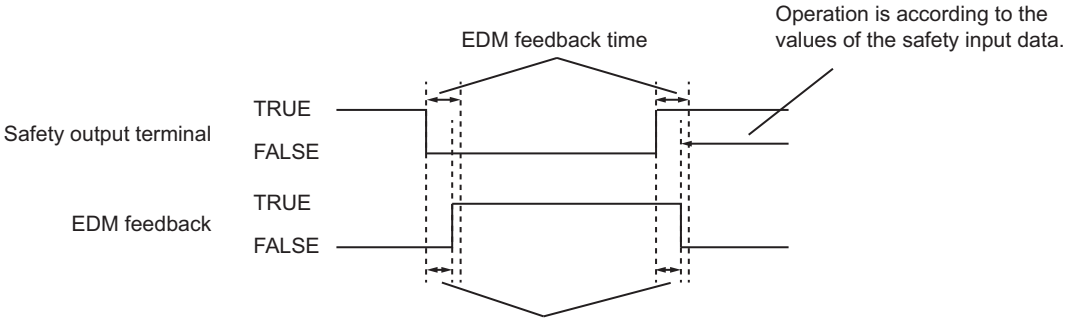
The time from the Si00 changing to the Si01 changing is within the discrepancy time, so operation is according to the values of Si00 and Si01.

EDM Error

If the time from the value of a safety output terminal changing to the value of EDM feedback changing exceeds the EDM feedback time when EDM feedback is set, an *EDM Error (652B0000 hex)* event occurs. When the *EDM Error (652B0000 hex)* event occurs, operation is performed as if the value of the safety input data is FALSE.
Refer to *6-5 Safety Output Functions* on page 6-16 for details on EDM feedback. In addition, refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details on events.



The time from the value of a safety output terminal changing to the value of EDM feedback changing exceeds the EDM feedback time, so operation is as though the values of the safety input data are FALSE.



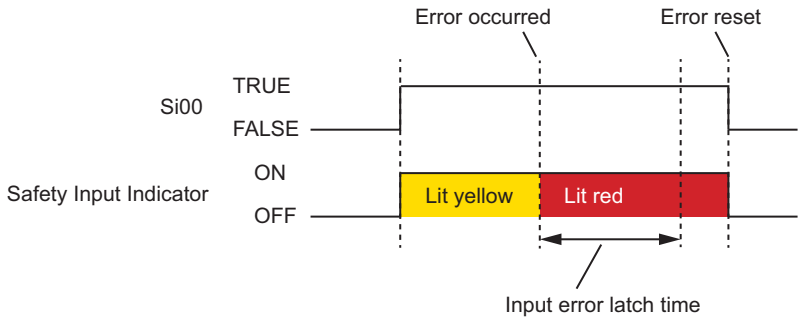
The time from the value of a safety output terminal changing to the value of EDM feedback changing is within the EDM feedback time, so operation is according to the values of the safety input data.

External Test Signal Failure at Safety Input

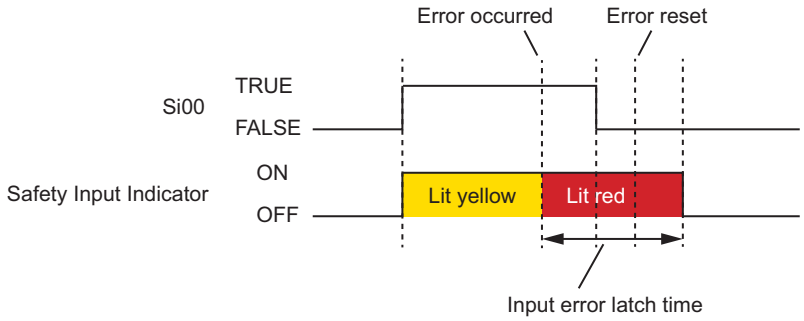
If an input signal line contacts with the power line (positive side), input signal lines are shorted, a connected external device fails, or other problem occurs when using the test pulse evaluation, the *External Test Signal Failure at Safety Input (65220000 hex)* event occurs. When the *External Test Signal Failure at Safety Input (65220000 hex)* event occurs, operation is performed as if the value of the safety input data is FALSE.
Refer to *6-4-3 Test Pulse Evaluation Function* on page 6-10 for details on the test pulse evaluation.
Refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details on events.

Error with Continuous Time Shorter than Input Error Latch Time

When the input error latch time is set, even if the time from error occurrence to error reset is shorter than the input error latch time, error processing continues for the duration of the input error latch time.
For example, the safety input indicator remains lit in red until the input error latch time ends even if the error has been reset.
Refer to *6-4-7 Input Error Latch Time* on page 6-15 for details on the input error latch time.



The safety input indicator turns off immediately after the error reset because the time from error occurrence to error reset exceeds the input error latch time.

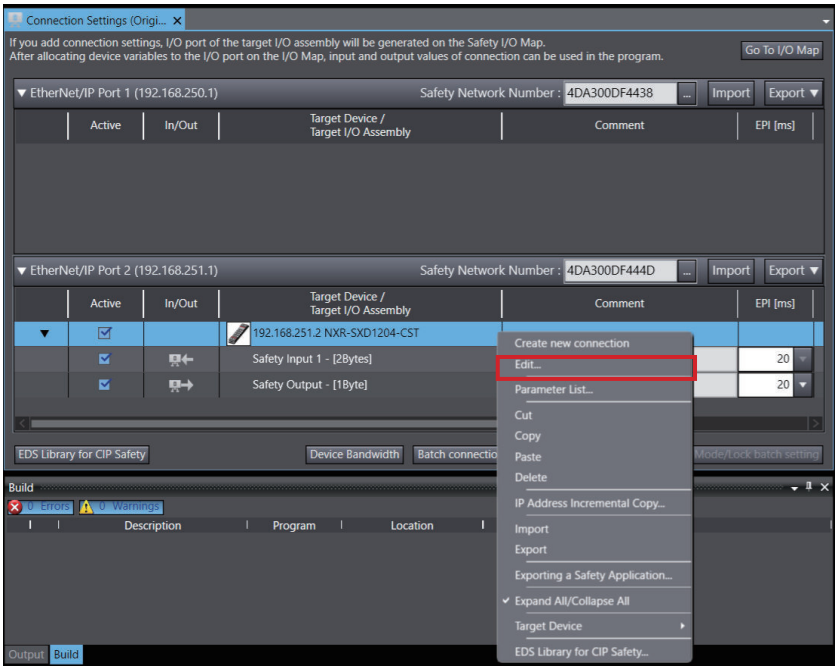


Even if the error is reset, the safety input indicator remains lit in red until the input error latch time ends.

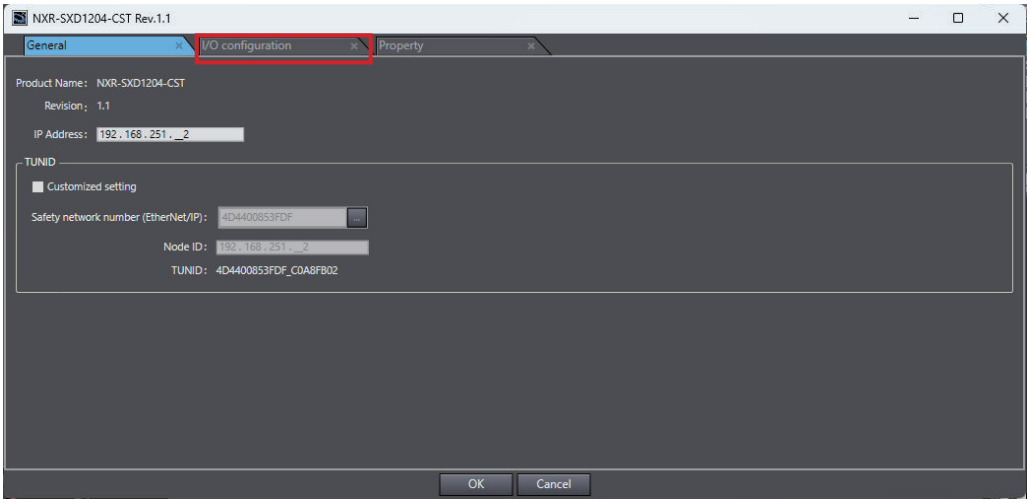
7-8 Setting the Safety Signatures

Configure the settings of the safety signatures on the Safety I/O Block.
In Sysmac Studio, these settings are located in the Connection Settings (Originator) Edit Pane, so the explanation begins from that pane.
Refer to *7-3-1 Connection Settings for CIP Safety Communications* on page 7-27 for details on the CIP Safety connection settings.
The following describes the procedure to configure the safety application settings to use for the devices registered in the Connection Settings (Originator) Edit Pane.

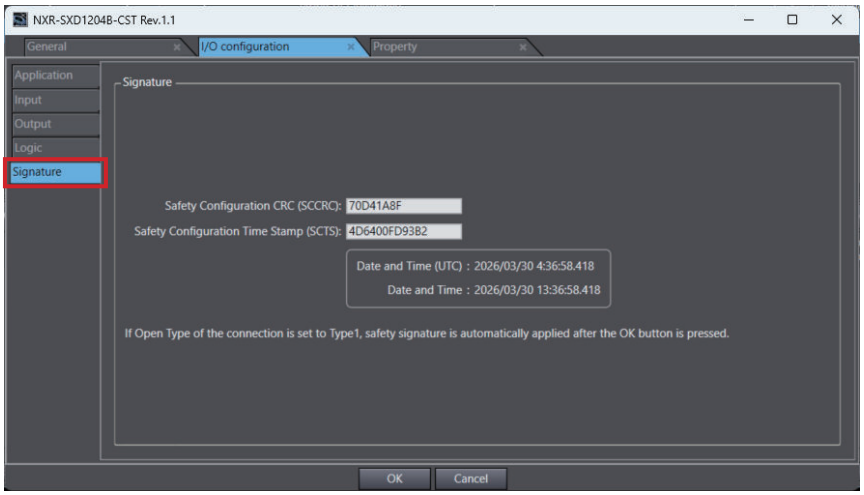
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane and double-click it, or right-click it and select **Edit** from the menu.



2 Select the **I/O configuration** tab.



3 Select the **Signatures** tab.



4 Set the Safety Configuration CRC (SCCRC) and Safety Configuration Time Stamp (SCTS), and click the **OK** button.

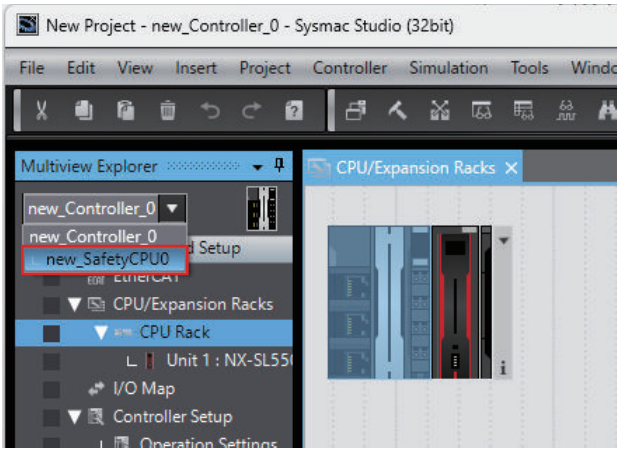
7-9 Create the safety application file

This section explains the steps for creating and exporting a safety application file.
If the safety control system is *configuration for the safety controller to perform control (configuration using the Web UI)*, create and export a safety application file for remote I/O mode. This safety application file defines only the I/O configuration settings.
If the safety control system is *configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user*, create and export a safety application file for the add-on application. This safety application file defines the logic settings and I/O configuration settings.

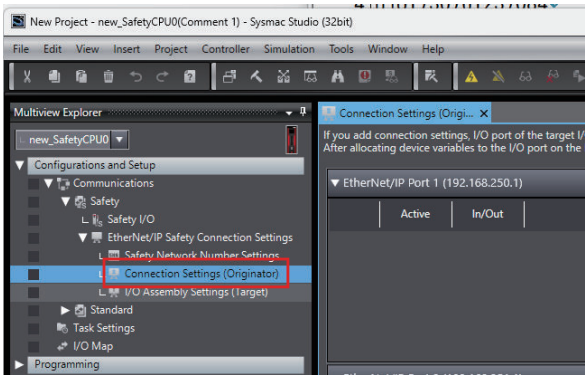
7-9-1 Registration of Safety I/O Block

To export the safety application file, register the Safety I/O Block.

1 In the Multiview Explorer, select the target Safety CPU Unit in the Controller Selection Box.



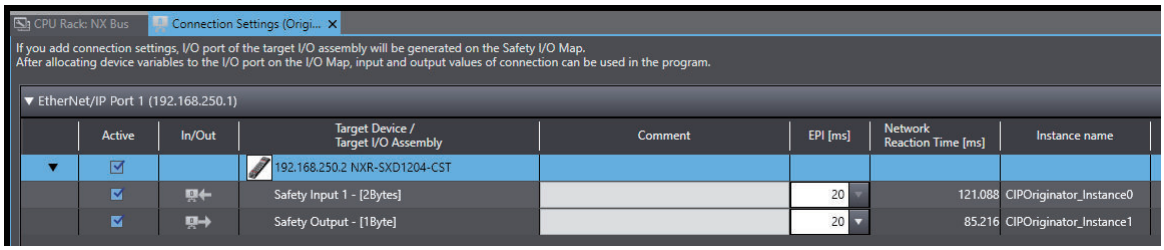
2 In Multiview Explorer, go to **Configurations and Setup** - **Communications** - **Safety** - **EtherNet/IP Safety Connection Settings** and double-click **Connection Settings (Originator)**, or right-click it and select **Edit**.
The Connection Settings (Originator) Edit Pane is displayed on the Edit Pane.



3 Select **Safety I/O and Logic Device** from Toolbox, and select **NXR-SXD1204-CST** or **NXR-SXD1204B-CST**.



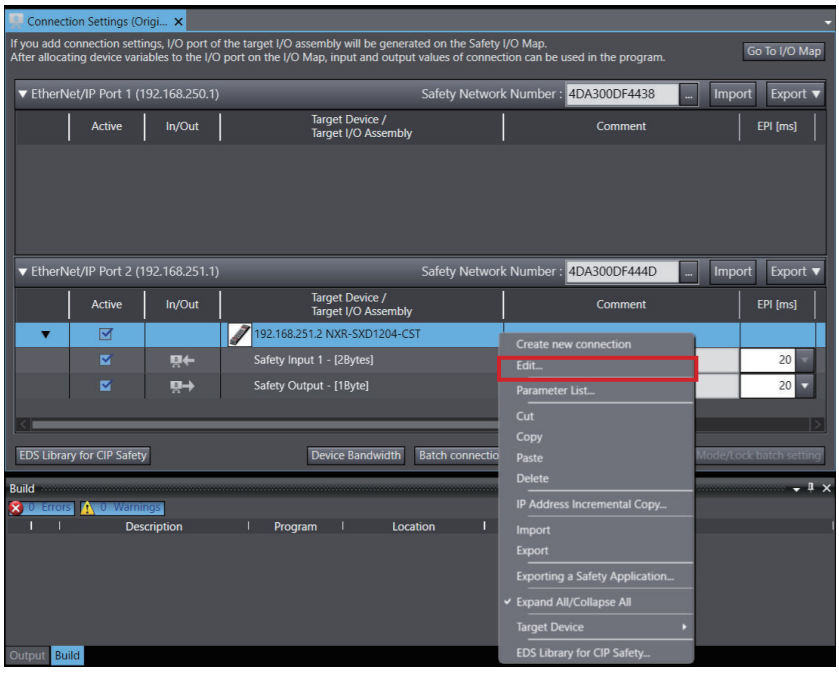
4 Drag the Safety I/O Block selected in the toolbox.



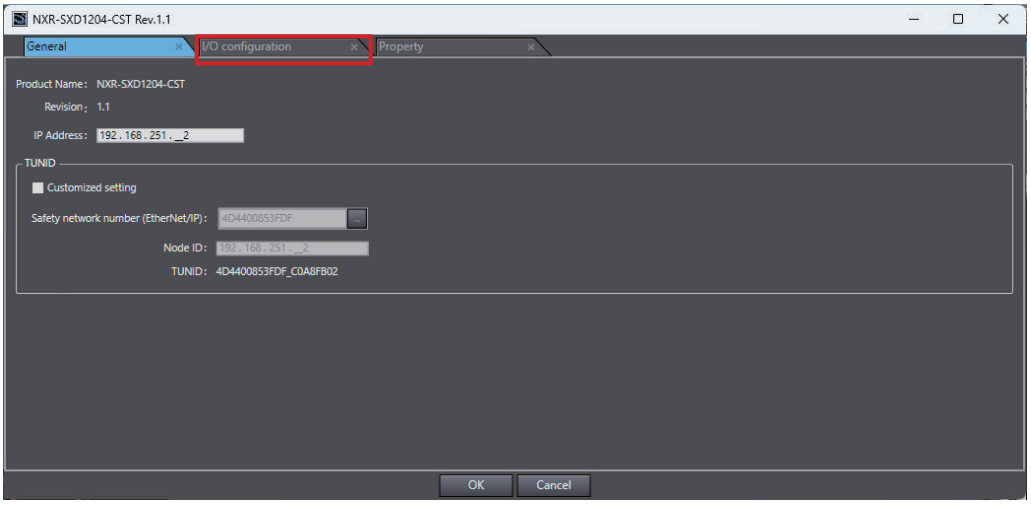
7-9-2 Safety Application Settings

Configure the settings of the safety application to use with the Safety I/O Block.

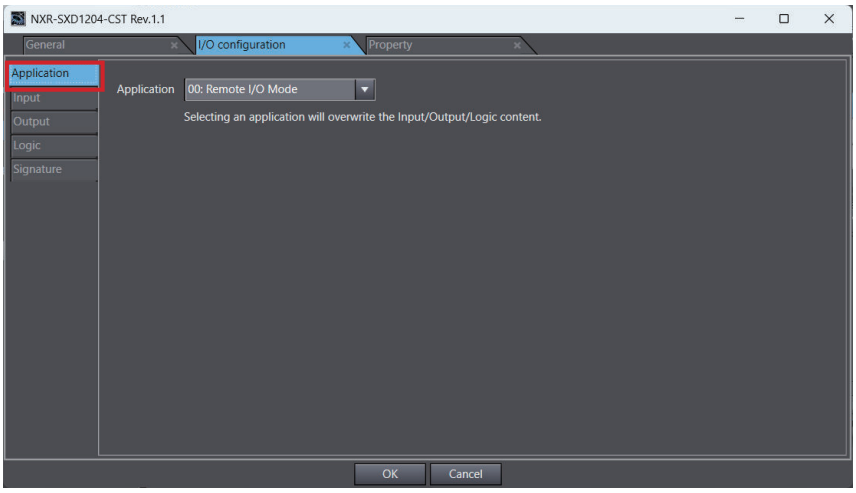
1 Select Safety I/O Block on the Connection Settings (Originator) Edit Pane and double-click it, or right-click it and select **Edit** from the menu.



2 Select the **I/O configuration** tab.



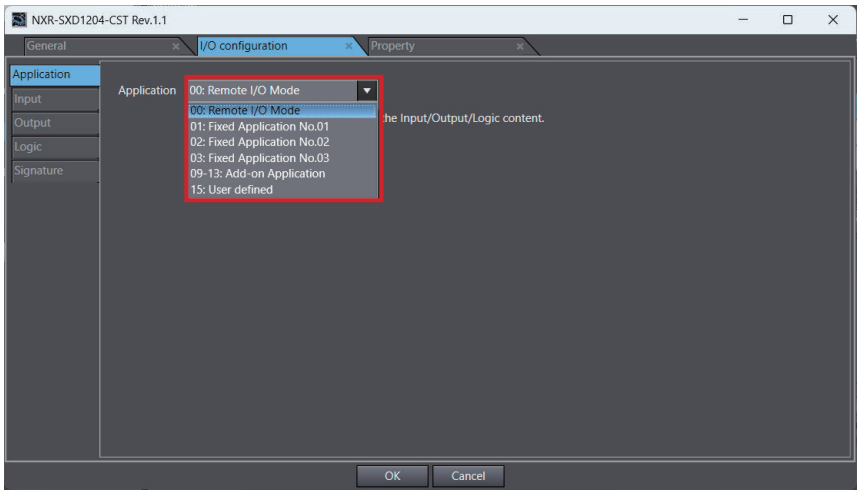
3 Select the **Application** tab.



4 Select the safety application to use.

The safety control system and the safety applications correspond as follows.

Safety Control System	Safety Application
Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open) on page 1-8 *Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI)* on page 1-9	00: Remote I/O Mode
Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application on page 1-10	01: Fixed Application No.01 02: Fixed Application No.02 03: Fixed Application No.03
Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User on page 1-11	15: User defined
Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User on page 1-12	09-13: Add-on Application



5 When setting is complete, click the **OK** button.

7-9-3 Safety I/O Functions Settings

Configure the I/O configuration settings for the Safety I/O Block in a project file of Sysmac Studio. Refer to *7-5 Safety Input Functions Settings* on page 7-44 and *7-6 Setting Safety Output Functions* on page 7-50 for details.

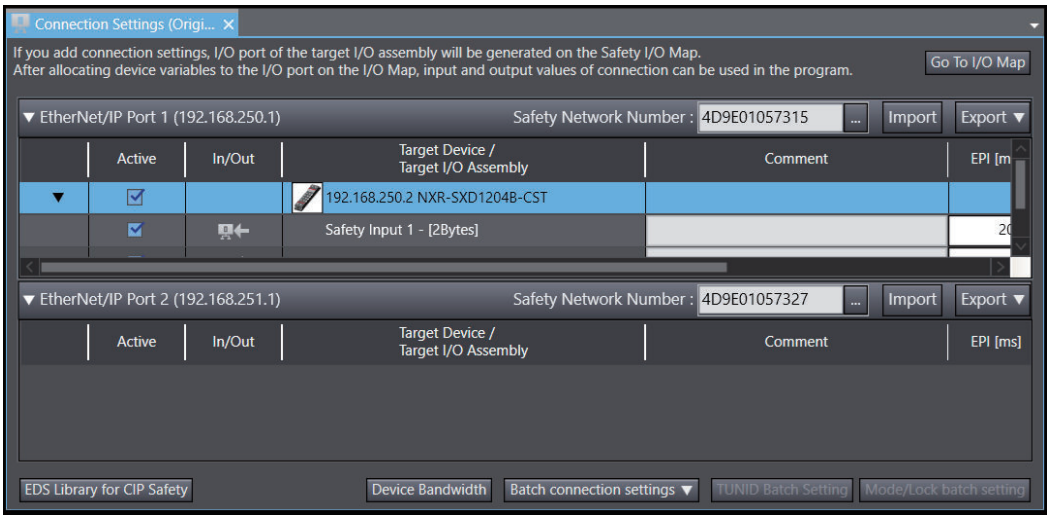
7-9-4 Logic Function Settings

Configure the settings for the logic and power-on mode of the Safety I/O Block in a project file of Sysmac Studio. This step is required only if the safety control system is a *configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by user*. Refer to *7-7 Logic Function Settings* on page 7-53 for details.

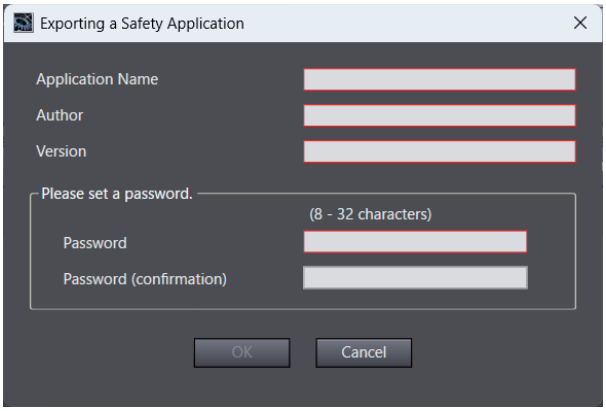
7-9-5 Exporting a Safety Application File

The procedure to export a safety application file is as follows.

1 In Sysmac Studio, go to **Configurations and Setup** - **Communications** - **Safety** - **EtherNet/IP Safety Connection Settings** of the Safety CPU Unit, and select **Connection Settings (Originator)**.
The **Connection Settings (Originator)** tab page is displayed.



2 Right-click the Safety I/O Block and select **Exporting a Safety Application**.
The **Exporting a Safety Application** screen of the Safety I/O Block is displayed.

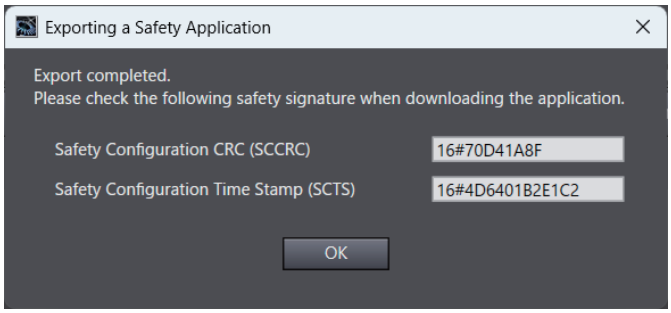


3 Enter the application name, creator, version, safety application file password, and safety application file password (for confirmation), and click the **OK** button.
The character limit for each setting item is as follows.

Setting item	Character limit
Application name	Up to 32 single-byte alphanumeric characters
Creator	Up to 32 single-byte alphanumeric characters
Version	Up to 32 single-byte alphanumeric characters
Safety application file password	From 8 to 32 single-byte alphanumeric characters
Safety application file password (for confirmation)	

A safety application file password is a password set for each safety application file for using the safety application. It differs from the safety password.

4 Specify the save location of the file to export, and save the file.
The export complete screen is displayed.



5 Check the safety signature, and click the **OK** button.
Exporting is executed, and the safety application file is saved.

Precautions for Correct Use

Keep a record of the entered application name, creator, version, safety application file password, and safety signatures (SCCRC and SCTS). They will be used when setting the safety application in the safety application file.

Safety Application File Password Specifications

The conditions for the text string that can be used for the safety application file password are as follows.

Item	Description
Number of characters	8 to 32
Usable characters	A to Z, a to z, 0 to 9, ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ single-byte space

Precautions for Correct Use

- To reduce the security risk, use a combination of alphabet letters, symbols, and numbers for the safety application file password that you set.
- The safety application file password can be neither displayed nor initialized. Manage the safety application file password in case you forget it.

Attribute Information Specifications

The following table shows the attribute information for an add-on application created by a user.

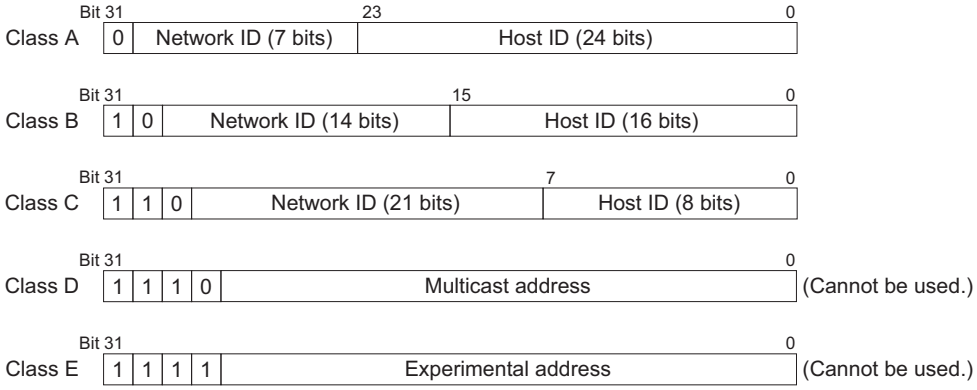
Item	Usable characters	Number of characters
Application name	Single-byte alphanumeric characters	1 to 32
Creator	Single-byte alphanumeric characters	1 to 32
Version	Single-byte alphanumeric characters	1 to 32

7-10 Setting IP Addresses

This section describes the IP address configuration and how to set IP addresses.

7-10-1 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 net ID is an address used for identifying an Ethernet network. The host ID is an address used for identifying a host (node).
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 4 sections of 8 bits each. IP addresses are represented by the decimal equivalent of each of the 4 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.

Assigning IP Addresses

IP addresses must be assigned to nodes in such a way that there are no duplications within the network or across multiple networks.

CIDR Function

CIDR stands for Classless Inter-Domain Routing, which is a function to assigns IP addresses without using classes.

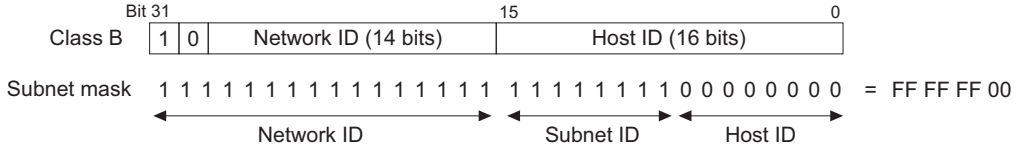
With class-based IP addresses, the network ID part and host ID part are separated into predetermined block units, which has the disadvantage of not efficiently allocating IP address space (number of hosts).
Since CIDR does not use classes, it can separate the network ID part and host ID part by any IP address space, allowing efficient use of IP address space (number of hosts).
For example, even if Class C (192.168....) is used, setting a netmask using CIDR enables building a horizontally distributed network that exceeds 254 nodes.

Subnet mask range
192.0.0.0 to 255.255.255.252

Subnet Mask

When many nodes are connected to one network, network operation and management becomes challenging. In such a case, it is convenient to build a system by dividing one network into multiple subnetworks.
The system operates as multiple networks internally, but appears as a single network from the outside.
To implement this type of operation, the host ID part of the IP address is divided into two parts: a subnet ID part and a host ID part.
The information for identifying this subnet ID part is a subnet mask.
A subnet mask is a bit mask where the network ID part and subnet ID part are set to "1", and the host ID part is set to "0".

(Example) For a Class B IP address using 8 bits for the subnet ID, the subnet mask would be as follows:



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). This allows you to set the subnet mask to 192.0.0.0 to 255.255.255.252.

Additional Information

If you will not use subnetworks, mask all of the host ID part of the IP address with "0".
Set the corresponding subnet mask value below depending on the class (Class A to Class C) of the IP address.

Class	Subnet mask value
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Network Address

The information for identifying each network using subnet masks includes network addresses.
Network addresses indicate whether certain multiple nodes belong to the same network.
A network address is calculated by performing a logical AND on the node's IP address and subnet mask.

The following shows an example of calculating network addresses.

If 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 address of each node is calculated as shown in the following tables.

- The calculation for the network address of node 1 is as follows.

Item	Decimal number 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

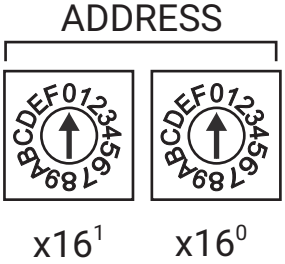
- The calculation for the network address of node 2 is as follows.

Item	Decimal number notation	Binary notation
IP address	192.168.245.30	11000000.10101000.11110101.00011110
Subnet mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

From the above, you can determine that node 1 and node 2 belong to the same network because they have the same network address.

7-10-2 Selecting the Method to Set the IP Address Using the Rotary Switches

You can select the method to set the IP address using the rotary switches of the Safety I/O Block, and then set the IP address itself.
Use the ADDRESS rotary switches.



Select either software setting or hardware setting by configuring the setting value with the rotary switches as follows. Set the IP address using the selected method.

Setting name	Set value (hex)	IP address setting method
Software setting	00	In Sysmac Studio or the Web UI, you select from the following methods to configure the setting. • Setting of fixed IP address • Obtaining from DHCP server The factory default is 192.168.250.1. Refer to *7-10-3 Setting by Sysmac Studio* on page 7-74 for how to configure the setting using Sysmac Studio. Refer to *7-10-4 Setting by Web UI* on page 7-76 for how to configure the setting using the Web UI.
Hardware setting*2	01 to FE	192.168.250.□*1
	FF	Obtain the IP address from the DHCP server.

***1.** "□" is the setting value of the rotary switches.

***2.** If you perform a restart after setting the rotary switches, the setting is applied.

Precautions for Correct Use

When the IP address is obtained from a DHCP server, the obtained IP address is cleared when the power is turned OFF or the unit is restarted, even if the acquisition is successful. Therefore, a DHCP server will be required for subsequent operations.

Additional Information

The recommended DHCP server is DHCP Server 3.06 or later.

7-10-3 Setting by Sysmac Studio

The TCP/IP Settings screen of Sysmac Studio is used to configure the IP address settings and LINK settings of the corresponding Unit.

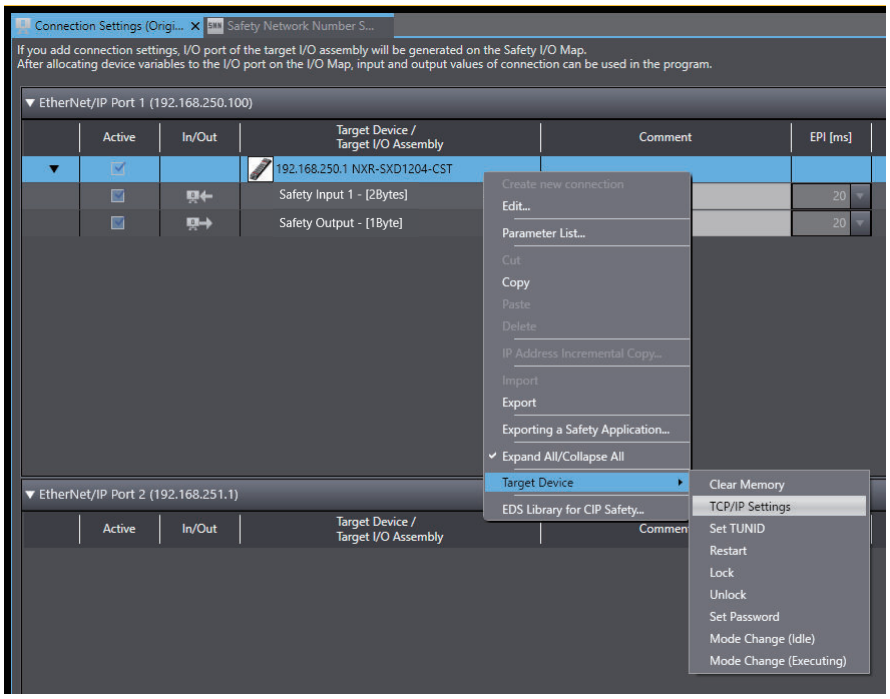
Precautions for Correct Use

The Safety I/O Block does not support the following functions in these TCP/IP settings.

- **IP Adress**, select **Obtain from BOOTP Server**
- **DNS**

1 Set the setting value of the ADDRESS rotary switch to"00" and then start up the Unit.
At initial startup, the value is 192.168.250.1.

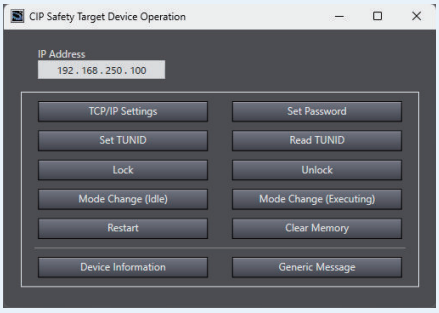
2 Right-click the Safety I/O Block on the settings screen for the connection settings (originator), and then click **Target Device** - **TCP/IP Settings** from the displayed menu.



Additional Information

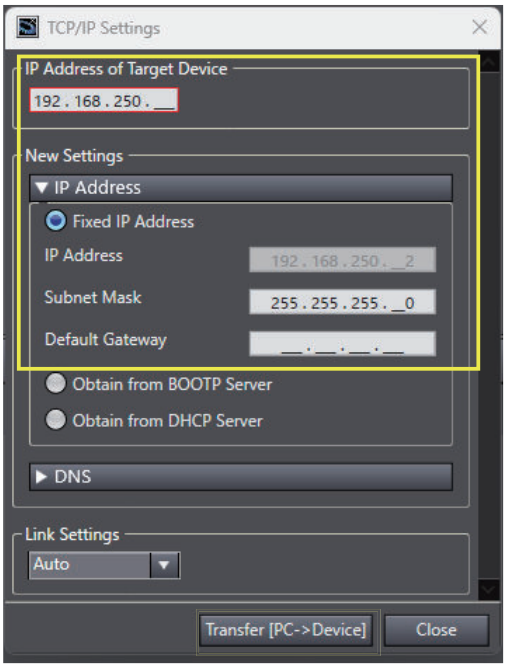
Execution from the CIP Safety Target Device Operation window is also possible.

1) Select Safety PLC (Initial display new_SafetyCPU_0) in the Multiview Explorer, and select **CIP Safety Target Device Operation** in the **Tools** menu from the menu bar at the top of the screen.
2) Enter the IP address that is currently set for the **IP Address** in Safety I/O Block, and click the **TCP/IP Settings** button.

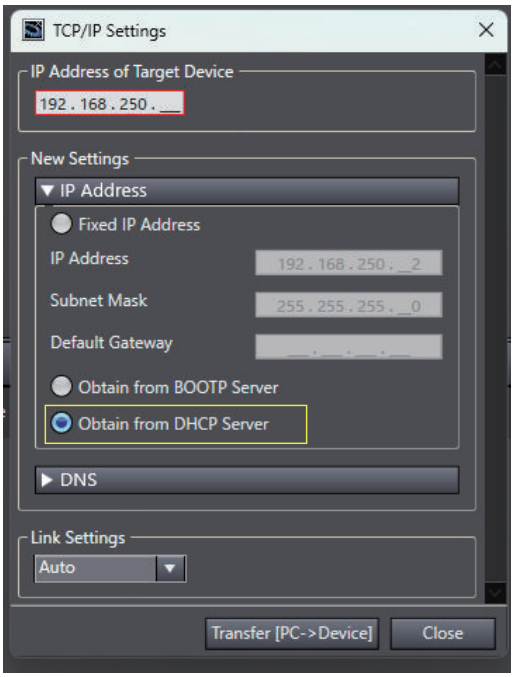


3 Set the IP address by using a static IP address or obtaining an IP address from a DHCP server.

a) When using a static IP address, select the **Static IP address settings** option and enter the **IP address** settings.



b) When obtaining an IP address from a DHCP server, select the **Obtain from DHCP server** option.



4 Set **LINK settings**.
The selection options are as follows.

- Auto
- 10 Mbps Half Duplex
- 10 Mbps Full Duplex
- 100 Mbps Half Duplex
- 100 Mbps Full Duplex

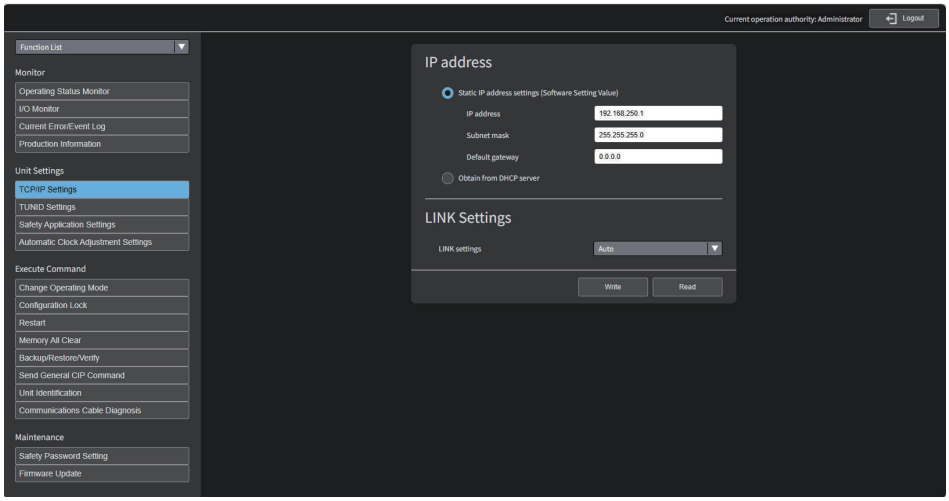
5 Click the **Transfer [PC->Device]** button.

The setting values are transferred to the Safety I/O Block.

6 To enable the transferred setting values, cycle the power supply or perform a restart.

7-10-4 Setting by Web UI

The TCP/IP Settings screen of the Web UI is used to configure the IP address settings and LINK settings of the corresponding Unit.
The settings on this screen can be configured only by a user with the administrator authority.



The setting procedure is as follows.

1 Select the method to determine the IP address from **Static IP address settings** and **Obtain from DHCP server**.

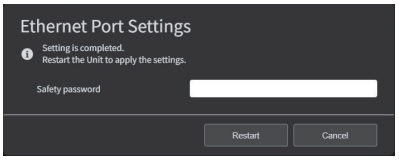
2 If **Static IP address settings** is selected, enter the values in **IP address**, **Subnet mask**, and **Default gateway**.
If you click the **Read** button, you can check the current IP address, subnet mask, and default gateway.

3 Set **LINK settings**.
The selection options are as follows.

- Auto
- 100 Mbps Half Duplex
- 100 Mbps Full Duplex

If you click the **Read** button, you can check the current LINK settings.

4 Click the **Write** button.
The configured settings are transferred to the corresponding Unit. If the transfer is successful, the following message is displayed.



5 Set the setting value of the ADDRESS rotary switch to 00"00".

6 Enter the safety password, and click the **Restart** button.
The Safety I/O Block restarts, and the IP address settings and LINK settings are reflected.

7-11 TUNID Settings

This section describes the TUNID setting procedure of the Safety I/O Block.

7-11-1 Purpose of TUNID

The TUNID is used to identify a specific safety connection in CIP Safety communications.
A TUNID is a value totaling 10 bytes, consisting of a 6-byte Safety Network Number (SNN) and a 4-byte Node ID.
A safety network number is a number to identify multiple safety networks, and a node ID is a number to identify each device in an EtherNet/IP network.

7-11-2 TUNID Setting Procedure

The TUNID setting has a method that uses Sysmac Studio and a method that uses the Web UI.

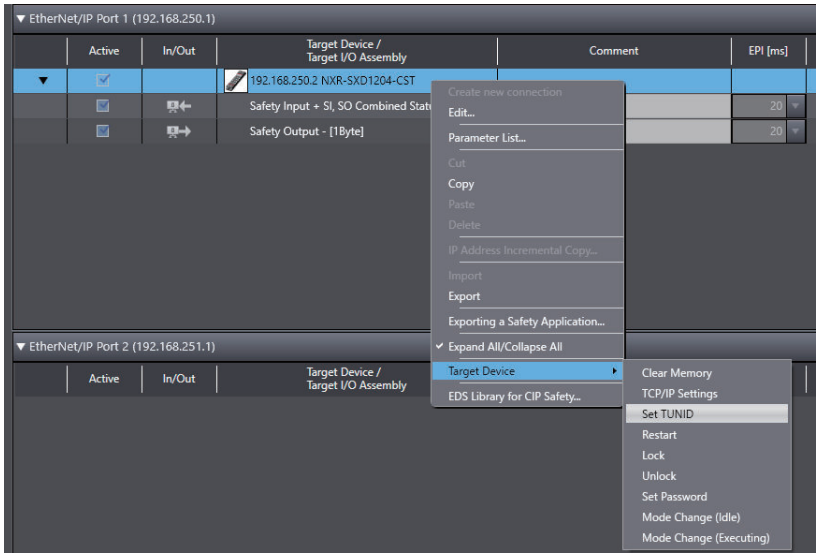
Setting by Sysmac Studio

There are two methods to set the TUNID for Units: individual setting and batch setting.

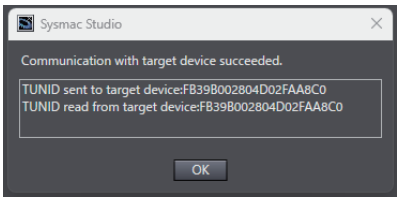
● TUNID Setting (Individually)

1 Go online with the Safety CPU Unit.

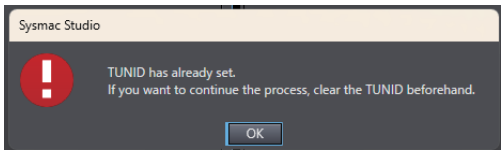
2 Select the Safety I/O Block on the Connection Settings (Originator) Edit Pane, then right-click it and select **Target Device** - **Set TUNID**.



3 If TUNID setting is successful, click the **OK** button.



If the TUNID is already set, the following screen is displayed.



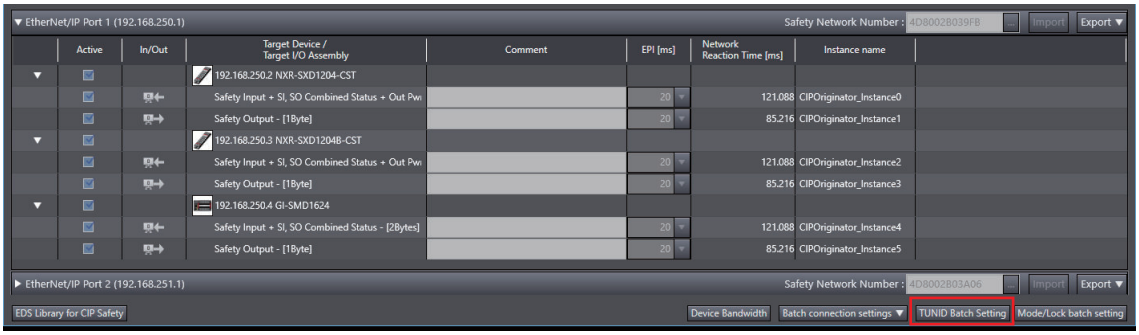
To set a new TUNID, use the clear all memory function to delete the TUNID from the Safety I/O Block. Refer to *8-2 Clear All Memory Function* on page 8-4 for details on the clear all memory function.

● Setting the TUNID (Batch Setting)

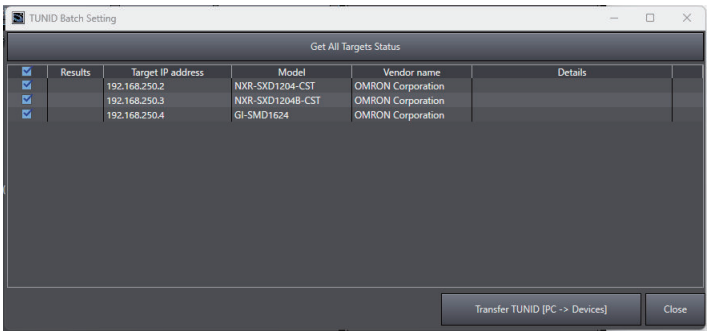
You can configure the TUNID setting for all targets registered in the Connection Settings (Originator) Edit Pane at once.

1 Go online with the Safety CPU Unit.

2 Click the **TUNID Batch Setting** button at the bottom right of the Connection Settings (Originator) Edit Pane.

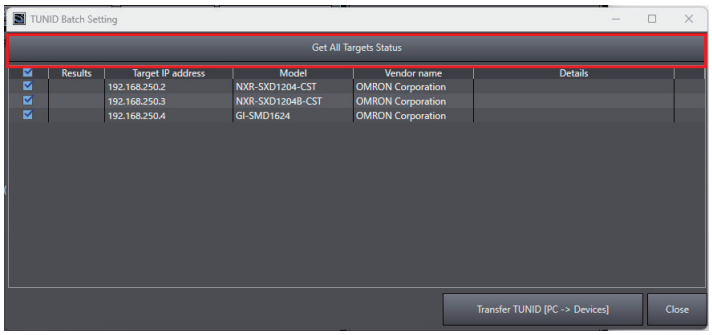


The TUNID Batch Setting window is displayed.



3 Click the **Get All Targets Status** button.

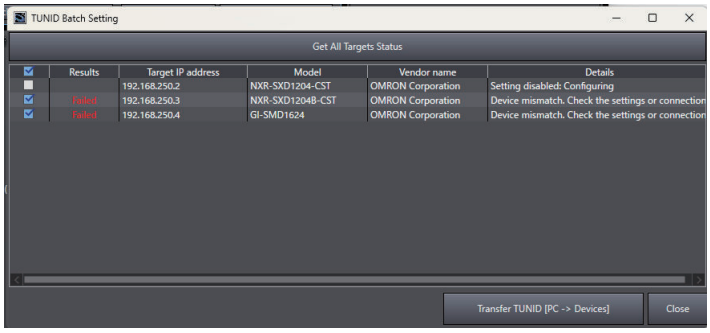
The Unit gets the status from the targets displayed in the list, and determines whether the targets are currently in a state in which the TUNID is settable.



Additional Information

A target can be excluded from the status acquisition targets by clearing the check box.

4 Check the acquired status.
If the status is that the TUNID is not settable, the check box is cleared.

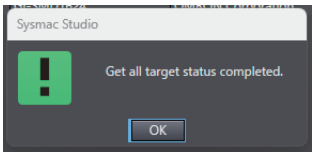


Furthermore, the Details column displays the status acquisition result as shown below.

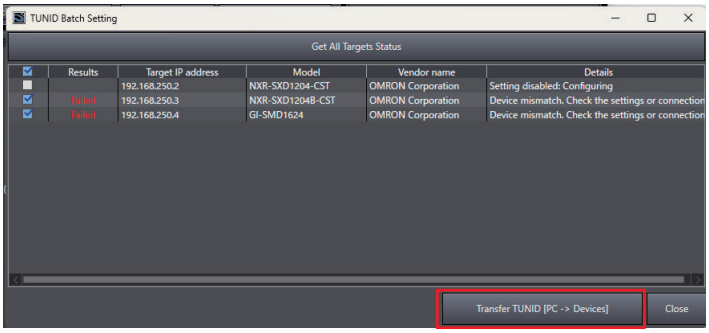
- When the TUNID is settable
  Setting enabled: Waiting for TUNID
- When the TUNID is not settable
  Setting disabled: The status of that device is displayed.
  The status information is defined in the specifications of CIP Safety.
- When communication with the device was not possible
  Communicate with target failed.

If **Communicate with target failed.** is displayed, check the communications cable connection state, the IP address settings of the target, etc.
Furthermore, if Setting disabled is displayed, use the clear all memory function to change the status of the target according to the conditions.

When the status acquisition is completed, the display is as follows.



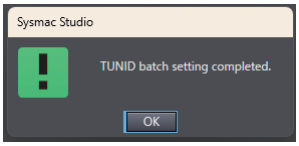
5 Click the **Transfer TUNID [PC -> Devices]** button.
TUNID batch setting starts.



Additional Information

You can also edit the selection status of the check box at this time.

6 Check the result of TUNID batch setting.



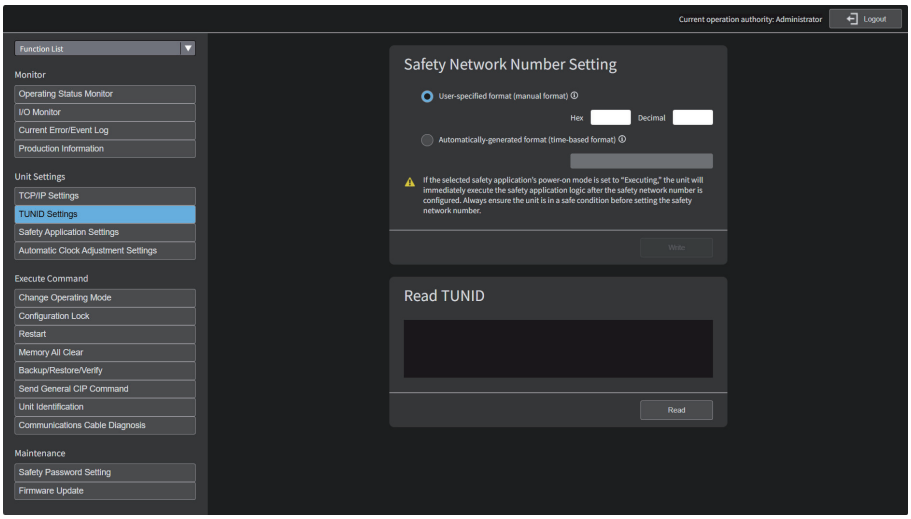
The TUNID setting result is displayed in the **Result** column.

Result column	Description
Successful	Setting of TUNID was executed correctly.
Failed	Setting of TUNID was not executed correctly.

Review the communications environment, or if the TUNID has already been set, clear the TUNID with the clear all memory function and then set the TUNID again.

Setting by Web UI

On the TUNID Settings screen of the Web UI, the TUNID of the corresponding Unit is set by confirming the safety network number.
The settings on this screen can be configured only by a user with the administrator authority.



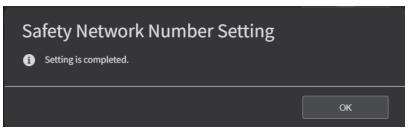
The setting procedure is as follows.

1 Select the determination method for the safety network number from **User-specified format (manual format)** and **Automatically-generated format (time-based format)**.
The meaning and specifications of each determination method are as follows. Set the safety network number of the network with the Safety I/O Block connected using any one of these methods.

Safety network number determination method	Meaning	Specifications
User-specified format (manual format)	The user decides and enters a safety network number that does not duplicate that of another system.	**Hex** The number of digits is 4, and the characters that can be entered are 0 to 9 and A to F. **Decimal** The number of digits is 4, and the characters that can be entered are 0 to 9.
Automatically-generated format (time-based format)	The user enters a safety network number generated automatically by the safety network configuration tool of the CIP Safety originator in advance.	The number of digits is 4, and the characters that can be entered are 0 to 9 and A to F.

2 Enter the safety network number according to the selected determination method for the safety network number.
If you click the **Read** button, you can check the current TUNID, safety network number, and node ID.

3 Click the **Write** button.
The configured settings are transferred to the corresponding Unit. If the transfer is successful, the following message is displayed.



4 Click the **OK** button.

7-12 Selecting the Safety Application

A safety application is selected with SETTING rotary switches SW1 and SW2.

Safety application type	SETTING rotary switches SW1 and SW2
Remote I/O mode application	Set both to *0*.
Fixed application	Set both to number *1-3* of the fixed application to be used.
User-defined application	Set both to *F*.
Add-on application	Set both to number *9-D* of the fixed application to be used.

7-13 Restart

Restart the Safety I/O Block.

7-13-1 Purpose of Restart

The purpose of a restart is to enable the settings or changes for the IP address and other setting information.

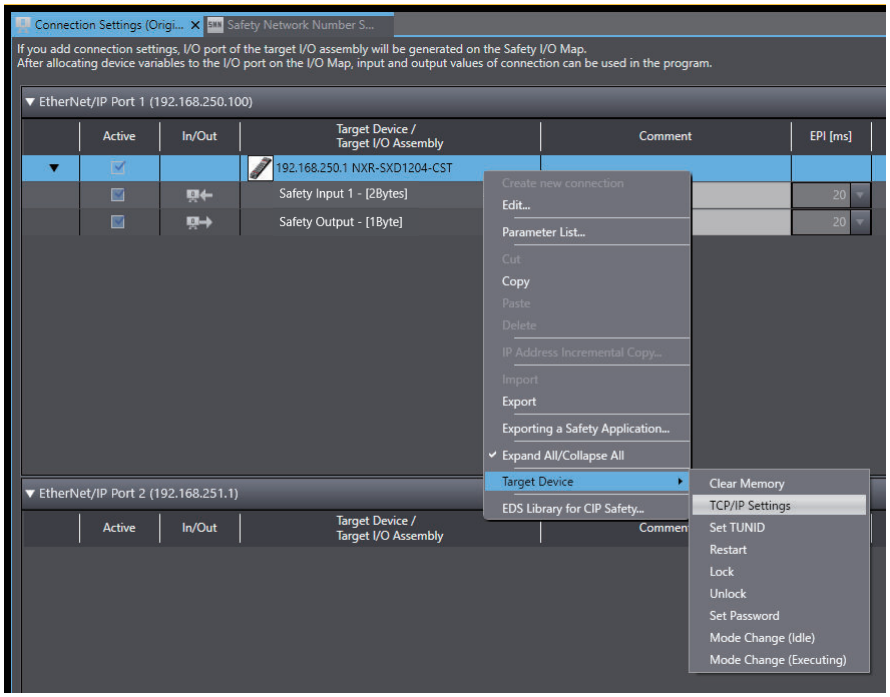
7-13-2 Procedure for Using Restart

For restating, there is a method that uses Sysmac Studio and a method that uses the Web UI.

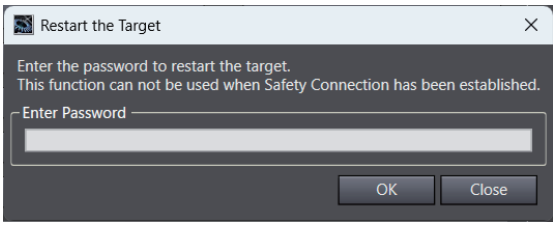
Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

1 Right-click the Safety I/O Block on the settings screen for the connection settings (originator), and then click **Target Device** from the displayed menu.



2 Click **Restart**.
The following screen is displayed.

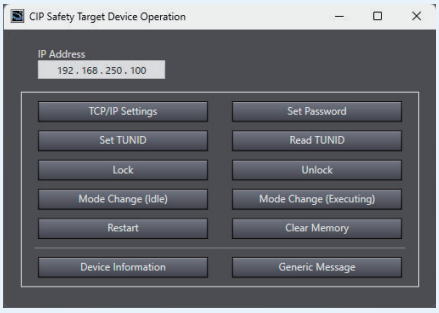


3 Enter the safety password, and click the **OK** button.
A restart is performed.

Additional Information

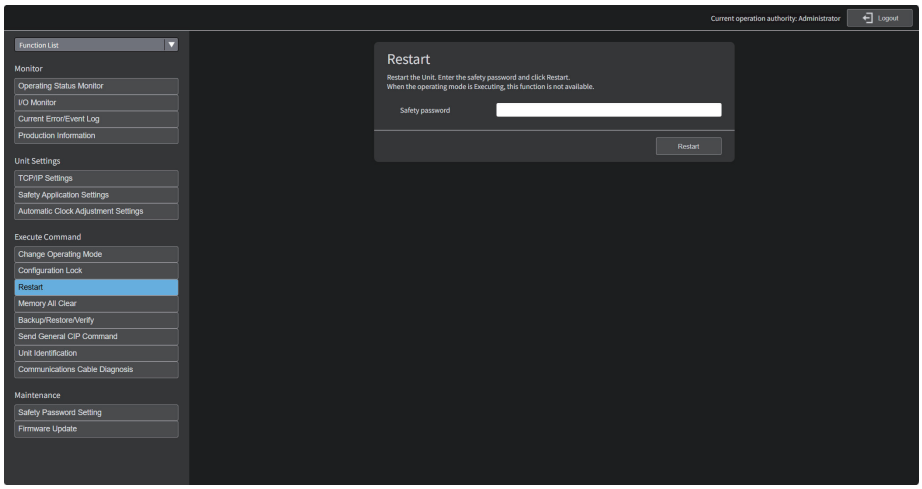
Execution from the CIP Safety Target Device Operation window is also possible.

1) Select Safety PLC (Initial display new_SafetyCPU_0) in the Multiview Explorer, and select **CIP Safety Target Device Operation** in the **Tools** menu from the menu bar at the top of the screen.
2) Enter the IP address that is set for the **IP Address** in Safety I/O Block.



Procedure Using the Web UI

Restart the Safety I/O Block on the Restart screen of the Web UI.
The settings on this screen can be configured only by a user with the administrator authority.



The setting procedure is as follows.

1 Enter the safety password, and click the **Restart** button.
The restart is executed and the following screen is displayed.



2 Click the **OK** button.
Logging out from the Web UI is performed and the Login screen is displayed.

7-14 Configuration

This section describes the procedure to configure the safety controller and Safety I/O Block.
Refer to *NX-series Safety Control Unit/Communication Control Unit User's Manual (Cat. No. Z395)* for details on the configuration of the safety controller.
Use a safety application file for the Safety I/O Block, and configure the settings on the Safety Application Settings screen of the Web UI.

7-14-1 Configuring the Safety Controller

Configure the safety controller.

1 Transfer a remote I/O mode application created in Sysmac Studio to the safety controller.
If the open type of the Safety I/O Block is *type1 Safety open*, the Safety I/O Block is configured by the safety controller when a Type1 Safety Open connection is established between the safety controller and Safety I/O Block.

7-14-2 Configuration of Safety I/O Block

This section explains the steps for setting up a safety application using the safety application file. Safety applications are used by assigning rotary switch numbers. If you have mistakenly downloaded the safety application file, remove the safety applicationSafety I/O Block from the rotary switch number.

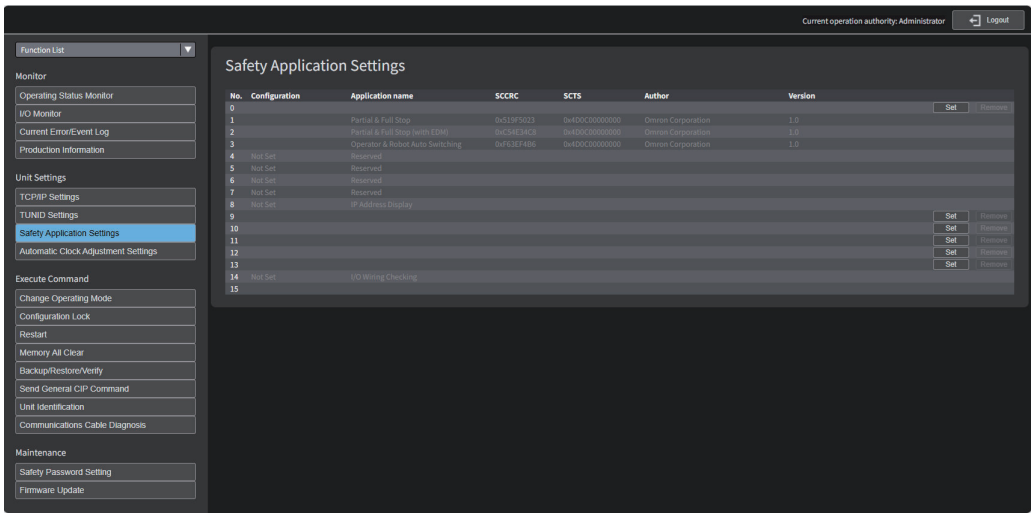
Configuring the Safety Application Selected Using the Rotary Switches

The procedure to configure the safety application selected using the rotary switches is as follows.

1 Prepare a safety application file created in Sysmac Studio.

2 Connect the PC to the EtherNet/IP port on the Safety I/O Block, and log in to the Web UI.

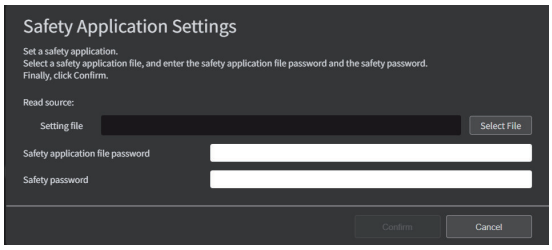
3 Display the Safety Application Settings screen of the Web UI. The settings on this screen can be configured only by a user with the administrator authority.



Precautions for Correct Use

A safety application file for a remote I/O mode application cannot be configured as an add-on application. Furthermore, a safety application file for an add-on application cannot be configured as a remote I/O mode application.

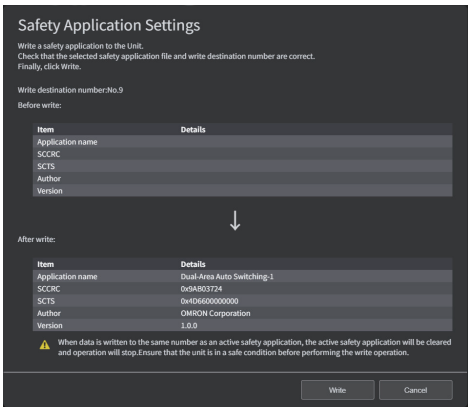
4 Click the **Set** button of the rotary switch number to which to assign the add-on application.
The following message is displayed.



5 Click the **Select File** button, and select the safety application file on the PC.
The selected safety application file is displayed in the **Setting file** field.

6 Enter the safety application file password and safety password.

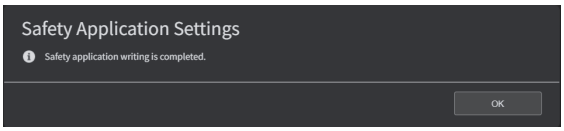
7 Click the **Confirm** button.
The following message is displayed.



Precautions for Correct Use

Check that the SCCRC and SCTS displayed in the Safety Application Settings screen are as intended.

8 Check the information displayed for the read source and write destination, and click the **Write** button.
The settings are reflected in the Safety I/O Block, and the following message is displayed.

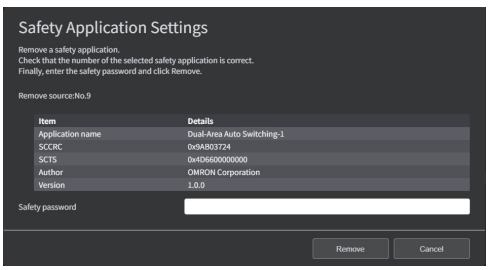


9 To operate the add-on application, turn the power supply OFF, set the rotary switches, and turn the power supply ON.

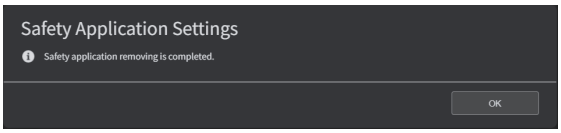
Removing Add-on Applications from Rotary Switch Numbers

The procedure to remove an add-on application from a rotary switch number is as follows.

1 Click the **Remove** button of the rotary switch number from which to remove the add-on application on the Safety Application Settings screen of the Web UI.
The following message is displayed.



2 Check the information displayed for the deletion source, enter the safety password, and click the **Remove** button.
The add-on application is removed from the rotary switch number, and the following message is displayed.


Safety Application Settings
Safety application removing is completed.
OK

7-15 Setting the Automatic Clock Adjustment

Automatic clock adjustment is for adjusting the time of the corresponding Unit.

7-15-1 Purpose of Automatic Clock Adjustment

The purpose of the automatic clock adjustment is to ensure that the correct dates and times are recorded in event logs.
This function adjusts the clock information of the Safety I/O Block automatically. Recording the exact time allows you to know the precise timing of error occurrence, helping facilitate a quick response and cause analysis.

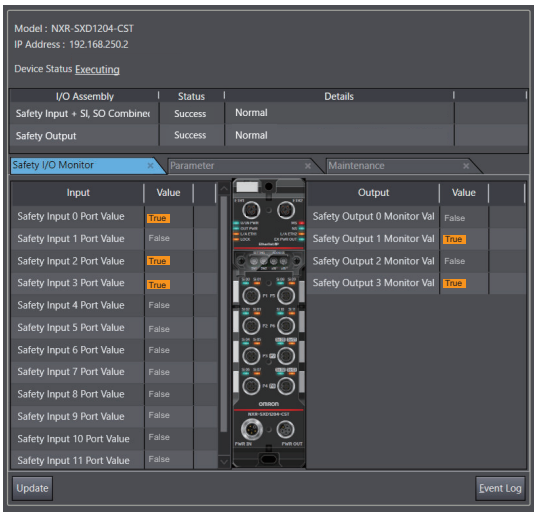
7-15-2 Procedure for Using the Automatic Clock Adjustment

The automatic clock adjustment has a method that uses Sysmac Studio, a method that uses the Web UI, and a method that uses explicit message communications.

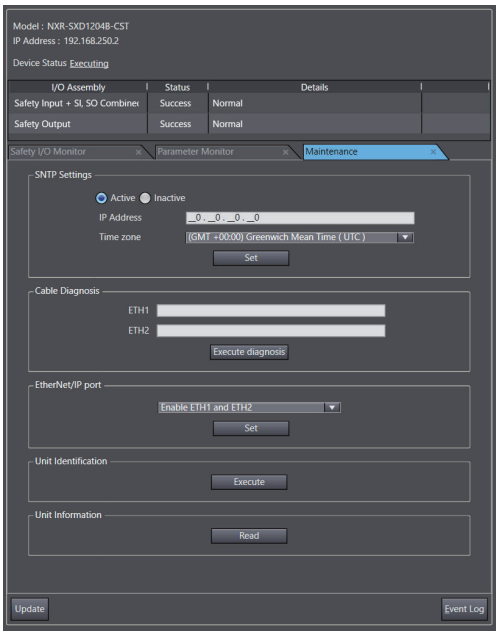
Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

1 Select Safety I/O Block on the CIP Safety Monitor screen of Sysmac Studio.
The following screen is displayed.



2 Select the **Maintenance** tab.
The following screen is displayed.



3 Select the **Active** radio button of **SNTP Settings**.

4 Set the IP address of the NTP server or SNTP server in **IP Address** of **SNTP Settings**.

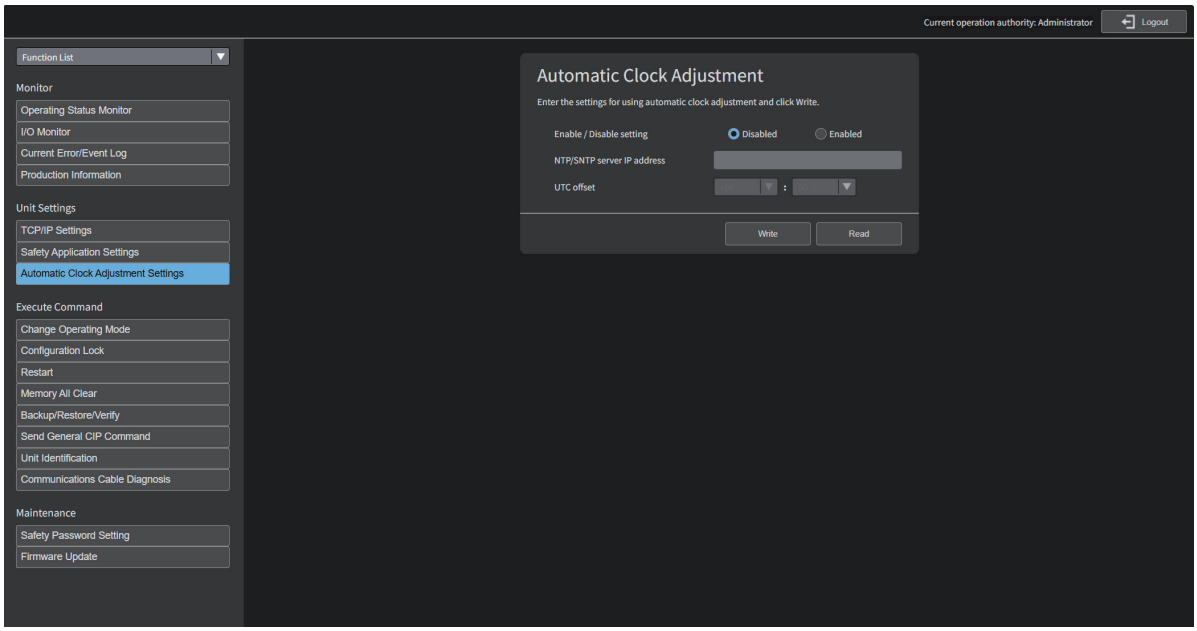
5 Select the timezone to set in **Time zone**.

6 Click **Set**.

7 Restart the Unit.
The date and time obtained from the NTP server or SNTP server are set for the clock built into the Unit.

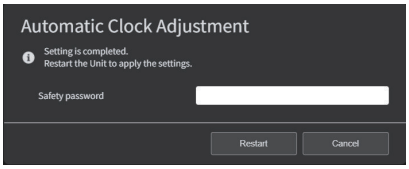
Procedure Using the Web UI

The Automatic Clock Adjustment Settings screen of the Web UI is used to adjust the time of the Safety I/O Block.
The settings on this screen can be configured only by a user with the administrator authority.



The setting procedure is as follows.

1. Set **Enable/Disable setting** to **Enabled**.
2. Enter the IP address of the NTP/SNTP server in **NTP/SNTP server IP address**. Set the time difference from Coordinated Universal Time (UTC) in **UTC offset**.
3. Click the **Write** button.
   The configured settings are transferred to the corresponding Unit. If the transfer is successful, the following message is displayed.



4. Enter the safety password, and click the **Restart** button.
   The Safety I/O Block restarts, and the time settings are reflected.

Procedure Using Explicit Message Communications

The send commands for the IP address setting and timezone setting of the NTP/SNTP server are as follows.

Implementation details	Send command item	Send command value
IP address setting of SNTP server	Service code	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01 hex (instance specification)
	Attribute ID	12 (SNTP Server IP Address)
	Service data	IP address of SNTP server

Implementation details	Send command item	Send command value
Offset in minutes for correcting present time	Service code	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01 hex (instance specification)
	Attribute ID	102 (Time Zone Offset - Minutes)
	Service data	-720 to 840

Refer to *Explicit Message Server Function* on page 6-7 for the method to access CIP objects through an explicit message.

7-15-3 Details on Automatic Clock Adjustment

The time information of the Unit is cleared by a power interruption.
Automatic adjustment of the clock information is performed periodically, but the adjustment timing cannot be set arbitrarily.
Daylight savings time is not supported.

If the connection with the NTP server or SNTP server fails, an *NTP Server Connection Error* (84040000 hex) event occurs. Refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details.

Precautions for Correct Use

- If the automatic clock adjustment is not used, the internal clock of the Unit is set to 00:00:00, January 1, 1972 when the power is turned ON, and timekeeping proceeds from that point.
- To reduce the security risks, always execute automatic clock adjustment.

7-16 Changing the Operating Mode

Change the operating mode of the Safety I/O Block to *Idle* or *Executing*.
Refer to *6-8 Operating Modes* on page 6-47 for details on operating modes.

7-16-1 Procedure for Using Change Operating Mode

Change operating mode has a method to use Sysmac Studio and a method to use the Web UI.

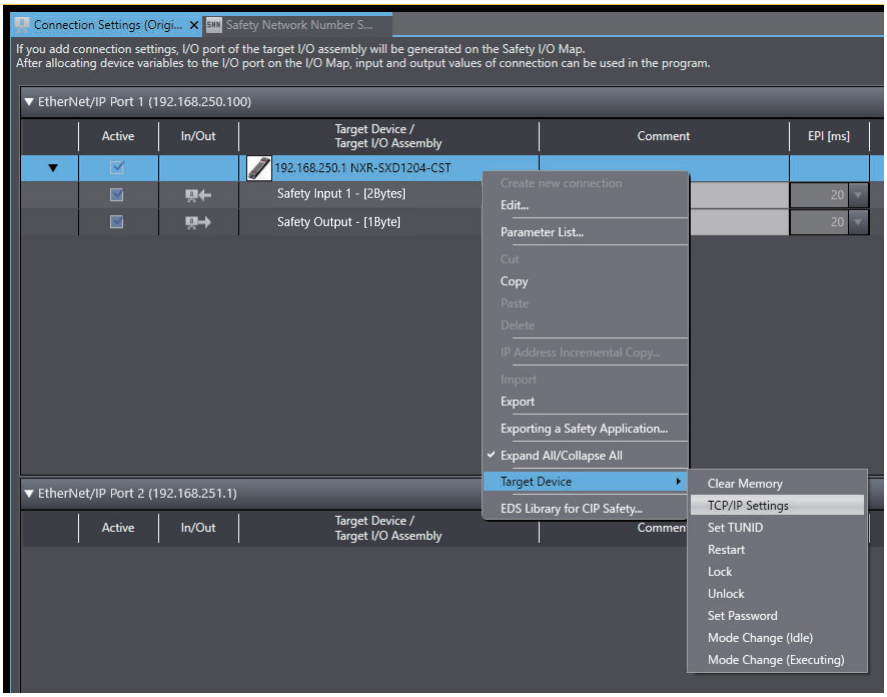
Procedure Using Sysmac Studio

In Sysmac Studio, there is a method to change operating mode for Units individually, and a method to change the operating mode for multiple Units registered to the CIP Safety Connection Setting screen at once.

● Changing the Mode on an Individual Unit Basis

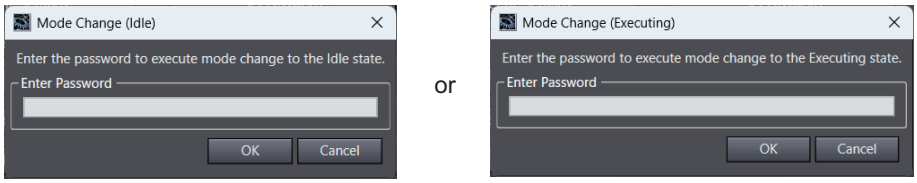
The procedure to change the mode on an individual unit basis is as follows.

1 Right-click the Safety I/O Block on the settings screen for the connection settings (originator), and then click **Target Device** from the displayed menu.



2 Click **Mode Change (Idle)** or **Mode Change (Executing)**.

3 The safety password input window is displayed. Enter the safety password.

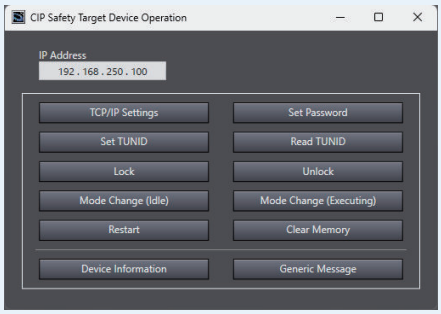


4 Click the **OK** button.
The operating mode changes.

Additional Information

Execution from the CIP Safety Target Device Operation window is also possible.

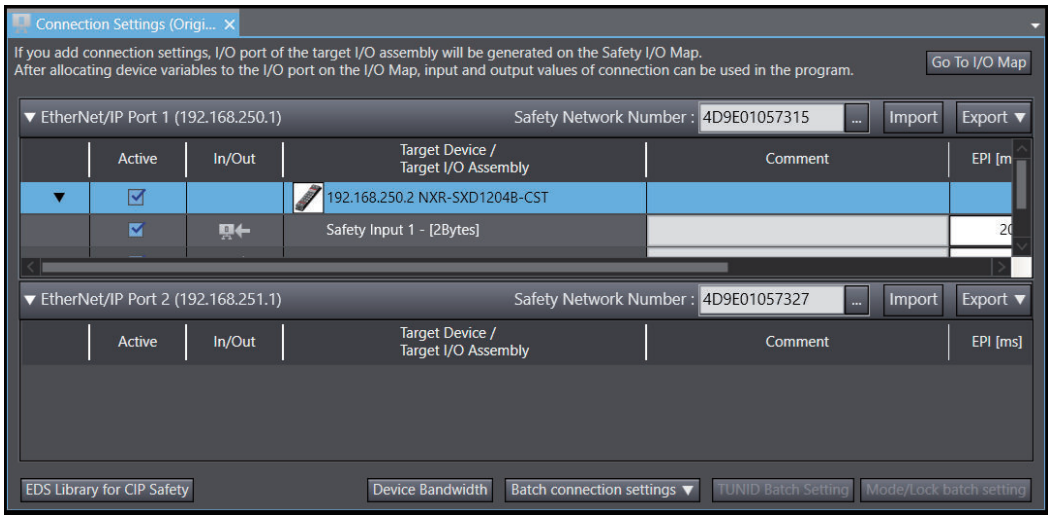
1) Select Safety PLC (Initial display new_SafetyCPU_0) in the Multiview Explorer, and select **CIP Safety Target Device Operation** in the **Tools** menu from the menu bar at the top of the screen.
2) Enter the IP address that is set for the **IP Address** in Safety I/O Block.



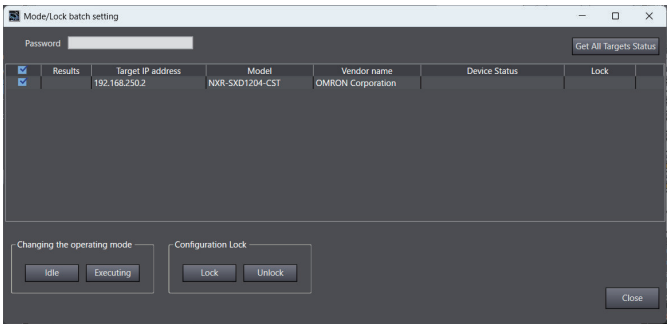
● Batch Changing the Operating Mode of Multiple Units

The procedure to use batch changing of the operating mode of multiple Units is as follows.

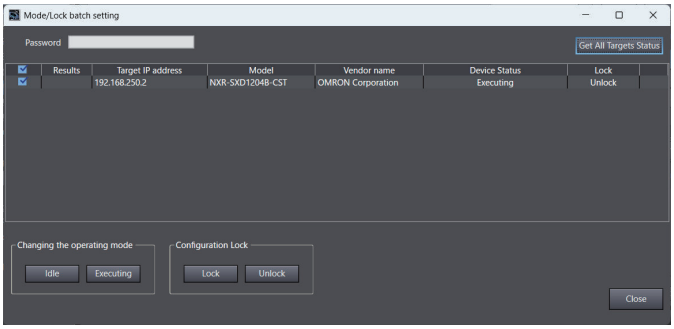
1 Display the settings screen for the connection settings (originator) in Sysmac Studio.



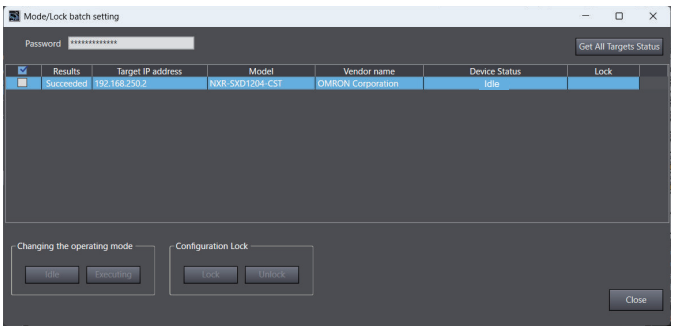
2 Click the **Mode/Lock batch setting** button.
The following screen is displayed.



3 Click the **Get All Targets Status** button.
The device status of each target is displayed in the **Device status** column as shown below. *Device status* has the same meaning as *operating mode*.

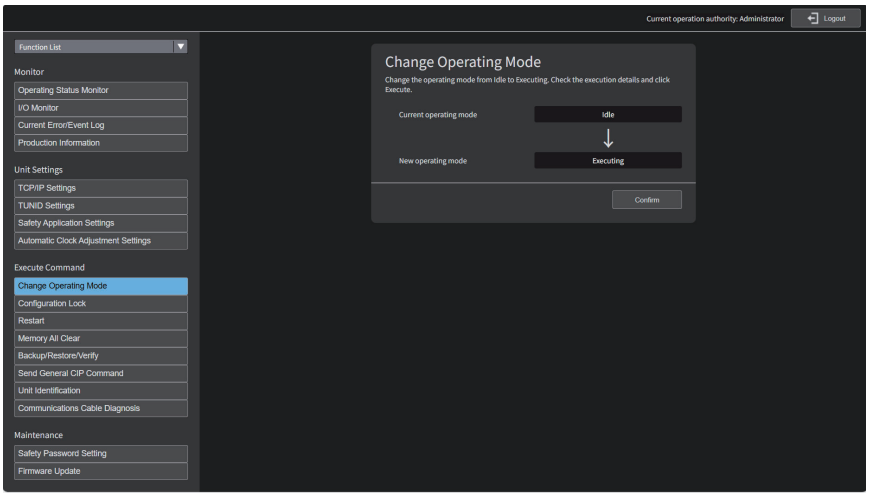


4 Enter the safety password, and click the **Idle** button or **Executing** button in **Changing the operating mode**.
The operating mode of multiple Units changes. Whether changing the operating mode of each target was a success or failure is displayed in the **Results** column as shown below.



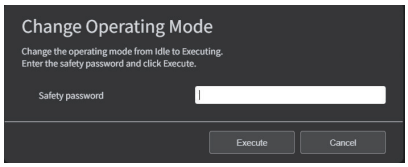
Procedure Using the Web UI

The Change Operating Mode screen of the Web UI is used to change the operating mode of the Safety I/O Block.
The settings on this screen can be configured only by a user with the administrator authority.

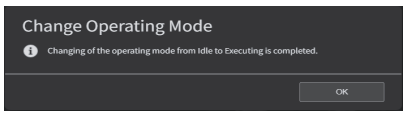


The setting procedure is as follows.

1 The **Current operating mode** field displays the current operating mode, and the **New operating mode** field displays the new operating mode. Click the **Confirm** button.
The following message is displayed.



2 Enter the safety password, and click the **Execute** button.
The operating mode changes, and the following message is displayed.



3 Click the **OK** button.

7-17 Configuration Lock

The configuration lock is used to lock and unlock the configuration of the Safety I/O Block.
It can also simultaneously execute configuration locking of multiple Safety I/O Block registered on the CIP Safety Connection Settings screen.

7-17-1 Purpose of Configuration Lock

The purpose of the configuration lock is to prevent setting data related to the safety of the Safety I/O Block and safety applications that are executed from being changed unintentionally. Executing the configuration lock makes all setting data unchangeable unless the safety password is entered.

7-17-2 Procedure for Using the Configuration Lock

The configuration lock has a method that uses Sysmac Studio and a method that uses the Web UI.

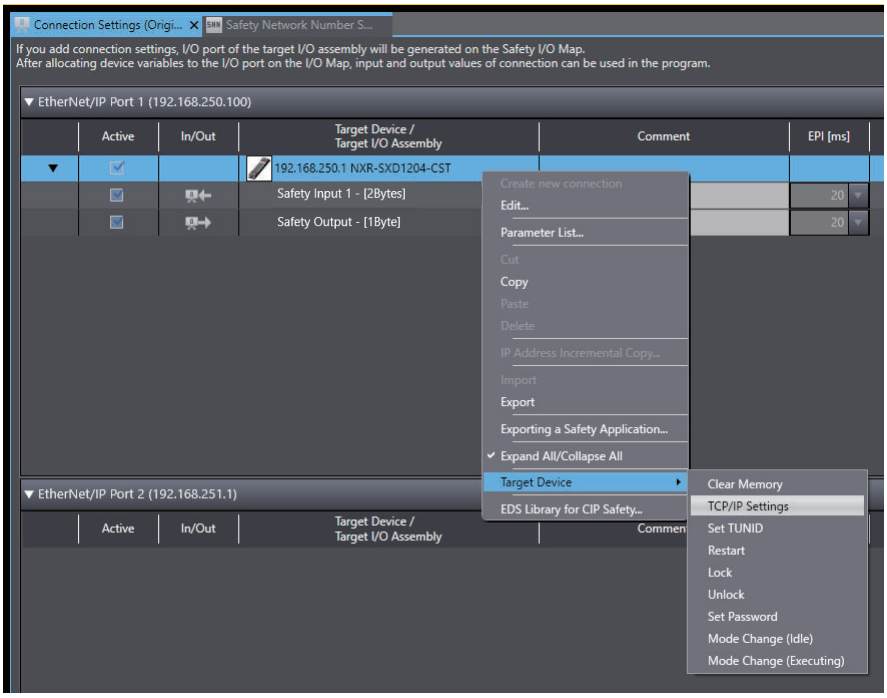
Procedure Using Sysmac Studio

In Sysmac Studio, there is a method to execute locking and unlocking of the configuration for Units individually, and a method to execute locking and unlocking of the configuration for multiple Units registered to the CIP Safety Connection Setting screen at once.

● Setting the Configuration Lock on an Individual Unit Basis

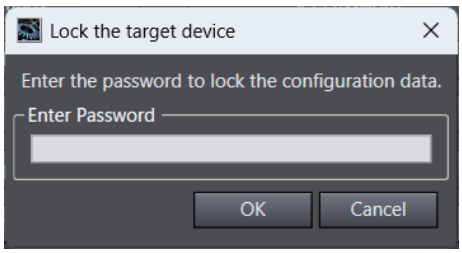
The procedure to lock or unlock the configuration on an individual unit basis is as follows.

1 Right-click the Safety I/O Block on the settings screen for the connection settings (originator), and then click **Target Device** from the displayed menu.



2 Click **Lock** or **Unlock**.

3 The safety password input window is displayed. Enter the safety password.

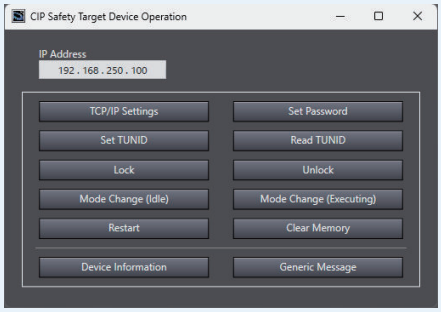


4 Click **OK**.
Locking or unlocking of the configuration is executed.

Additional Information

Execution from the CIP Safety Target Device Operation window is also possible.

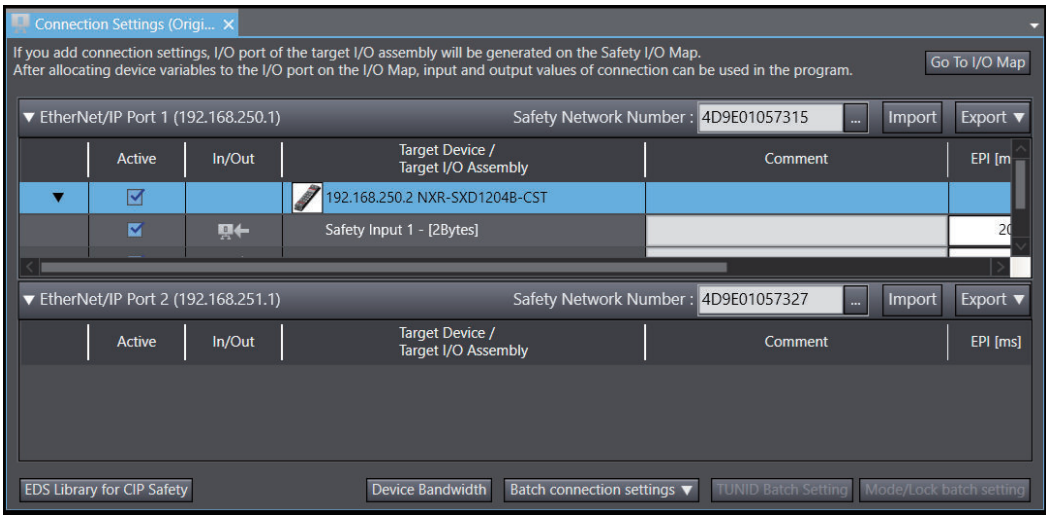
1) Select Safety PLC (Initial display new_SafetyCPU_0) in the Multiview Explorer, and select **CIP Safety Target Device Operation** in the **Tools** menu from the menu bar at the top of the screen.
2) Enter the IP address that is set for the **IP Address** in Safety I/O Block.



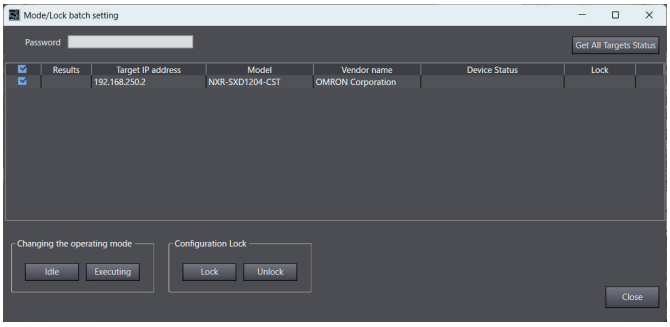
● Batch Configuration of Multiple Units

The procedure to use batch configuration of multiple units is as follows.

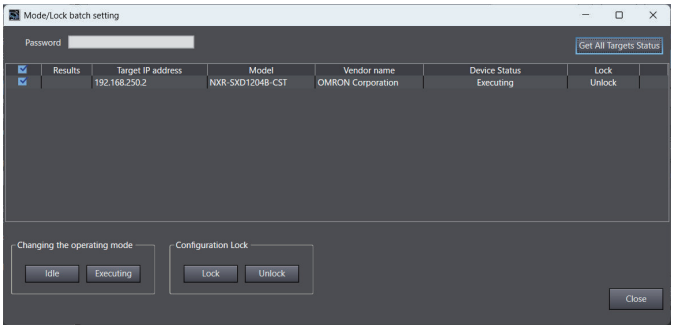
1 Display the settings screen for the connection settings (originator) in Sysmac Studio.



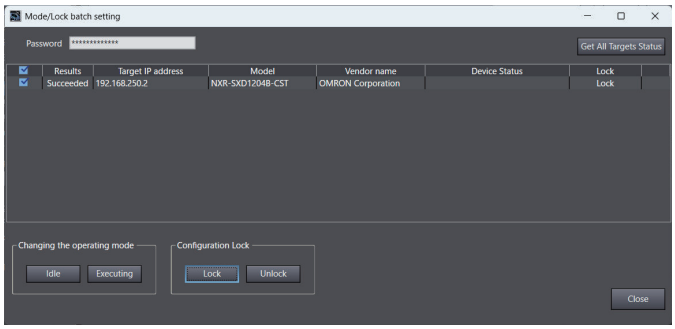
2 Click the **Mode/Lock batch setting** button.
The following screen is displayed.



3 Click the **Get All Targets Status** button.
The configuration lock status of each target is displayed in the **Lock** column as shown below.

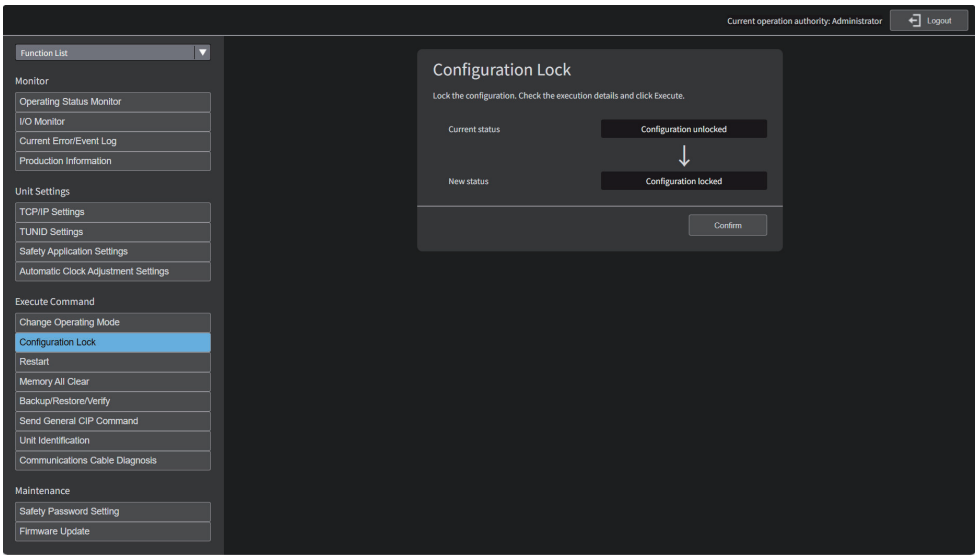


4 Enter the safety password and click the **Lock** button or **Unlock** button of **Configuration lock**.
Locking or unlocking of the configuration is executed for multiple units at once. Whether locking or unlocking the configuration was a success or failure is displayed in the **Results** column as shown below.



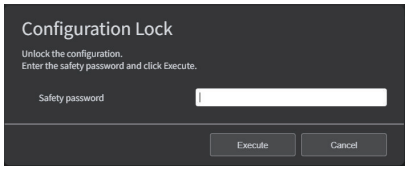
Procedure Using the Web UI

Use the Configuration Lock screen of the Web UI to lock and unlock the configuration of the Safety I/O Block. The settings on this screen can be configured only by a user with the administrator authority.

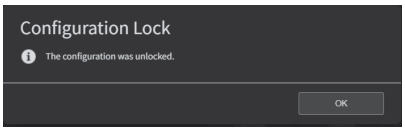


The setting procedure is as follows.

1 The current configuration lock state is displayed in the **Current status** field, and the new configuration lock state is displayed in the **New status** field. Click the **Confirm** button.
The following message is displayed.



2 Enter the safety password, and click the **Execute** button.
The configuration is locked or unlocked, and the following message is displayed.



3 Click the **OK** button.

7-17-3 Details on Configuration Lock

You can check whether the configuration is locked from the LOCK indicator of the Unit indicators. The LOCK indicator is lit when the configuration is locked, and flashing or not lit when it is unlocked. Refer to *LOCK Indicator* on page 3-7 for details on the LOCK indicator.

Target Data of Configuration Lock

The target data of the configuration lock is as follows. In the locked state, these data cannot be changed.

Item	Description
CIP Safety communications settings	CIP Safety communications basic settings including TUNID
Safety application settings	Settings of add-on applications and user-defined applications and I/O configuration settings of remote I/O mode applications The settings of fixed applications cannot be changed regardless of the lock state.
Setting data of non-safety functions	EtherNet/IP communications settings, TCP/IP settings, LINK settings, Ethernet port enable/disable settings, LLDP function settings, enable/disable setting of power shut-off function for through-wiring output, SNTP settings

If the rotary switches are changed to a different value after the configuration lock is executed and then the power is turned ON, the *Rotary switch settings changed after configuration was locked* event occurs and the corresponding Unit stops operating.

Target Functions of Configuration Lock

The target functions of the configuration lock are as follows. In the locked state, these functions cannot be executed.

- I/O wiring checking function
- Restoration of backup function
- Clear all memory function

Conversely, the configuration cannot be locked while the following functions are executing.

- I/O wiring checking function

7-18 Setting the Safety Password

The safety password is for preventing unauthorized access to the Safety I/O Block Unit, and protecting the assets stored in the Safety I/O Block Unit.

7-18-1 Purpose of Safety Password

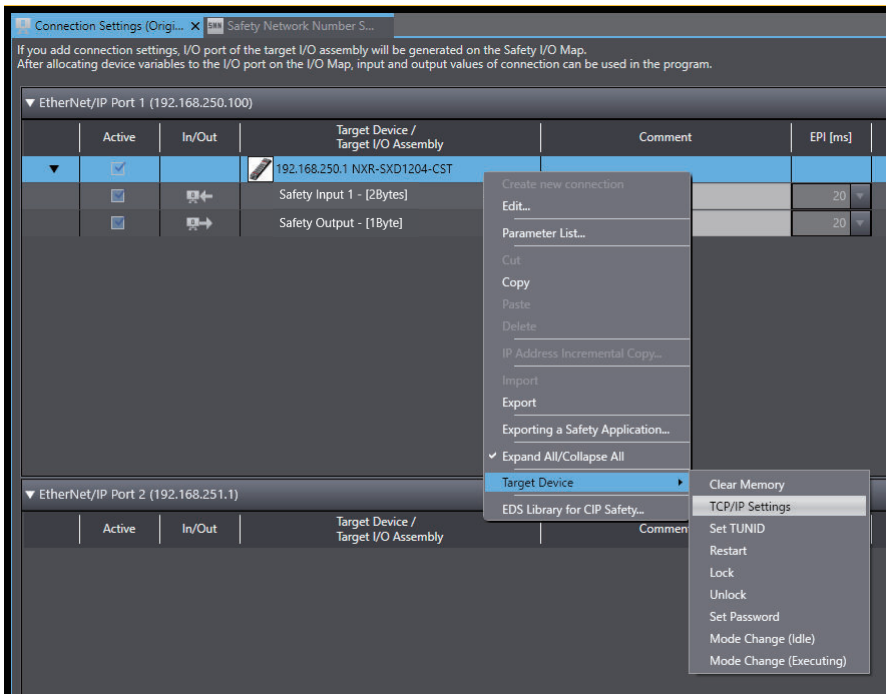
The purpose of the safety password is to prevent tampering with and leakage of the assets of the Safety I/O Block by enabling use of only operations corresponding to the authority of the user.
Therefore, the account information of users including the safety password must be managed appropriately.

7-18-2 Procedure for Using Safety Password Setting

Safety password setting has a method that uses the Web UI.
Furthermore, the safety password can be changed also in Sysmac Studio.

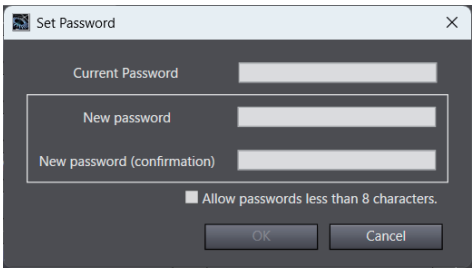
Procedure for Changing the Safety Password in Sysmac Studio

1 Right-click the Safety I/O Block on the settings screen for the connection settings (originator), and then click **Target Device** from the displayed menu.



2 Click **Set Password**.

3 The password setting window is displayed. Enter the current safety password and new safety password.

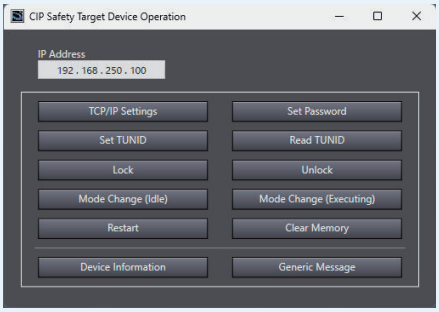


4 Click **OK**.
The new safety password is set.

Additional Information

Execution from the CIP Safety Target Device Operation window is also possible.

1) Select Safety PLC (Initial display new_SafetyCPU_0) in the Multiview Explorer, and select **CIP Safety Target Device Operation** in the **Tools** menu from the menu bar at the top of the screen.
2) Enter the IP address that is set for the **IP Address** in Safety I/O Block.



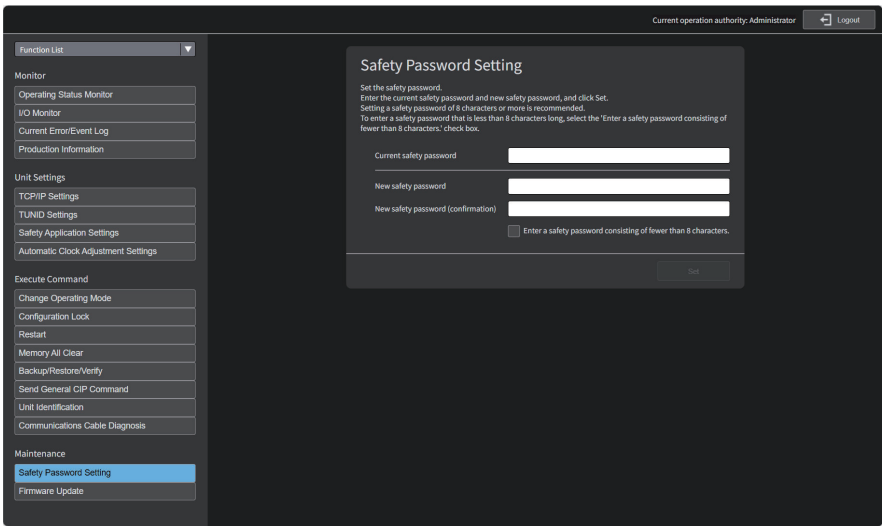
Procedure Using the Web UI

Refer to the following table for the safety password related usage procedures of the Web UI.

Function	Reference
Safety password authentication	*7-2-6 Login* on page 7-22
Safety password setting	*Safety Password Setting Procedure Using the Web UI* on page 7-105
Change Initial Safety Password	*Change Initial Safety Password* on page 7-24

Safety Password Setting Procedure Using the Web UI

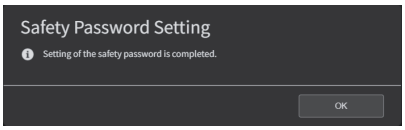
Set the safety password on the Safety Password Setting screen of the Web UI.
The settings on this screen can be configured only by a user with the administrator authority.



The setting procedure is as follows.

1 Enter the current safety password in **Current safety password**. Enter a new safety password in **New safety password** and **New safety password (confirmation)**.
To enhance the security, enter a safety password that is at least 8 characters long.
However, in special circumstances, such as when you wish to use the same password as another device, you can set a safety password that is less than 8 characters long if you select the **Enter a safety password less than 8 characters long** check box.

2 Click the **Set** button.
The safety password is set, and the following message is displayed.



3 Click the **OK** button.
Logging out from the Web UI is performed and the Login screen is displayed.

7-18-3 Details on Safety Password

This section describes various specifications of the safety password.

Operations Requiring Entering of the Safety Password

With Sysmac Studio, entering of the safety password is required when performing the following operations. If you do not enter the safety password, these operations are not executed.

- Changing the safety password
- Locking/unlocking the configuration
- Restarting
- Changing the operating mode

- Clearing all memory

The Web UI divides user authorities into observers who can view various information displayed on screens by the Web UI, and administrators who can configure various settings provided by the Web UI.
Refer to *7-2-4 Main Menu List* on page 7-18 for the relationship between the various screens of the Web UI and whether use is possible as an observer or administrator.

Safety Password Specifications

The conditions for the text string that can be used for the safety password are as follows.

Item	Description
Number of characters	8 to 32
Usable characters	A to Z, a to z, 0 to 9, ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ single-byte space

The safety password is not set at shipment from the factory.

Precautions for Correct Use

To reduce the security risk, always set a safety password. Use alphabet letters, symbols, and numbers for the safety password that you set to make it complicated.

Other Specifications

If there is no operation for at least 10 minutes after logging in to the Web UI, you will be required to re-enter the safety password to prevent unauthorized use by a third party without editing authority.

As a measure against brute force attacks, if you enter the safety password 5 times incorrectly in the Web UI, you will be unable to log in for 10 minutes. The count for entering the safety password incorrectly is reset by any of a successful login, cycling of the power supply, or 10 minutes elapsing.

Precautions for Correct Use

- The safety password cannot be displayed. Furthermore, if the safety password is initialized by clearing all memory, you need to enter a safety password.
- To prevent unauthorized use by third parties, log out from the Safety I/O Block before interrupting operations via the Web UI and leaving your computer. In the Web UI, by selecting **Refresh automatically** on the Operating Status Monitor screen, I/O Monitor screen, Current Error screen and Event log screen, re-entry of the safety password is not required even after more than 10 minutes of inactivity.

7-19 Backup

Backup has three functions: backup, restore, and verify.

- **Backup**

  Save all setting data of the corresponding Unit collectively to the PC as a backup file. Set a backup file password for a backup file as a security measure.

- **Restore**

  Deploy the contents of a backup file on the PC to the corresponding Unit.

- **Verify**

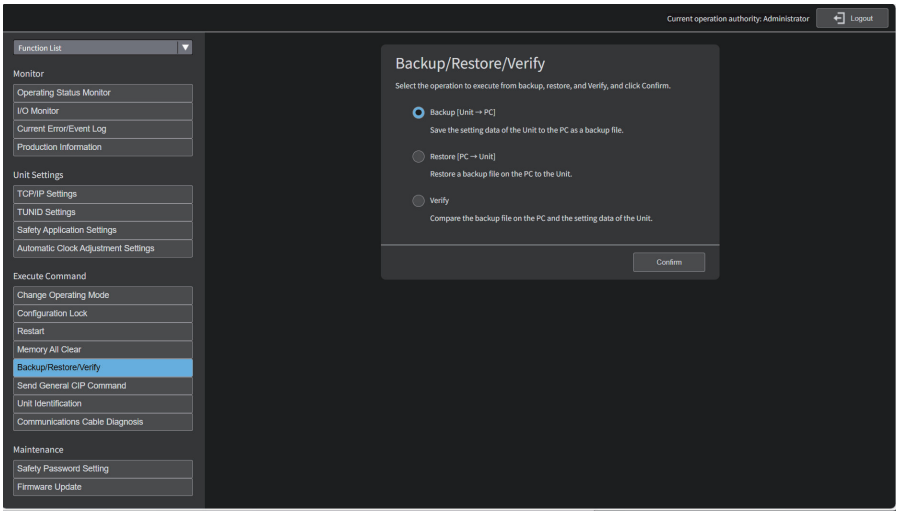
  Verifies the setting data of the corresponding Unit and the backup file on the PC to verify whether the content is the same.

7-19-1 Purpose of Backup

The purpose of a backup is to reduce the parameter setting time during replacement of the Safety I/O Block by backing up, restoring, and verifying all setting data of the Safety I/O Block at once.
Make a backup regularly and when you have changed settings to ensure that the settings of the Safety I/O Block always match those in the backup file.

7-19-2 Procedure for Using Backup

Use the Backup/Restore/Verify screen of the Web UI to perform backing up, restoring, and verification.
The settings on this screen can be configured only by a user with the administrator authority.



This section describes each of the procedures.

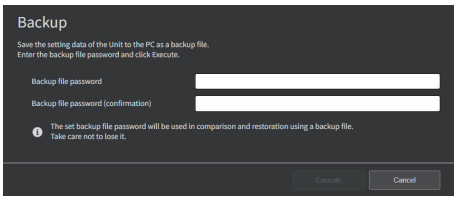
Precautions for Correct Use

To execute a backup, you need to use the configuration lock function to set the Safety I/O Block to the locked state. Furthermore, to execute a restore, you need to set the Safety I/O Block to the unlocked state. Refer to *7-17 Configuration Lock* on page 7-99 for details on the configuration lock function.

Backup

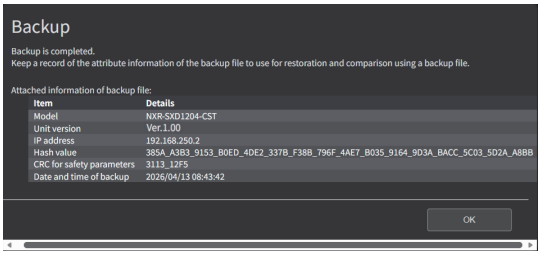
The backup procedure is as follows.

1 Select **Backup [Unit → PC]**, and click the **Confirm** button.
The following screen is displayed.



2 Enter a backup file password in **Backup file password** and **Backup file password (confirmation)**.
The backup file password is for creating, restoring, and verifying a backup file. It differs from the safety password.

3 Click the **Execute** button.
A backup file is stored in the Downloads folder on the PC. The file name is *Unit Model_IP Address_Date.dat*.
The following message is displayed.



The backup file attribute information displayed is required for the restore. Keep a note of it.

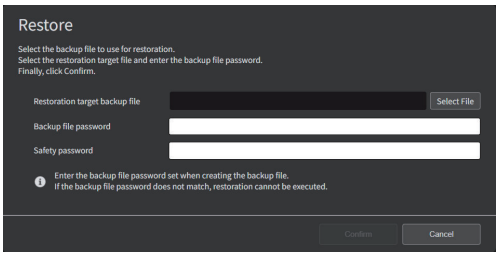
4 Click the **OK** button.

Restore

The restore procedure is as follows.

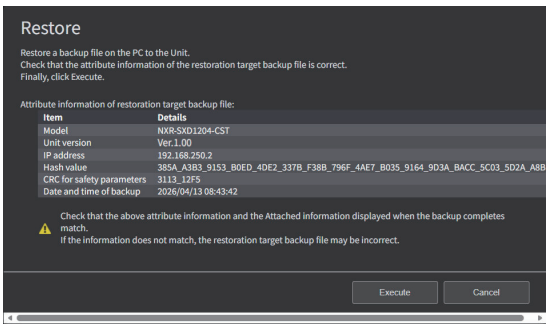
1 Prepare the restore destination Safety I/O Block in the factory default state or with all memory cleared, and the backup file and the attribute information of the backup file recorded when the backup file was created.

2 Select **Restore [PC → Unit]** on the Backup/Restore/Verify screen of the Web UI, and click the **Confirm** button.
The following screen is displayed.



3 Click the **Select** button, and select the restoration target backup file on the PC.
The selected backup file is displayed in the **Restoration target backup file** field.

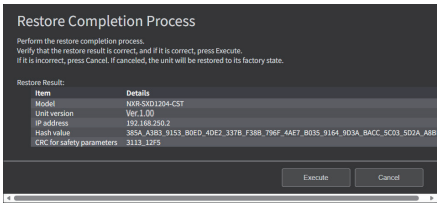
4 Enter the backup file password and safety password, and click the **Confirm** button.
The following message is displayed.



5 Check that the attribute information displayed in the **Attribute information of restoration target backup file** field matches the attribute information displayed when creating the backup file, and click the **Execute** button. If it does not match, click the **Cancel** button because the specified backup file may be damaged.
When the **Execute** button is clicked, restoration is executed and the following message is displayed.



6 Enter the safety password, and click the **Restart** button.
The Safety I/O Block restarts, and the restored content is reflected. The following message is displayed.



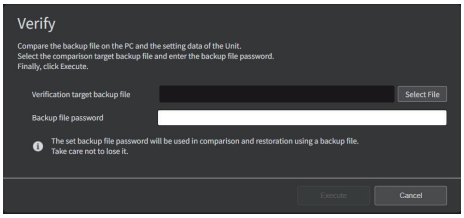
7 Check that the attribute information displayed in the **Restore Result** field matches the attributed information displayed when creating the backup file, and click the **Execute** button. If it does not match, click the **Cancel** button because the restoration may have failed.

8 Cycle the power supply or use the Restart screen of the Web UI to restart the Safety I/O Block.
The restoration completes and the Safety I/O Block restarts. If the **Cancel** button was clicked in step 7, all memory is cleared automatically.
The operating mode after the restart is in accordance with the power-on mode setting of the restored backup data. The configuration lock is locked.

Verifying Data

The verification procedure is as follows.

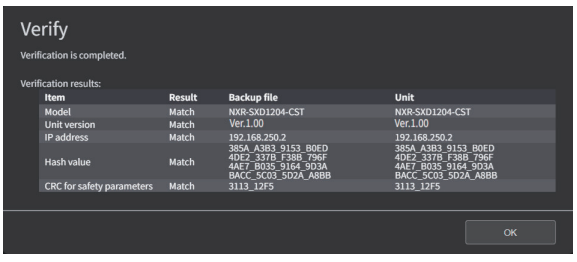
1 Select **Verify**, and then click the **Confirm** button.
The following screen is displayed.



2 Click the **Select File** button, and select the verification target backup file on the PC.
The selected backup file is displayed in the **Verification target backup file** field.

3 In **Backup file password**, enter the backup file password set when creating the backup file.
The backup file password is for creating, restoring, and verifying a backup file. It differs from the safety password.

4 Click the **Execute** button.
If the backup file password matches, the verification is executed and the verification result is displayed.



5 Click the **OK** button.

7-19-3 Details on Backup

This section describes the various specifications of backup.

Data to Be Backed Up

The data to be backed up, restored, and verified is as follows.

Item	Description
CIP Safety communications settings	CIP Safety communications basic settings including SNN and TUNID
Safety application settings	Settings of add-on applications and user-defined applications and I/O configuration settings of remote I/O mode applications The settings of fixed applications are not included.
Configuration locked state	Information indicating that configuration is locked, and the various setting values stored when the configuration was locked
Production information	Unit model, Unit version
Setting data of non-safety functions	EtherNet/IP communications settings, TCP/IP settings *1, LINK settings, Ethernet port enable/disable settings, LLDP function settings, enable/disable setting of power shut-off function for through-wiring output, SNTP settings

***1.** If the IP address is configured using DHCP, the IP address obtained from the DHCP server is excluded from backup, restores, and verifications.

File Name of Backup File

The default file name of the backup file is *Unit Model_IP Address_Date.dat*. You can freely change the file name.

Specifications of Backup File Password

The conditions for the text string that can be used for the backup file password are as follows.

Item	Description
Number of characters	8 to 32
Usable characters	A to Z, a to z, 0 to 9, ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ single-byte space

Precautions for Correct Use

- To reduce the security risk, use a combination of alphabet letters, symbols, and numbers for the backup file password.
- The backup file password can be neither displayed nor initialized. Manage the backup file password in case you forget it.

8

Functions of Safety I/O Block

This chapter describes the various functions of the Safety I/O Block.

8-1 List of Functions 8-3

8-2 Clear All Memory Function 8-4
8-2-1 Purpose of Clear All Memory Function 8-4
8-2-2 Procedure for Using the Clear All Memory Function 8-4
8-2-3 Details on Clear All Memory Function 8-7

8-3 HTTPS Communications Function 8-8
8-3-1 Purpose of HTTPS Communications Function 8-8
8-3-2 Procedure for Using the HTTPS Communications Function 8-8
8-3-3 Details on HTTPS Communications Function 8-9

8-4 Device Level Ring (DLR) Function 8-10
8-4-1 Purpose of DLR Function 8-10
8-4-2 Procedure for Using the DLR Function 8-10
8-4-3 Details on DLR Function 8-10

8-5 Power OFF Function for Through-wiring Output 8-11
8-5-1 Purpose of Power OFF Function for Through-wiring Output 8-11
8-5-2 Procedure for Using the Power OFF Function for Through-wiring Output 8-11

8-6 I/O Wiring Checking Function 8-13
8-6-1 Purpose of I/O Wiring Checking Function 8-13
8-6-2 Operation of the I/O Wiring Checking Function 8-13
8-6-3 I/O Configuration Settings for I/O Wiring Checking Function 8-13
8-6-4 Procedure for Using I/O Wiring Checking Function 8-14

8-7 Send General CIP Command Function 8-15
8-7-1 Purpose of Send General CIP Command Function 8-15
8-7-2 Procedure for Using Send General CIP Command Function 8-15

8-8 Unit Identification Function 8-16
8-8-1 Purpose of Unit Identification Function 8-16
8-8-2 Procedure for Using the Unit Identification Function 8-16
8-8-3 Details on Unit Identification Function 8-18

8-9 IP Address Indication Function 8-19
8-9-1 Purpose of IP Address Indication Function 8-19
8-9-2 Procedure for Using the IP Address Indication Function 8-19
8-9-3 Details on IP Address Indication Function 8-19

8-10 Power Supply Monitor Function 8-22
8-10-1 Purpose of Power Supply Monitor Function 8-22
8-10-2 Procedure for Using the Power Supply Monitor Function 8-22

8-10-3 Details on Power Supply Monitor Function 8-24

8-11 I/O Monitor Function 8-27
8-11-1 Purpose of I/O Monitor Function 8-27
8-11-2 Procedure for Using the I/O Monitor Function 8-27

8-12 Contact Operation Count Monitor Function 8-29
8-12-1 Purpose of the Contact Operation Count Monitor Function 8-29
8-12-2 Procedure for Use with Safety Input Terminals 8-29
8-12-3 Procedure for Use with Safety Output Terminals 8-29

8-13 Communications Cable Diagnosis Function 8-31
8-13-1 Purpose of Communications Cable Diagnosis Function 8-31
8-13-2 Procedure for Using the Communications Cable Diagnosis Function 8-31
8-13-3 Details on Communications Cable Diagnosis Function 8-33

8-14 Firmware Update Function 8-35
8-14-1 Purpose of Firmware Update Function 8-35
8-14-2 Procedure for Using the Firmware Update Function 8-35
8-14-3 Details on Firmware Update Function 8-36

8-1 List of Functions

The various functions of the Safety I/O Block include the following.

Function name	Purpose	Description	Reference
Clear all memory function	Prevent leaking of the setting data information of the corresponding Unit.	Return all setting data of the corresponding Unit to the factory default settings.	*8-2 Clear All Memory Function* on page 8-4
HTTPS communications function	Prevent leaking of the communications data information.	Perform encrypted communication between the PC and corresponding Unit when using the Web UI.	*8-3 HTTPS Communications Function* on page 8-8
Device Level Ring (DLR) function	Enable normal communications to be maintained even when a communications cable is broken in one place.	Connect communications cables in ring topology.	*8-4 Device Level Ring (DLR) Function* on page 8-10
Power OFF function for through-wiring output	Reduce the amount of power used.	Shut off the supply of output power to Units beyond that Unit when an output power supply is connected to multiple Units via through-wiring.	*8-5 Power OFF Function for Through-wiring Output* on page 8-11
I/O wiring checking function	Enable reliable and easy checking of the wiring to safety I/O terminals.	Check that the wiring to the safety I/O terminals has been performed correctly.	*8-6 I/O Wiring Checking Function* on page 8-13
Send general CIP command function	Execute the functions of CIP objects held by the corresponding Unit without a dedicated tool or SNCT.	Issue CIP message commands.	*8-7 Send General CIP Command Function* on page 8-15
Unit identification function	Enable identification of the running Unit.	Light the Unit identification indicator of the corresponding Unit.	*8-8 Unit Identification Function* on page 8-16
IP address indication function	Check the IP address of a Unit for which you know its location but have forgotten its IP address.	Use the I/O indicators to indicate the value of the IP address.	*8-9 IP Address Indication Function* on page 8-19
Power supply monitor function	Enable appropriate measures to be taken when the power supply voltage or power supply current values are outside the normal range.	Check the power supply voltage and power supply current values.	*8-10 Power Supply Monitor Function* on page 8-22
I/O monitor function	Shorten the time required to check the operation of the corresponding Unit and identify the cause of an error.	Display the value of each I/O terminal of the corresponding Unit.	*8-11 I/O Monitor Function* on page 8-27
Contact operation count monitor function	Check the maintenance timing for the corresponding Unit.	Monitor the ON/OFF count of the safety input terminals and safety output terminals of the corresponding Unit.	*8-12 Contact Operation Count Monitor Function* on page 8-29
Communications cable diagnosis function	Improve the efficiency of identifying the causes of communications errors.	Check whether the communications cables are broken or short-circuited.	*8-13 Communications Cable Diagnosis Function* on page 8-31
Firmware update function	Fix any found security vulnerabilities of the corresponding Unit.	Update the firmware of the corresponding Unit.	*8-14 Firmware Update Function* on page 8-35

8-2 Clear All Memory Function

The clear all memory function is used to return all setting data of the Safety I/O Block to the factory default settings.
However, you can remove the following information from the targets for clearing all memory.

- IP address
- TUNID
- Safety password
- Event logs
- Add-on applications of rotary switch settings No. 9 to D

Precautions for Correct Use

When disposing of the Safety I/O Block, be sure to execute the clear all memory function in the Web UI to prevent information leakage. With clear all memory using Sysmac Studio, the event logs and add-on applications of rotary switch settings No. 9 to D cannot be cleared. If the clear all memory function cannot be executed due to a failure or other problem, contact your OMRON representative.

8-2-1 Purpose of Clear All Memory Function

The purpose of the clear all memory function is to restore the settings to factory default during Safety I/O Block setup changes or to clear all setting data when disposing of the Safety I/O Block.

8-2-2 Procedure for Using the Clear All Memory Function

The clear all memory function has a method that uses Sysmac Studio and a method that uses the Web UI.

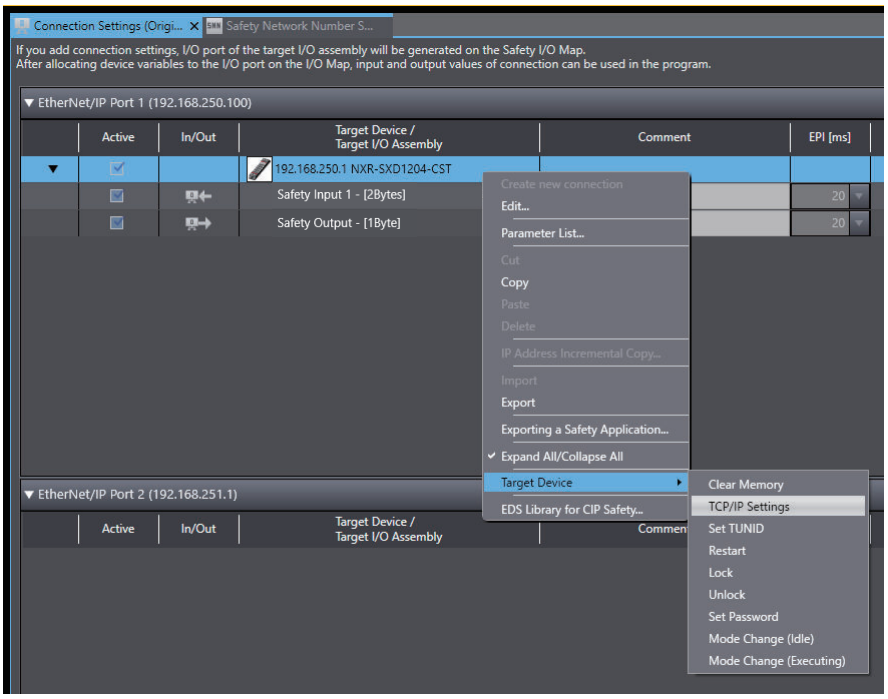
Precautions for Correct Use

To execute the memory all clear function, you need to use the configuration lock function to set the Safety I/O Block to the unlocked state. Refer to *7-17 Configuration Lock* on page 7-99 for details on the configuration lock function.

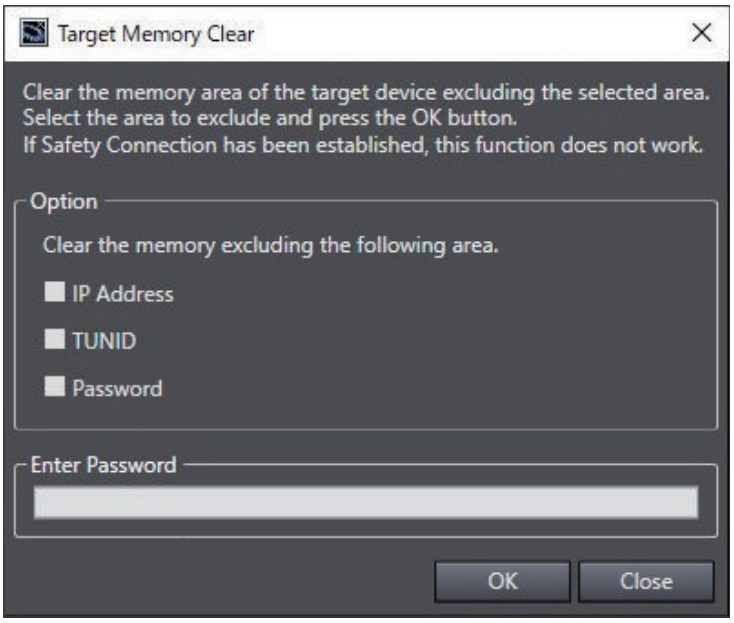
Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

1 Right-click the Safety I/O Block on the settings screen for the connection settings (originator), and then click **Target Device** from the displayed menu.



2 Click **Clear Memory**.
The following Target Memory Clear window is displayed.

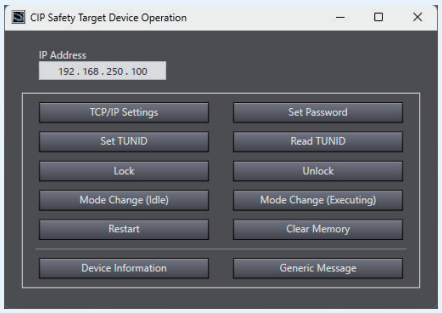


3 Select the check boxes for the items you do not want to clear from **IP Address**, **TUNID**, and **Password**, enter the safety password in the **Enter Password** box, and click the **OK** button.
The clear all memory function is executed.

Additional Information

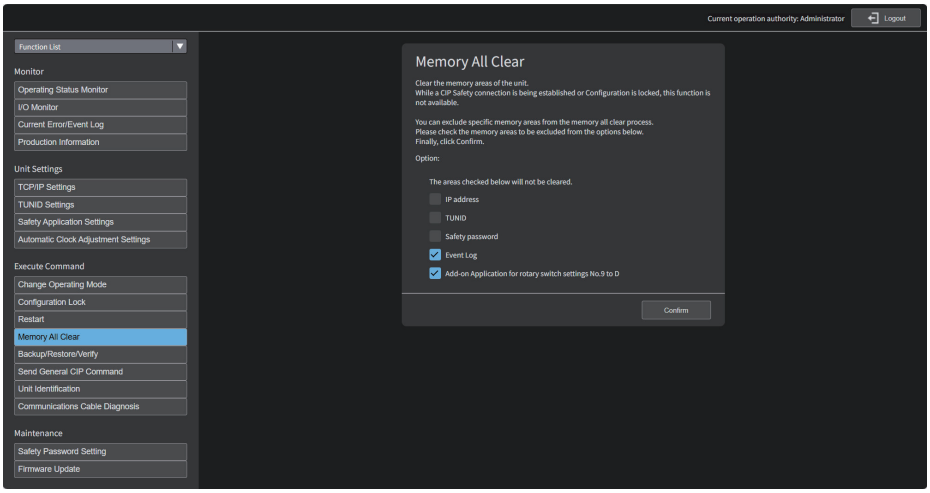
Execution from the CIP Safety Target Device Operation window is also possible.

1) Select Safety PLC (Initial display new_SafetyCPU_0) in the Multiview Explorer, and select **CIP Safety Taget Device Operation** in the **Tools** menu from the menu bar at the top of the screen.
2) Enter the IP address that is set for the **IP Address** in Safety I/O Block.



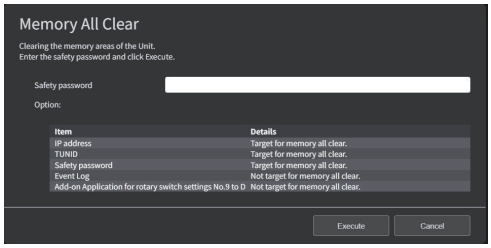
Procedure Using the Web UI

Clear all of the settings of the Safety I/O Block on the Memory All Clear screen of the Web UI.
The settings on this screen can be configured only by a user with the administrator authority.



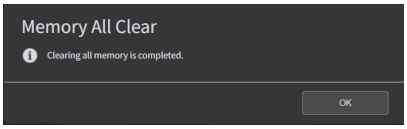
The setting procedure is as follows.

1 Select the check boxes of the items to not clear from memory, and click the **Confirm** button.
The following message is displayed.



2 Enter the safety password, and click the **Execute** button.

All memory is cleared, and the following screen is displayed.



3 Click the **OK** button.
Log out from the Web UI.

8-2-3 Details on Clear All Memory Function

The target data of the clear all memory function is as follows.
The target data differs depending on whether the clear all memory function is executed in Sysmac Studio or the Web UI.

Category	Description	Execute by Sysmac Studio	Execute by Web UI
CIP Safety communications settings	IP address	Target (selectable)	Target (selectable)
	TUNID	Target (selectable)	Target (selectable)
	CIP Safety communications basic settings excluding IP address and TUNID	Target	Target
Safety application settings	Settings of user-defined applications and I/O configuration settings of remote I/O mode applications	Target	Target
	Settings of add-on applications	Not target	Target (selectable)
Setting data of non-safety functions	EtherNet/IP communications settings, TCP/IP settings, LINK settings, Ethernet port enable/disable settings, LLDP function settings, enable/disable setting of power shut-off function for through-wiring output, SNTP settings	Target	Target
Safety password	Safety password	Target (selectable)	Target (selectable)
Event logs	System event log and access event log	Not target	Target (selectable)

8-3 HTTPS Communications Function

The HTTPS communications function encrypts communications between the PC and the Safety I/O Block when using the Web UI.
Use of the HTTPS communications function requires the CA certificate for the Web server certificate of the Safety I/O Block to be installed in the Web browser of the PC you are using. Download the CA certificate from the OMRON website. Once installed, you can continue using the HTTPS communications function on that PC.

Precautions for Correct Use

To use the Web UI, there is the method to enter an IP address and the method to enter a domain name. The method to enter a domain name has the highest security. The content explained here is required to use the method to enter a domain name. Refer to *Method to Enter an IP Address* on page 7-21 and *Method to Enter Domain Name* on page 7-22 for details on the method to enter the IP address and the method to enter a domain name, respectively.

8-3-1 Purpose of HTTPS Communications Function

The purpose of the HTTPS communications function is to prevent information leakage due to eavesdropping on the communications path between the PC and the Safety I/O Block.

8-3-2 Procedure for Using the HTTPS Communications Function

The procedure to use the Web UI by using the HTTPS communications function is as follows.

1. Download the CA certificate from the OMRON website.
2. Install the CA certificate in the Web browser of the PC.
3. Install a domain name server in the production area to perform name resolution with the domain name server. This will result in the domain name defined by the user being assigned to the IP address of the Safety I/O Block.

   Set the domain name as **.NXR-SXD.local*.
   Enter any text string for *. However, set a different text string for each IP address of the Safety I/O Block. The following table shows examples of domain names.

IP address	Domain name
192.168.250.1	device1.NXR-SXD.local
192.168.250.2	device2.NXR-SXD.local

4. Use an Ethernet cable to connect the EtherNet/IP port of the Safety I/O Block and the Ethernet port of the PC.
5. Start the Web browser of the PC.
6. Enter the domain name assigned in step 3 in the Web browser. For example, enter a domain name such as the following. *https://device1.NXR-SXD.local*
   The Web UI starts.

Steps 1 to 3 need to be performed only once on each PC. Subsequently, the Web UI can be started by simply performing the procedure from step 4.

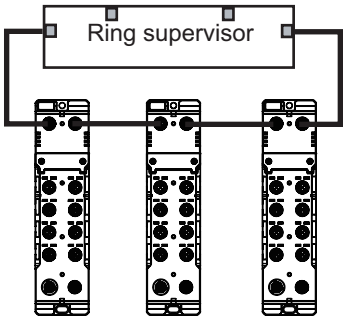
8-3-3 Details on HTTPS Communications Function

The CA certificate has a validity period. When the validity period expires, you need to install the latest CA certificate again. Check the download source and validity period of the CA certificate on the OMRON website.

The Web server certificate of the Safety I/O Block also has a validity period. If the validity period has expired, the *NET::ERR_CERT_DATE_INVALID* error message is displayed when you access the Safety I/O Block in a Web browser. The server certificate can be updated by executing the firmware update function. Refer to *8-14 Firmware Update Function* on page 8-35 for details on the firmware update function.

8-4 Device Level Ring (DLR) Function

The Device Level Ring (DLR) function is used to connect the communications cables in ring topology as follows.



8-4-1 Purpose of DLR Function

If a communications cable of the EtherNet/IP network breaks, communications with the Units after the place of the break will normally no longer be performed. The purpose of the DLR function is to enable normal communications to be maintained even when a communications cable is broken in one place.
To use the DLR function, connect the communications cables in ring topology through the ring supervisor. This enables maintaining communications by using the path in reverse direction, even if a communications cable breaks in one place.

8-4-2 Procedure for Using the DLR Function

Special settings are not required to use the DLR function. You can use the DLR function by simply connecting the communications cables in ring topology through the ring supervisor.

8-4-3 Details on DLR Function

A ring supervisor that supports a beacon-based ring node is required to use the DLR function. The following table shows the recommended ring supervisor products.

Type of device	Manufacturer	Model
Managed switch	Rockwell Automation	Stratix 5400 switches
EtherNet/IP tap	Rockwell Automation	1756-EN2TR

Precautions for Correct Use

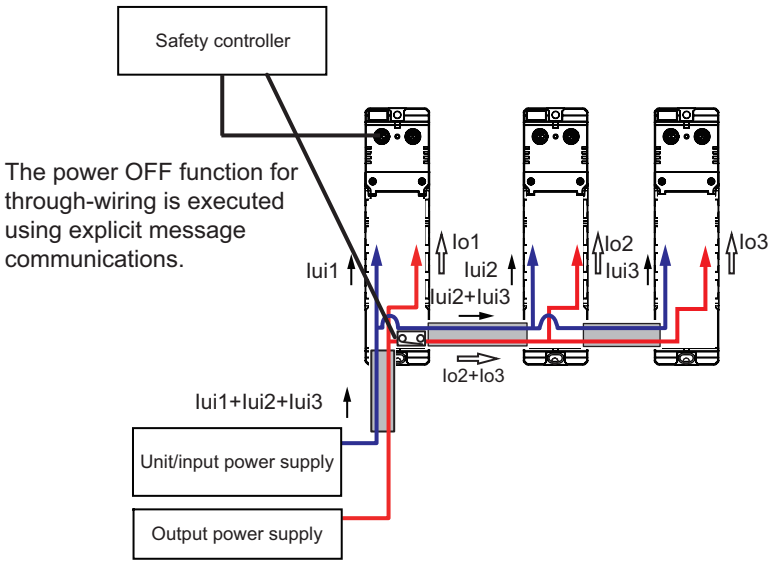
When using Safety I/O Block as a ring node, ensure that the number of ring nodes in the ring topology is 128 or fewer.

8-5 Power OFF Function for Through-wiring Output

The power OFF function for through-wiring output is used to shut OFF the supply of output power to Units beyond the corresponding Unit when an output power supply is connected to multiple Units via through wiring.

8-5-1 Purpose of Power OFF Function for Through-wiring Output

The purpose of the power OFF function for through-wiring output is to reduce the amount of power used. Normally, the supply of output power to each Unit connected by through-wiring continues regardless of whether output from the safety output terminal is ON or OFF. When the power OFF function for through-wiring output is used, the supply of output power to Units beyond the corresponding Unit is shut OFF.



Precautions for Correct Use

The power OFF function for through-wiring output is for reducing the amount of power used, and is not a safety function. Secure the safety of the equipment by other means.

8-5-2 Procedure for Using the Power OFF Function for Through-wiring Output

The power OFF function for through-wiring is executed using explicit message communications.
The send commands for executing the power OFF function for through-wiring are as follows.

Implementation details	Send command item	Send command value
Through-wiring output power supply	Service code	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01Hex
	Attribute ID	28 (Cross-Wiring Output Power Shut-off Control)
	Service data	TRUE: Through-wiring output power is supplied (default). FALSE: Through-wiring output power is not supplied.
	Update timing	Immediately
	Operation when restart	Through-wiring output power is supplied.
Enable or disable the power shut-off function for through-wiring output	Service code	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Assembly Instance ID	01Hex
	Attribute ID	29 (Cross-Wiring Output Power Shut-off Enable)
	Service data	TRUE: The power shut-off function for through-wiring output is used (default). FALSE: The power shut-off function for through-wiring output is not used.
	Update timing	Immediately
	Operation when restart	The settings before the restart continue to be used.

Refer to *Explicit Message Server Function* on page 6-7 for the method to access CIP objects through an explicit message.

8-6 I/O Wiring Checking Function

The I/O wiring checking function checks that the wiring to the safety I/O terminals of the Safety I/O Block has been performed correctly.

8-6-1 Purpose of I/O Wiring Checking Function

A mistake with the wiring to the safety I/O terminals of the Safety I/O Block may lead to a serious accident. However, wiring becomes complicated for some applications, and checking the wiring is not easy in some cases. The purpose of the I/O wiring checking function is to enable reliable and easy checking of the wiring to safety I/O terminals.

8-6-2 Operation of the I/O Wiring Checking Function

The operation of the safety output terminals of the I/O wiring checking function is as follows.
The I/O wiring checking function can check the operation of safety input terminals Si00 to Si03 and safety output terminals So00 to So03. Check the operation of safety input terminals Si04 to Si11 by visually confirming the safety input indicators.

Safety output terminal	Operation
So00	TRUE while Si00 is TRUE and the enable switch is pressed. Otherwise, FALSE.
So01	TRUE while Si01 is TRUE and the enable switch is pressed. Otherwise, FALSE.
So02	TRUE while Si02 is TRUE and the enable switch is pressed. Otherwise, FALSE.
So03	TRUE while Si03 is TRUE and the enable switch is pressed. Otherwise, FALSE.

8-6-3 I/O Configuration Settings for I/O Wiring Checking Function

The I/O wiring checking function assumes that an I/O wiring check is performed by pressing an enable switch connected to safety input terminals Si06 and Si07. The I/O configuration settings are as follows.

Inputs

Input	Device	Test Output Mode
Si00/T00	User-specified (single)	Power Supply Output
Si01/T01	User-specified (single)	Power Supply Output
Si02/T02	User-specified (single)	Power Supply Output
Si03/T03	User-specified (single)	Power Supply Output
Si04/T04	User-specified (single)	Power Supply Output
Si05/T05	User-specified (single)	Power Supply Output
Si06/T06	Enable switch (dual-channel equivalent input)	Test Output
Si07/T07	Enable switch (dual-channel equivalent input)	Test Output
Si08/T08	User-specified (single)	Power Supply Output
Si09/T09	User-specified (single)	Power Supply Output
Si10/T10	User-specified (single)	Power Supply Output
Si11/T11	User-specified (single)	Power Supply Output

Outputs

Output	Device
So00	Single channel (without test pulse)
So01	Single channel (without test pulse)
So02	Single channel (without test pulse)
So03	Single channel (without test pulse)

8-6-4 Procedure for Using I/O Wiring Checking Function

The procedure for using the I/O wiring checking function is as follows.

1 Connect the wiring to the safety I/O terminals of the Safety I/O Block as desired.

2 Set both the SETTING SW1 and SW2 rotary switches of the Safety I/O Block to *E* and then turn ON the power.

3 Perform arbitrary input to the safety input terminals of the Safety I/O Block. Check that the appropriate output is performed from the corresponding safety output terminals. Also, check that the I/O indicators light appropriately.

8-7 Send General CIP Command Function

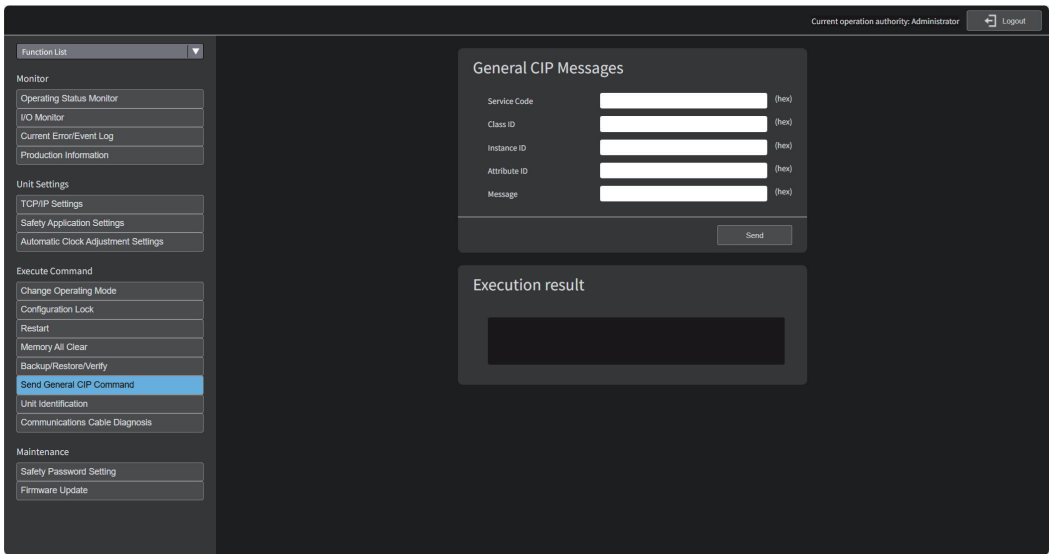
The send general CIP command function is used to issue any CIP message command to the CIP objects provided by the Safety I/O Block.

8-7-1 Purpose of Send General CIP Command Function

The purpose of the send general CIP command function is to execute the functions of CIP objects provided by the Safety I/O Block without a dedicated tool or Safety Network Configuration Tool (SNCT).

8-7-2 Procedure for Using Send General CIP Command Function

Issue a CIP message command on the Send General CIP Command screen of the Web UI.
The settings on this screen can be configured only by a user with the administrator authority.
Refer to *A-4 Supported CIP Objects* on page A-16 for details on CIP object specifications.



The setting procedure is as follows.

1. Enter each item in **Service Code**, **Class ID**, **Instance ID**, **Attribute ID**, and **Message**, and then click the **Send** button.
   The general CIP command is sent to the corresponding Unit.

2. Check the **Execution result** field.

8-8 Unit Identification Function

The Unit identification function flash the Unit identification indicator of the corresponding unit.

8-8-1 Purpose of Unit Identification Function

The purpose of the Unit identification function is to enable identification of the Unit currently operating by flashing the Unit identification indicator when you are using multiple Safety I/O Block.

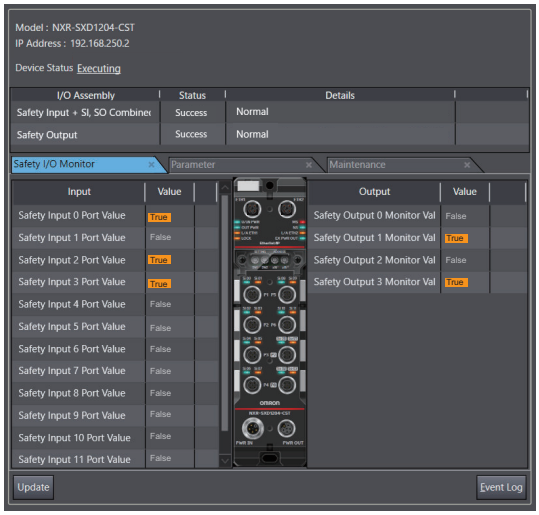
8-8-2 Procedure for Using the Unit Identification Function

The Unit identification function has a method that uses Sysmac Studio and a method that uses the Web UI.

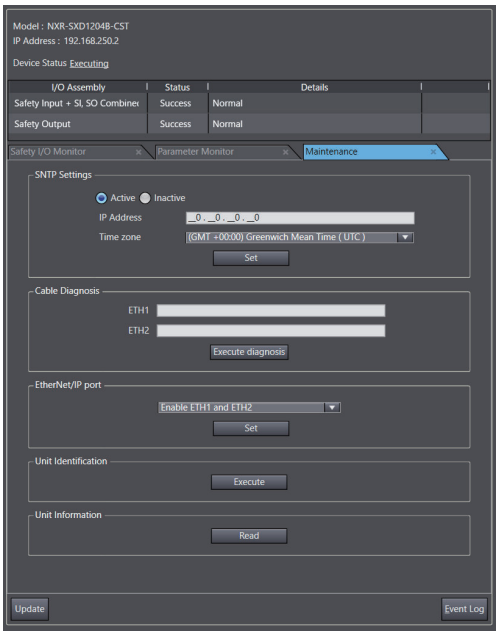
Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

1 Select Safety I/O Block on the CIP Safety Monitor screen of Sysmac Studio.
The following screen is displayed.



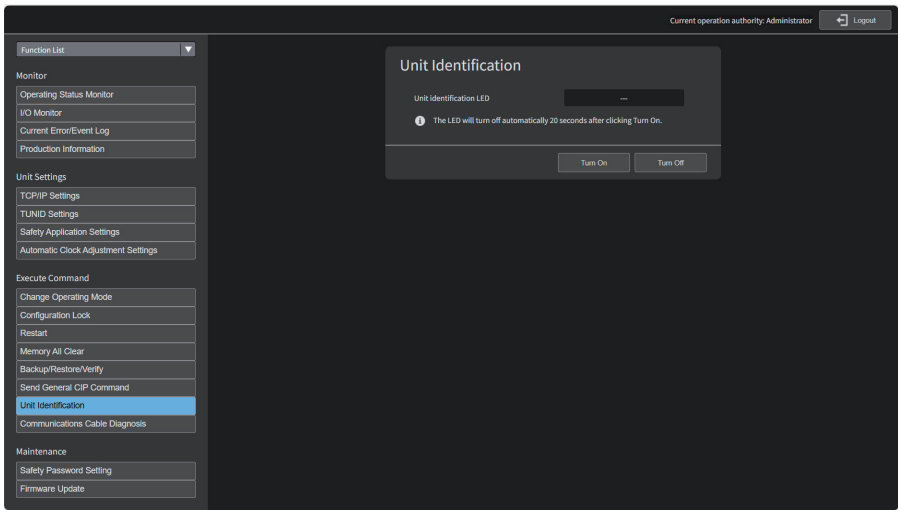
2 Select the **Maintenance** tab.
The following screen is displayed.



3 Click the **Execute** button of **Unit Identification**.
The Unit identification indicator of the specified Unit flashs.

Procedure Using the Web UI

The Unit Identification screen of the Web UI is used to flash the Unit identification indicator of the operating Unit.



The setting procedure is as follows.

1 Click the **Turn On** button.
The Unit identification function is executed on the corresponding Unit, and the Unit identification indicator flashs. **Lit** is displayed in the **Unit identification LED** field.

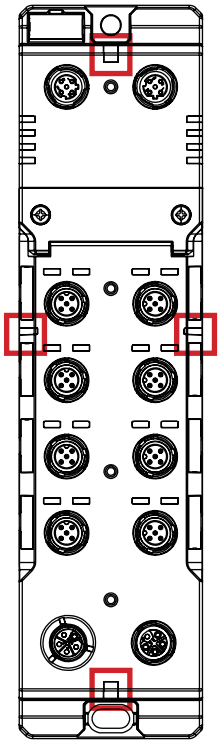
2 Click the **Turn Off** button.
The Unit identification function stops, and the Unit identification indicator turns off. **Not lit** is displayed in the **Unit identification LED** field.

Even if the **Turn Off** button is not clicked, the Unit identification indicator turns off automatically 60 seconds after you click the **Turn On** button.

8-8-3 Details on Unit Identification Function

When the Unit identification function is executed, the Unit identification indicators in the four places in the following figure flash.

- The indicators light up sequentially for a period of 100 ms each in a clockwise direction, and this is repeated four times.
- Then, all of the indicators in four places are off for 500 ms.
- The above is repeated for a period of 60 seconds.



8-9 IP Address Indication Function

The IP address indication function is used to indicate the IP address of the Safety I/O Block set by Sysmac Studio or Web UI with the I/O indicators of the Unit.

8-9-1 Purpose of IP Address Indication Function

The purpose of the IP address indication function is to allow you to check the IP address of the Safety I/O Block set by Sysmac Studio or Web UI without using a special tool such as Support Software.

8-9-2 Procedure for Using the IP Address Indication Function

This section describes the procedure to use the IP address indication function.

1 Disconnect the corresponding Unit from the network.

2 Set both SETTING rotary switches SW1 and SW2 to *8*.

3 Restart the Unit.
The I/O indicator starts lighting to indicate the IP address.

8-9-3 Details on IP Address Indication Function

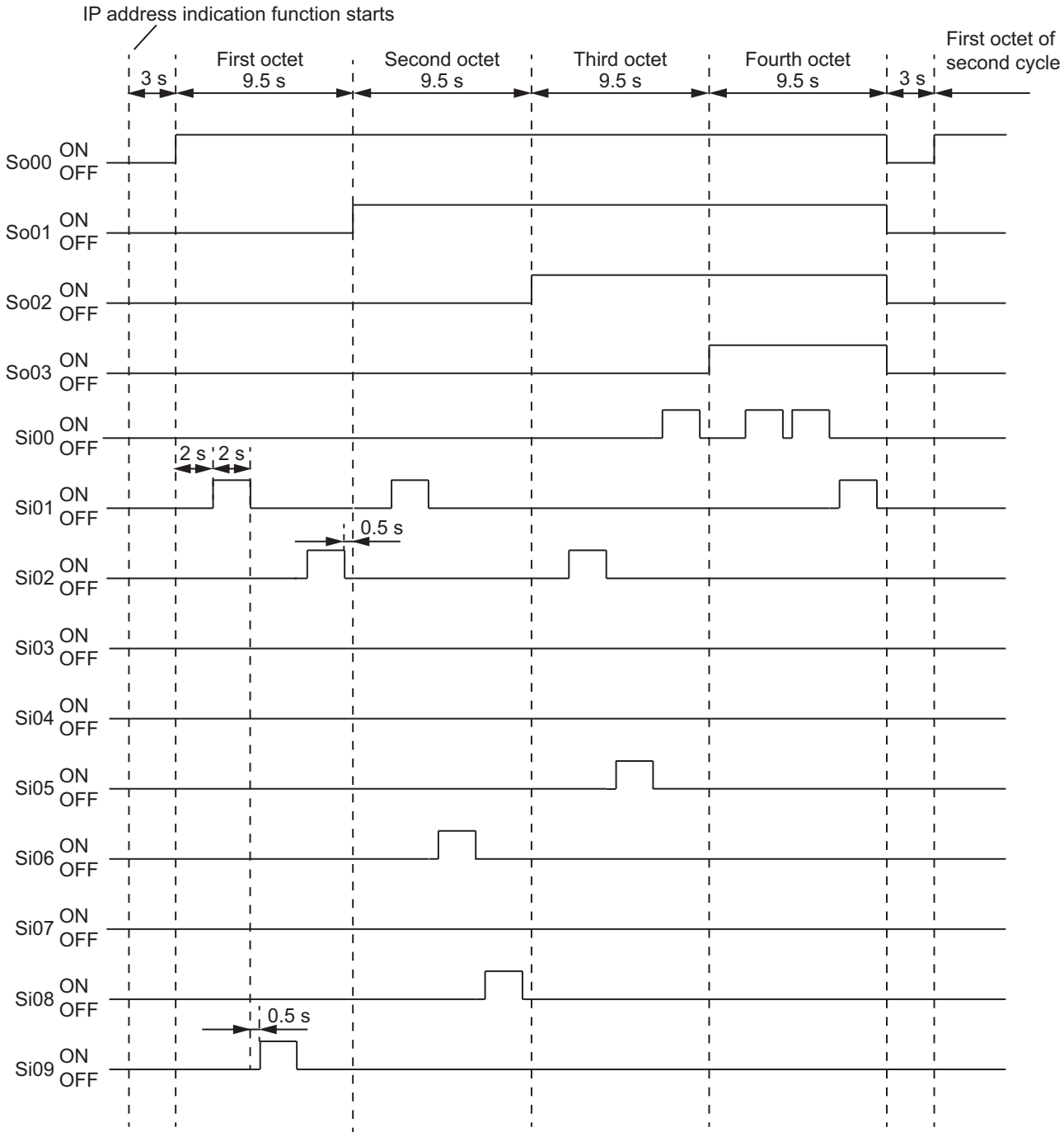
The IP address is indicated in the order of the first octet, second octet, third octet, and fourth octet. The I/O indicator that shows each octet is as follows. First, the I/O indicator of the first octet lights for 9.5 seconds. The same process is executed in order for the I/O indicators of the second octet, third octet, and fourth octet.

Octet	I/O indicator
First octet	So00
Second octet	So00 to So01
Third octet	So00 to So02
Fourth octet	So00 to So03

The three-digit number of each octet is indicated by lighting each digit in order for 2 seconds each. The indicators are off for a period of 0.5 seconds between each indicator lighting. The I/O indicator representing each number is as follows.

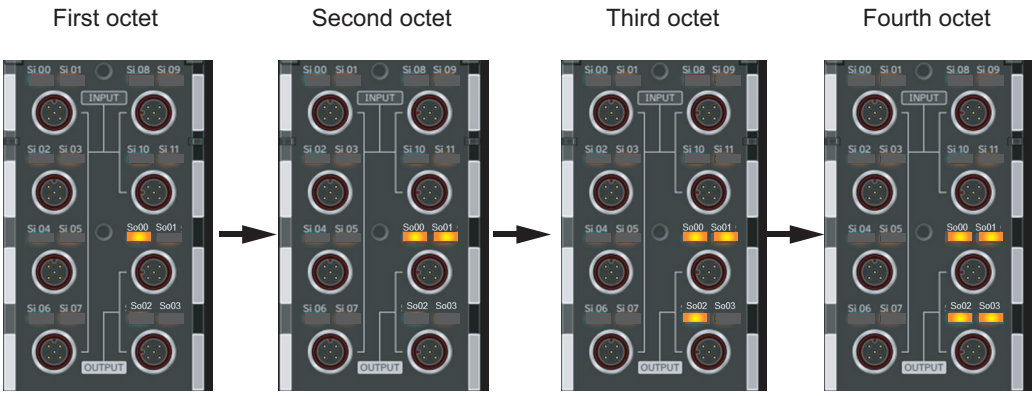
Number	I/O indicator
0	Si00
1	Si01
2	Si02
3	Si03
4	Si04
5	Si05
6	Si06
7	Si07
8	Si08
9	Si09

Lighting of the first octet starts 3 seconds after the IP address indication function starts. Furthermore, lighting of the first digit of the first octet starts 2 seconds after the lighting of the first octet starts.
As an example, the following shows a timing chart for the I/O indicators when indicating the IP address *192.168.250.001*.



The same process is repeated until the rotary switch value is changed.

The actual states of the I/O indicators that indicate from the first octet to fourth octet are as follows.
This figure shows the case of the NXR-SXD1204-CST.


First octet
Second octet
Third octet
Fourth octet
INPUT
OUTPUT

8-10 Power Supply Monitor Function

The power supply monitor function is used to check the power supply voltage value and power supply current value of the Safety I/O Block.

8-10-1 Purpose of Power Supply Monitor Function

For the Safety I/O Block to operate normally, the power supply voltage value and power supply current value must both be within the normal ranges. The purpose of the power supply monitor function is to check whether the power supply voltage value and power supply current value are within the normal ranges so that appropriate measures can be taken when they are outside the normal ranges.

8-10-2 Procedure for Using the Power Supply Monitor Function

The power supply monitor function can check the following values.

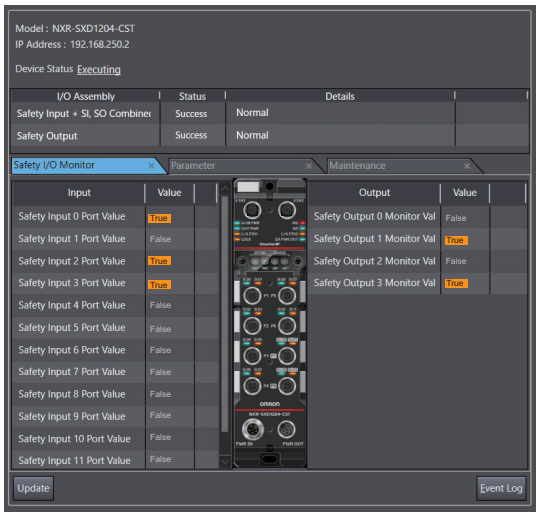
- Unit/input power supply voltage
- Output power supply voltage
- Unit/input power supply current
- Output power supply current

The power supply monitor function has a method that uses Sysmac Studio and a method that uses the Web UI.

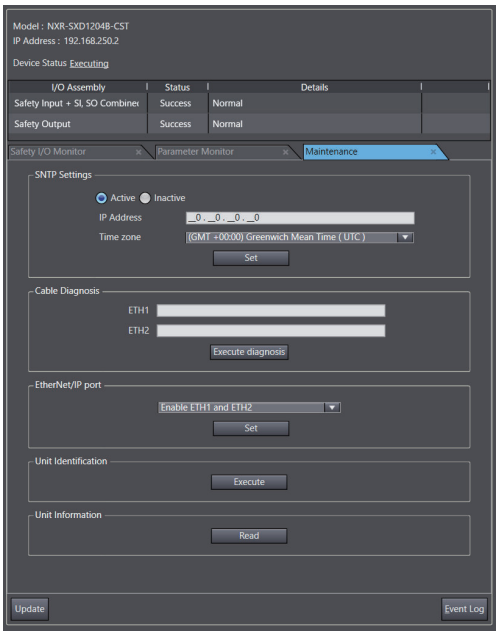
Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

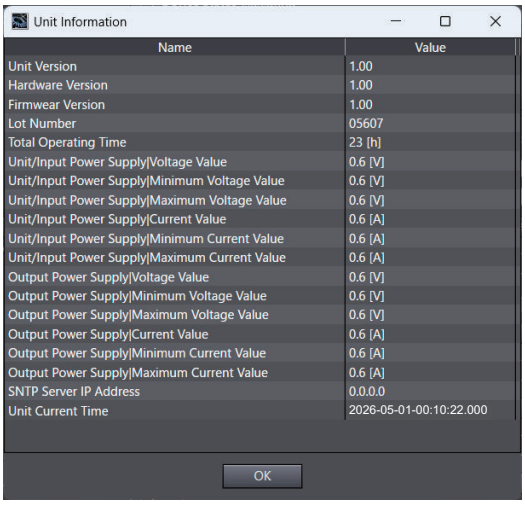
1 Select Safety I/O Block on the CIP Safety Monitor screen of Sysmac Studio.
The following screen is displayed.



2 Select the **Maintenance** tab.
The following screen is displayed.

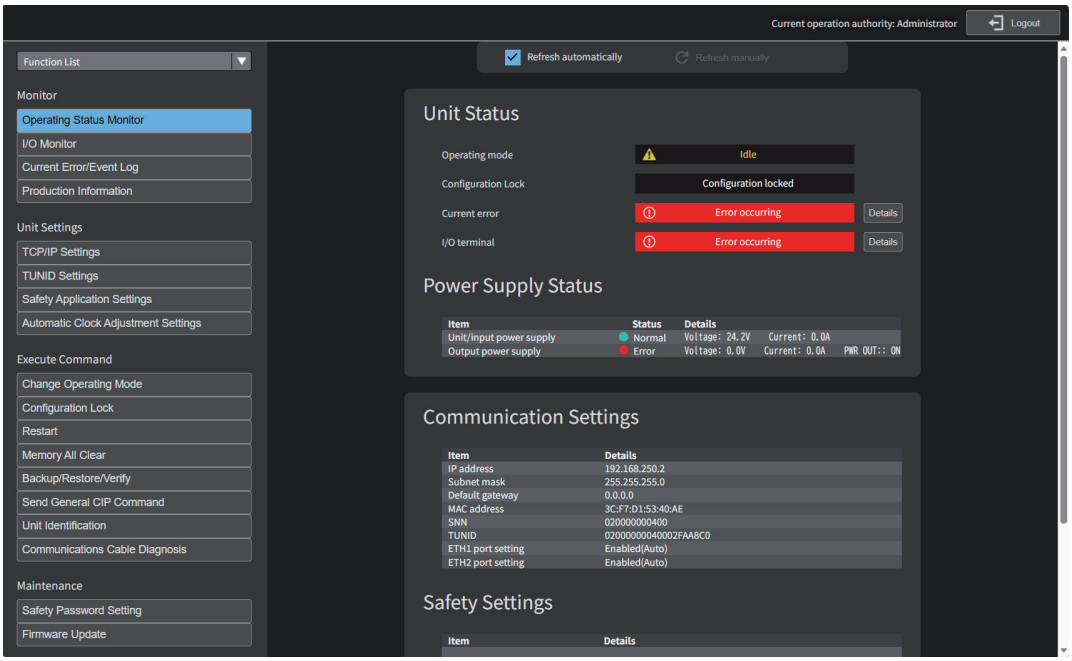


3 Click the **Read** button of **Unit Information**.
The following screen is displayed.



Procedure Using the Web UI

Check the Unit status and power supply status of the corresponding Unit in the Operating Status Monitor screen of the Web UI.



8-10-3 Details on Power Supply Monitor Function

The power supply monitor function has a power supply voltage monitor and power supply current monitor.

Monitoring the Power Supply Voltage

Monitor the power supply voltage. The status of the Unit/input power supply voltage and output power supply voltage can be checked with the U/IN PWR indicator and OUT PWR indicator.In the event of a voltage anomaly, an event will be triggered. If the power supply voltage exceeded the tolerance, the power supply input is shut off automatically.

● Unit/Input Power Supply Voltage

The following table shows the relationship of Unit/input power supply voltage values and indicator status, values that can be monitored, event occurrence, and recovery method.

Voltage value [V]	Status	U/IN PWR indicator	Values that can be monitored	Event	Recovery method
0 to low voltage detection threshold value	Power supply shut off by low voltage detection*1	Not lit	Cannot be monitored.	An event does not occur.	Supply power with the appropriate value.
Low voltage detection threshold value to 19.2	Voltage outside specification range	Lit	Voltage value	Detection of voltage outside Unit/input power supply specification range	Supply power with the appropriate value.
19.2 to 28.8	Normal voltage	Lit	Voltage value	An event does not occur.	Recovery is not required.

Voltage value [V]	Status	U/IN PWR indicator	Values that can be monitored	Event	Recovery method
28.8 to overvoltage detection threshold value	Voltage outside specification range	Lit	Voltage value	Detection of voltage outside Unit/input power supply specification range	Supply power with the appropriate value.
Voltage exceeding overvoltage detection threshold value	Power supply shut off by overvoltage detection*2	Not lit	Cannot be monitored.	An event does not occur.	Supply power with appropriate value, and then restart.

*1. The power supply of the internal circuits of the Unit is shut off. The Unit/input power supply from the power supply connector (output) is not shut off. The output power supply from the power supply connector (output) is shut off.

*2. The power supply of the internal circuits of the Unit is shut off. The Unit/input power supply from the power supply connector (output) may be shut off or may remain active depending on the detection voltage. The output power supply from the power supply connector (output) is shut off.

● Output Power Supply Voltage

The following table shows the relationship of output power supply voltage values and indicator status, values that can be monitored, event occurrence, and recovery method.

Voltage value [V]	Status	OUT PWR indicator	Values that can be monitored	Event	Recovery method
0 to low voltage detection threshold value	Power supply shut off by low voltage detection*1 All safety outputs are OFF	Not lit	Voltage value	Output Power Supply Error	Supply power with the appropriate value.
Low voltage detection threshold value to 19.2	Voltage outside specification range	Lit	Voltage value	Detection of Voltage Outside Output Power Supply Specification Range	Supply power with the appropriate value.
19.2 to 28.8	Normal voltage	Lit	Voltage value	An event does not occur.	Recovery is not required.
28.8 to overvoltage detection threshold value	Voltage outside specification range	Lit	Voltage value	Detection of Voltage Outside Output Power Supply Specification Range	Supply power with the appropriate value.
Voltage exceeding overvoltage detection threshold value	Power supply shut off by overvoltage detection*2 All safety outputs are OFF	Not lit	Voltage value	Output Power Supply Error	Supply power with appropriate value, and then restart.

*1. The power supply of the internal circuits of the Unit is shut off. The output power supply from the power supply connector (output) is not shut off.

*2. The power supply of the internal circuits of the Unit is shut off. The output power supply from the power supply connector (output) may be shut off or may remain active depending on the detection voltage.

Monitoring the Power Supply Current

Monitor the power supply current. In the event of an overcurrent anomaly that results in power being interrupted, an event will be triggered. When the power supply current exceeds the allowable value, the power input is automatically shut off.

● Unit/Input Power Supply Current

The following table shows the relationship of Unit/input power supply current values and values that can be monitored, event occurrence, and recovery method.

Current value [A]	Status	Values that can be monitored	Event	Recovery method
0 to 9	Normal current	Current value	An event does not occur.	Recovery is not required.
9 to overcurrent detection threshold value	Current outside specification range	Current value	Detection of Current Outside Unit/Input Power Supply Specification Range	Supply power with the appropriate value.
Current exceeding overcurrent detection threshold value	Power supply shut off by overcurrent detection*1	Cannot be monitored.	An event does not occur.	Supply power with appropriate value, and then restart.

***1.** The power supply of the internal circuits of the Unit is shut off. The Unit/input power supply and the output power supply from the power supply connector (output) is shut off.

● Output Power Supply Current

The following table shows the relationship of output power supply current values and values that can be monitored, event occurrence, and recovery method.

Current value [A]	Status	Values that can be monitored	Event	Recovery method
0 to 9	Normal current	Current value	An event does not occur.	Recovery is not required.
9 to overcurrent detection threshold value	Current outside specification range	Current value	Detection of Current Outside Output Power Supply Specification Range	Supply power with the appropriate value.
Current exceeding overcurrent detection threshold value	Power supply shut off by overcurrent detection*1 All safety outputs are OFF	Current value	Output Power Supply Error	Supply power with appropriate value, and then restart.

***1.** The power supply of the internal circuits of the Unit is shut off. The output power supply from the power supply connector (output) is shut off.

8-11 I/O Monitor Function

The I/O monitor function displays the values of the I/O terminals.

8-11-1 Purpose of I/O Monitor Function

When checking the operation of the Safety I/O Block or identifying the cause of an error, it is useful to check the state of the safety I/O data. The purpose of the I/O monitor function is to shorten the time required to check the operation of the Safety I/O Block and identify the cause of an error by checking the safety I/O data.

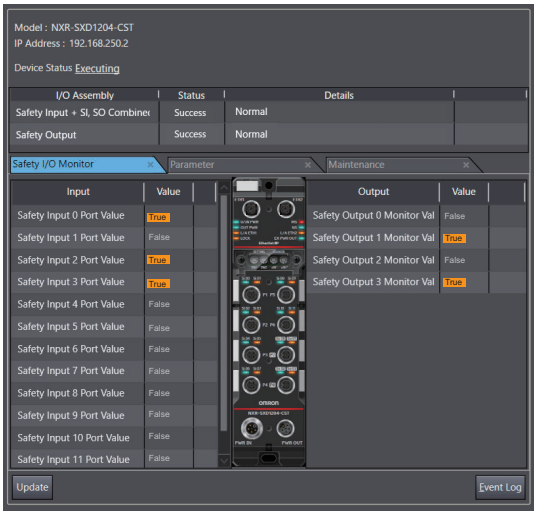
8-11-2 Procedure for Using the I/O Monitor Function

The I/O monitor function has a method that uses Sysmac Studio and a method that uses the Web UI.

Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

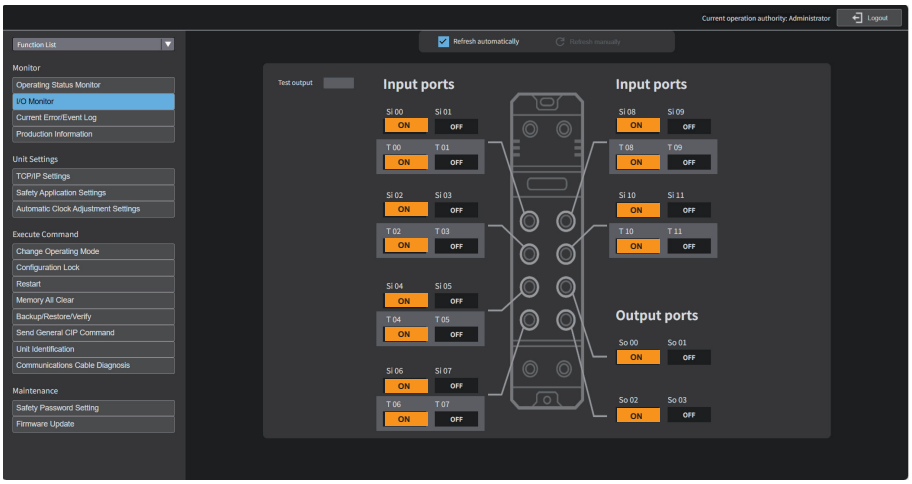
1 Select Safety I/O Block on the CIP Safety Monitor screen of Sysmac Studio.
The following screen is displayed.



2 Select the **Safety I/O Monitor** tab.
The values of the safety I/O output data are displayed.

Procedure Using the Web UI

Check the values of the I/O terminals in the I/O Monitor screen of the Web UI.


Current operation authority: Administrator
Logout
Function List
Monitor
Operating Status Monitor
I/O Monitor
Current Error/Event Log
Production Information
Unit Settings
TCP/IP Settings
Safety Application Settings
Automatic Clock Adjustment Settings
Execute Command
Change Operating Mode
Configuration Lock
Restart
Memory All Clear
Backup/Restore/Verify
Send General CIP Command
Unit Identification
Communications Cable Diagnosis
Maintenance
Safety Password Setting
Firmware Update
Refresh automatically
Refresh manually
Test output
Input ports
Si 00
Si 01
T 00
T 01
Si 02
Si 03
T 02
T 03
Si 04
Si 05
T 04
T 05
Si 06
Si 07
T 06
T 07
Input ports
Si 08
Si 09
T 08
T 09
Si 10
Si 11
T 10
T 11
Output ports
So 00
So 01
So 02
So 03
ON
OFF

8-12 Contact Operation Count Monitor Function

The contact operation count monitor function is used to check the contact operation count (unit: times).
This function counts the number of times that safety input terminals and safety output terminals turn ON/OFF, and retains the results as the current count values.
These values are obtained as current count values through CIP message communications (explicit message communications).
Furthermore, the current count values can also be cleared.

8-12-1 Purpose of the Contact Operation Count Monitor Function

The purpose of the contact operation count monitor function is to check the maintenance timing by monitoring the number of contact operations.

Additional Information

It is not a function to notify when the threshold value is reached or exceeded.

8-12-2 Procedure for Use with Safety Input Terminals

Execute the contact operation count monitor function for safety input terminals by using CIP message communications (explicit message communications).
The commands to send are as follows.

Implementation details	Send command item	Send command value
Obtain the current count value of the safety input terminals	Service code	0E hex (Get_Attribute_Single)
	Class ID	3D hex (Safety Discrete Input Point (SDIP) object)
	Instance ID	01 hex to 0C hex (Specify the instance of each safety input terminal.)
	Attribute ID	102 (Maintenance Counter)
Clear the current count value of the safety input terminals	Service code	10 hex (Set_Attribute_Single)
	Class ID	3D hex (Safety Discrete Input Point (SDIP) object)
	Instance ID	01 hex to 0C hex (Specify the instance of each safety input terminal.)
	Attribute ID	102 (Maintenance Counter)
	Service data	00000000 hex (To clear the value, write 0.)

Refer to *Explicit Message Server Function* on page 6-7 for the procedure for using CIP message communications (explicit message communications).

8-12-3 Procedure for Use with Safety Output Terminals

Execute the contact operation count monitor function for safety output terminals by using CIP message communications (explicit message communications).
The commands to send are as follows.

Implementation details	Send command item	Send command value
Obtain the current count value of the safety output terminals	Service code	0E hex (Get_Attribute_Single)
	Class ID	3B hex (Safety Discrete Output Point (SDOP) object)
	Instance ID	01 hex to 04 hex (Specify the instance of each safety output terminal.)
	Attribute ID	102 (Maintenance Counter)
Clear the current count value of the safety output terminals	Service code	10 hex (Set_Attribute_Single)
	Class ID	3B hex (Safety Discrete Output Point (SDOP) object)
	Instance ID	01 hex to 04 hex (Specify the instance of each safety output terminal.)
	Attribute ID	102 (Maintenance Counter)
	Service data	00000000 hex (To clear the value, write 0.)

Refer to *Explicit Message Server Function* on page 6-7 for the procedure for using CIP message communications (explicit message communications).

8-13 Communications Cable Diagnosis Function

The communications cable diagnosis function is used when a communications error occurs to check whether the cause is a break or short circuit in the communications cable. It also allows you to check an estimate of the location of the break or short circuit occurrence.

8-13-1 Purpose of Communications Cable Diagnosis Function

There are several possible causes for communications errors in communications performed using EtherNet/IP port 1 and port 2. The purpose of the communications cable diagnosis function is to check the causes of communications errors.

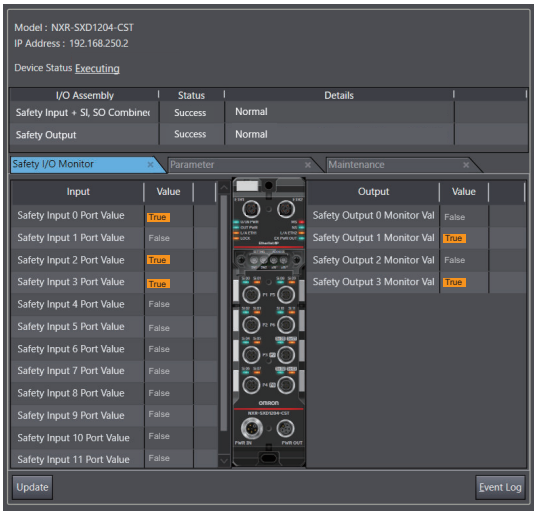
8-13-2 Procedure for Using the Communications Cable Diagnosis Function

The communications cable diagnosis function has a method that uses Sysmac Studio, a method that uses the Web UI, and a method that uses explicit message communications.

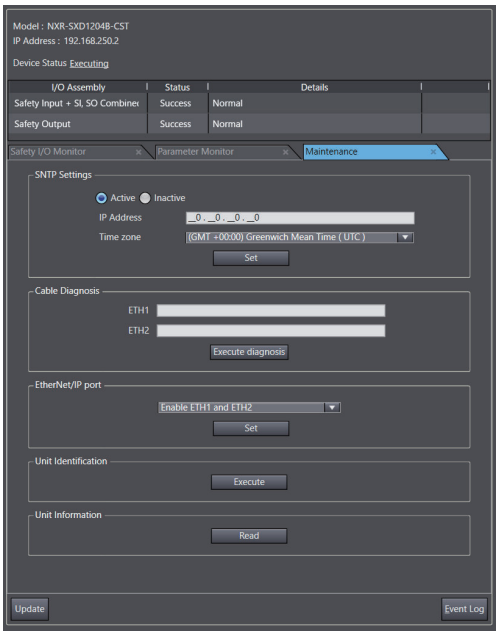
Procedure Using Sysmac Studio

The procedure using Sysmac Studio is as follows.

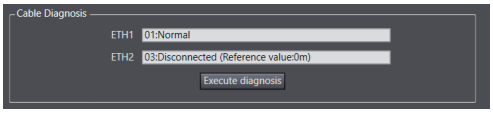
1 Select Safety I/O Block on the CIP Safety Monitor screen of Sysmac Studio.
The following screen is displayed.



2 Select the **Maintenance** tab.
The following screen is displayed.

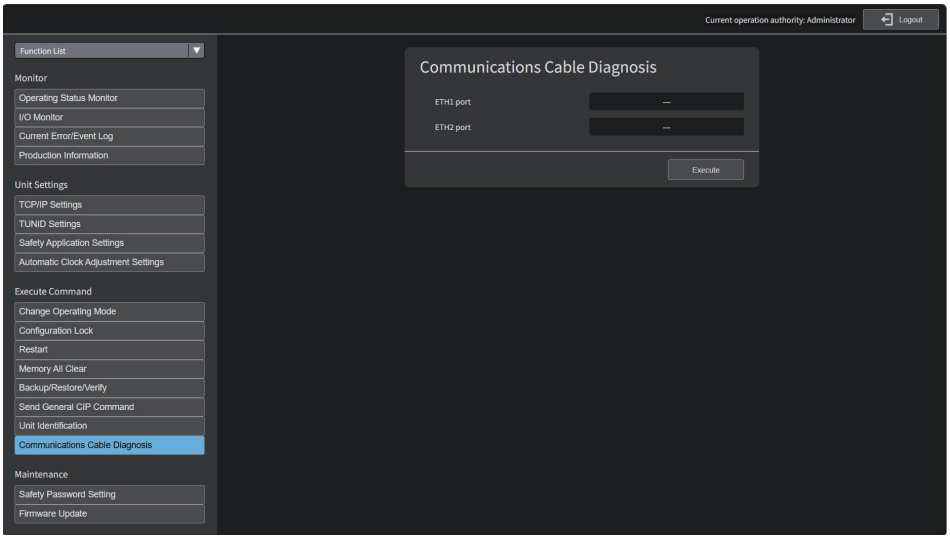


3 Click the **Execute diagnosis** button in **Cable Diagnosis**.
Whether the cable is normal or broken is displayed for port 1 and port 2. In case of a broken cable, a reference value for the distance from the Unit to the position where the communications cable is broken is also displayed.



Procedure Using the Web UI

The Communications Cable Diagnosis screen of the Web UI is used to check whether the EtherNet/IP communications cables are broken or short-circuited.



When you click the **Execute** button, the diagnosis result for EtherNet/IP port 1 is displayed in the **ETH1 port** field, and the diagnosis result for EtherNet/IP port 2 is displayed in the **ETH2 port** field.
One of the following results is displayed.

- 01: Normal
- 02: Short-circuit (reference value: ☐ m) ☐ is a numerical value.
- 03: Disconnection (reference value: ☐ m) ☐ is a numerical value.
- 04: Port disabled
- F1: Diagnosing
- F2: Failed to read
- F3: Other diagnosis error

Procedure Using Explicit Message Communications

The commands to send for communications cable diagnosis execution and diagnostic result acquisition are as follows.

Implementation details	Send command item	Send command value
Communications cable diagnosis execution	Service code	3A hex (Exec_Cable_Diagnosis)
	Class ID	F6 hex (Ethernet Link object)
	Instance ID	01 hex: Port1 02 hex: Port2
Communications cable diagnosis result	Service code	0E hex (Get_Attribute_Single)
	Class ID	F6 hex (Ethernet Link object)
	Instance ID	01 hex: Port1 02 hex: Port2
	Attribute ID	100 (Communication Cable Diagnosis)
	Response data	Refer to *Values of Communication Cable Diagnosis* on page A-50.

Refer to *Explicit Message Server Function* on page 6-7 for the procedure for using explicit message communications.

8-13-3 Details on Communications Cable Diagnosis Function

The communications cable diagnosis function has the following limitations.

- The diagnosis result for a port with a link established is always normal.
- If the send line and receive line of a communications cable are short-circuited, a broken wire cannot be detected. The diagnosis result is normal.
- If a connection timeout occurs or establishing a connection is not possible, the diagnosis result may be normal if that cause is due to the transmission characteristics of the communications cable.

The network topology and the connection configuration of the PC for executing the communications cable diagnosis function have the following relationship. Refer to *1-3-2 Network Topology* on page 1-13 for details on network topologies.

Network topology	Connection configuration of PC
Line or ring	Connection to Ethernet switch

Network topology	Connection configuration of PC
Star or tree	Connection to Ethernet port of unused Safety I/O Block

8-14 Firmware Update Function

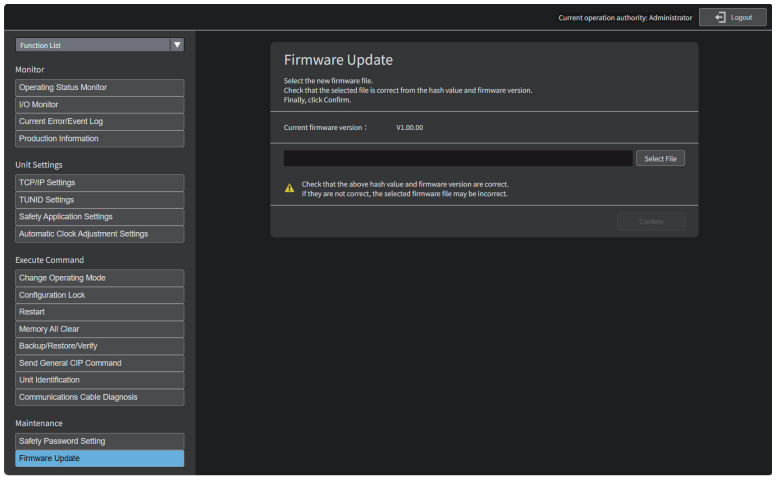
The firmware update function updates the firmware related to the communications functions and safety functions of the Safety I/O Block.
Check the OMRON website for details on how to obtain the latest firmware file.

8-14-1 Purpose of Firmware Update Function

The purpose of the firmware update function is to fix security vulnerabilities in the Safety I/O Block.

8-14-2 Procedure for Using the Firmware Update Function

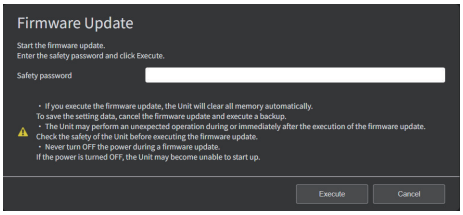
The firmware update function is executed using the Firmware Update screen of the Web UI.
The settings on this screen can be configured only by a user with the administrator authority.



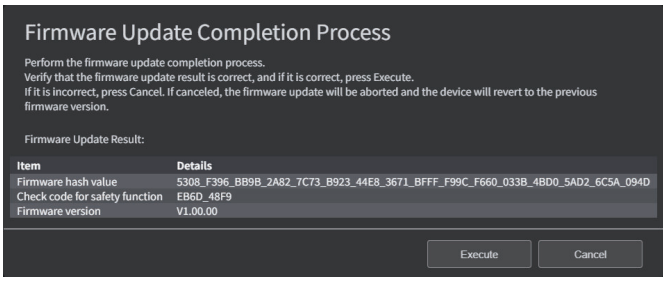
The setting procedure is as follows.

1 Click the **Select File** button, and select the firmware file on the PC.
The selected file is displayed. In addition, the selected firmware's hash value, check code for safety function, and firmware version are displayed.

2 Check that there is no problem with the firmware hash value, check code for safety function, and firmware version, then click the **Confirm** button.
The following message is displayed.



3 Enter the safety password, and click the **Execute** button.
The following message is displayed.



4 Check that there is no problem with the firmware hash value, check code for safety function, and firmware version, then click the **Execute** button.
The firmware update completion process is executed. The following message is displayed.



5 Cycle the power supply to the Safety I/O Block.

6 Check that the firmware version has changed on the Production Information screen of the Web UI.

8-14-3 Details on Firmware Update Function

When the firmware update function is executed, you can check the status of the Safety I/O Block with the MS indicator and Unit identification indicators. The following table shows the relationship between the status of the Safety I/O Block and the status of the MS indicator and Unit identification indicators.

Status of Safety I/O Block	MS indicator	Unit identification indicator
Preparing to update firmware	Not lit	All lit
Updating firmware	Flashing in green with 0.5 s ON and 0.5 s OFF	All lit
Firmware update successful	Lit green	All lit
Firmware update failed	Lit red	All lit

There are no firmware version constraints for the firmware update function. Not only version upgrades but also version downgrades are possible.

Precautions for Correct Use

- Do not turn OFF the power during execution of the firmware update function. Restarting may become no longer possible.

9

Safety Response Performance

This chapter describes how to calculate the safety response performance (safety reaction times) of the Safety I/O Block.

9-1 Safety Response Performance of Safety I/O Block 9-2
9-1-1 Calculating Safety Response Performance..... 9-2
9-1-2 Verifying Safety Response Performance..... 9-5

9-1 Safety Response Performance of Safety I/O Block

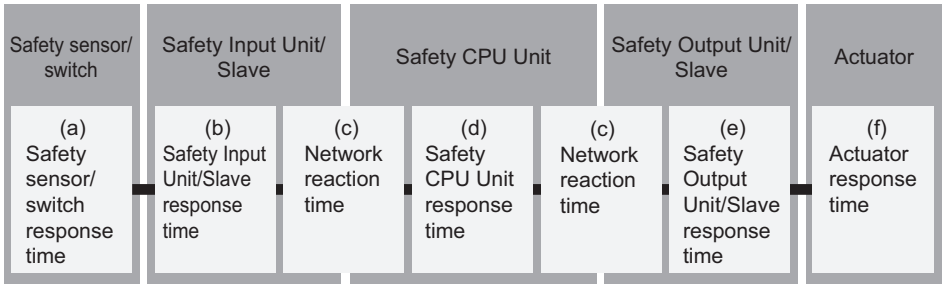
The safety response performance (safety reaction time) is the maximum time required to turn OFF an output when considering failures and breakdowns of safety chains*1.
In the safety system design, the safety distance is calculated from the safety response performance.
For all safety chains, the longest time required to stop running devices from when a safety input was activated must satisfy the required specifications.
This section describes the safety response performance of the Safety I/O Block.

***1.** A safety chain is a logical connection for achieving a safety function that connects from a safety input device to a safety output via the Safety I/O Block or Safety Control Unit.

9-1-1 Calculating Safety Response Performance

This section describes the calculation method for safety response performance separately for when using and when not using CIP Safety communications.

a. When performing safety control with a safety controller using CIP Safety communications
   As shown in the figure below, the safety response performance is determined by the sum of (a) Safety sensor/switch response time, (b) Safety Input Unit/slave response time, (c) Network reaction time, (d) Safety controller response time, (e) Safety Output Unit/slave response time, and (f) Actuator response time.
   The number of elements and the duration of time will vary depending on the path of the safety chains.

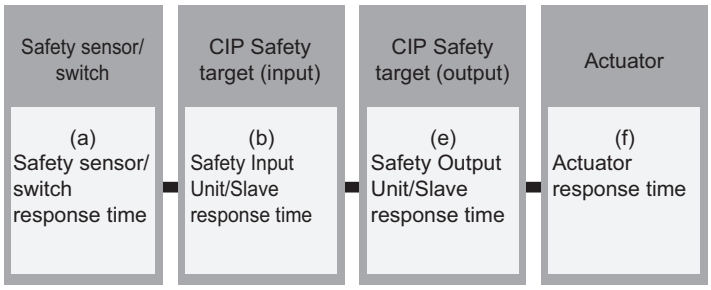


Letter	Time element	Value
(a)	Safety sensor/ switch response time	This is the response time that is required for a safety sensor or switch, such as a light curtain, to turn OFF. The value is defined for each sensor or switch.

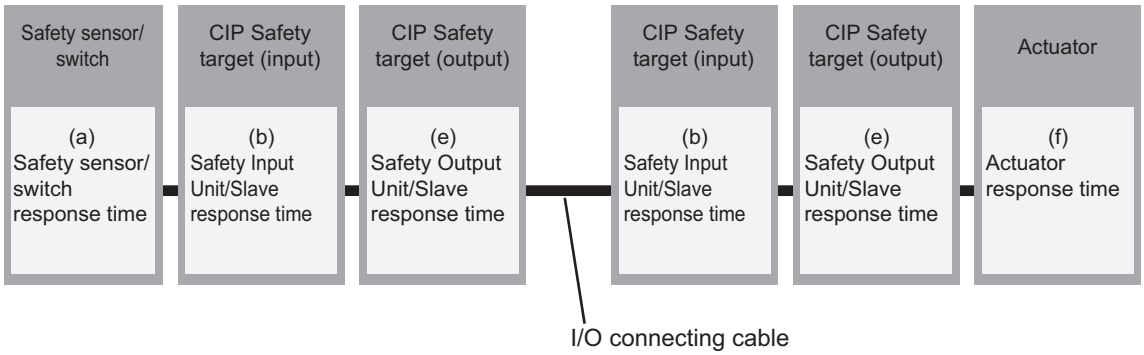
Letter	Time element	Value
(b)	Safety Input Unit/slave response time	This is the input response time of a CIP Safety target. There are the following three times depending on the channel mode and safety requirement level of the input terminal. • When using dual channel 10 ms • When using single channel and there is no dangerous failure of a safety input (safety requirement level is Cat.2/PLc/SIL1) 10 ms • When using single channel and consideration is given to a dangerous failure of a safety input (safety requirement level is Cat.2/PLd/SIL2) 260 ms For the input response time of the Safety I/O Block, add the ON->OFF delay time of the input terminal to the times above.
(c)	Network reaction time	This is the response time of the CIP Safety connection. For the NJ/NX/NY Series, it is calculated and displayed in Sysmac Studio. *1 For details on how to check the network reaction time, refer to *Connection Parameter Editing Procedure* on page 7-32.
(d)	Safety controller response time	This is the response time of the safety controller. Refer to *NX-series Safety Control Unit/Communication Control Unit User's Manual (Cat. No. Z395)* for Safety CPU Units. *1
(e)	Safety Output Unit/slave response time	This is the output response time of a CIP Safety target. There are the following two times depending on the channel mode and safety requirement level of the output terminal. • When using dual channel 5 ms • When using single channel 5 ms (response time under the assumption that there will be no failure because the single channel is up to Cat.2) For the output response time of the Safety I/O Block, add the ON->OFF delay time of the output terminal to the times above. When using the logic function of the Safety I/O Block, the logic execution time is also included in this time.
(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.** When connecting the Unit to a Controller from another company, check the instruction manual for the support software of the Controller to be connected.

b. When performing safety control with a safety application not using CIP Safety communications
For the safety response performance, the times of (c) and (d) of a. are excluded because the processing of inputs and outputs is performed in the Safety I/O Block.
• Configuration for an individual Safety I/O Block



- Configuration for connecting two Safety I/O Block units with an I/O connection cable
  For the safety response performance, add the total time of (b) and (e) for the number of connected Safety I/O Block units.



Precautions for Correct Use

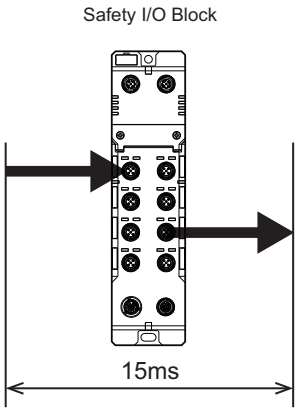
- For the calculation of the safety response performance, add the effect of "ON->OFF delay time of input terminal" and "ON->OFF delay time of output terminal".

When Using an Individual Safety I/O Block Configuration

The slave response time (I/O response time) for an individual Safety I/O Block is as follows, depending on the combination of safety input and safety output settings.

Safety input	Safety output	Safety requirement level	Slave response time
Dual channel	Dual channel	Cat.4/PLe/SIL3	15 ms (= 10 ms + 5 ms)
Dual channel	Single channel	Cat.2/PLc/SIL1	15 ms (= 10 ms + 5 ms)*1
Single channel	Dual channel	Cat.2/PLd/SIL2	265 ms (= 260 ms + 5 ms)
Single channel	Single channel	Cat.2/PLc/SIL1	15 ms (= 10 ms + 5 ms)*1

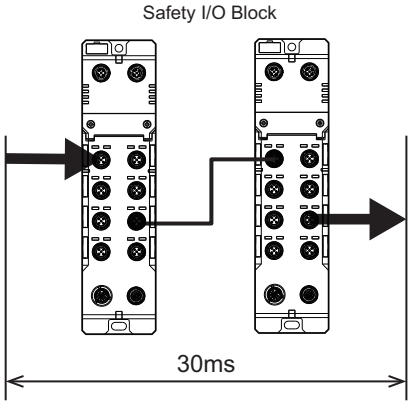
***1.** The safety requirement level is Cat.2/PLc/SIL1, and the response time assumes that no fault has occurred. When the safety output is used in single-channel mode, the fault detection time is 265 ms + network response time. Refer to *2-1-3 Safety Specifications* on page 2-4 for details.



When I/O Cable Connection Configuration

The I/O response performance when you connect two Safety I/O Block Units with an I/O cable to use a safety application under the following conditions is 30 ms.

- CIP Safety communications are not used.
- Safety input terminals and safety output terminals are all set to dual channel.
- "ON->OFF delay time of input terminal" and "ON->OFF delay time of output terminal" are not added.



9-1-2 Verifying Safety Response Performance

Check that the calculated safety response performance for all safety chains satisfies the required specifications. If the calculated safety response performance does not satisfy the required specifications, consider the following measures and correct the software or hardware design.

- Reduce the data packet interval (EPI) value of CIP Safety connections.
  Refer to *Connection Parameter Editing Procedure* on page 7-32 for the data packet interval (EPI).

10

Security Guidelines

This chapter describes the security guidelines for using the Safety I/O Block.
Refer to *Security Guideline for Factory Automation System (Cat. No. P162)* for security measures for the overall FA system. Additionally, refer to *Security Guideline for NJ/NX Controller (Cat. No. P166)* for security measures that you can implement using the NJ/NX-series CPU Units.

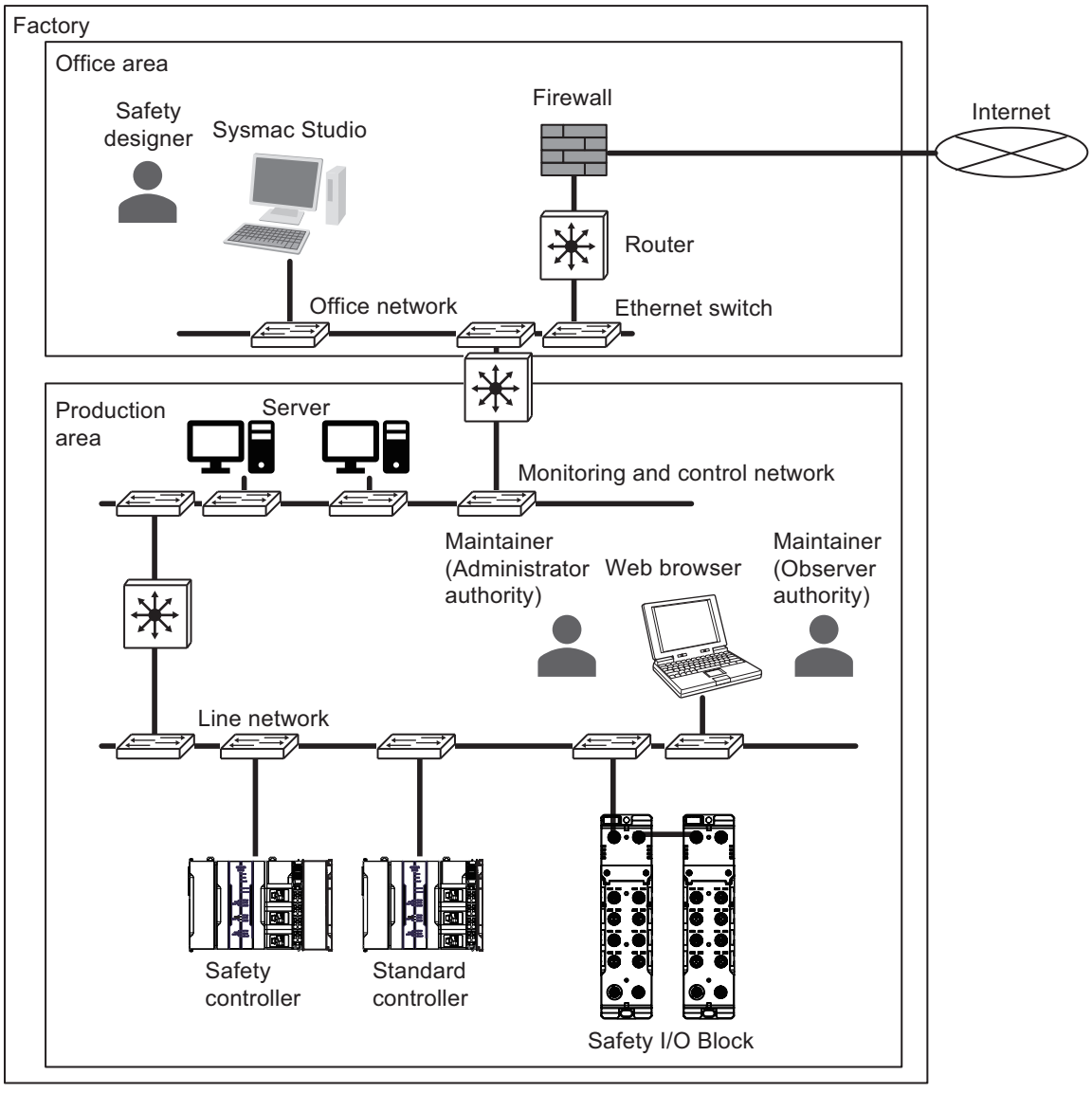
10-1 Defense in Depth Provided by the Safety I/O Block 10-2
10-1-1 Operating Environment of the Safety I/O Block..... 10-2
10-1-2 Security Measures for the Technical Layer Using the Safety I/O Block 10-3
10-2 Security Functions of Safety I/O Block to Protect Assets 10-5
10-2-1 Protecting Data on Communication Lines 10-5
10-2-2 Blocking External Attacks on the Safety I/O Block 10-7
10-2-3 Preventing Unauthorized Operations on the Safety I/O Block 10-9
10-2-4 Preventing Tampering of the Assets of the Safety I/O Block..... 10-10
10-2-5 Protecting Safety Application Files and Backup Files 10-11
10-2-6 Preventing Repudiation 10-12
10-3 Applying Security Patches 10-13
10-3-1 Updating the Safety I/O Block 10-13
10-3-2 Updating the Sysmac Studio 10-13
10-3-3 Updating the OS of Your PC..... 10-13
10-4 Safely Disposing of Equipment 10-14
10-4-1 Erasing Your Assets in the Safety I/O Block..... 10-14

10-1 Defense in Depth Provided by the Safety I/O Block

The Safety I/O Block provides multiple security functions to achieve defense in depth.
This section describes the defense in depth achieved by the security functions of the Safety I/O Block.

10-1-1 Operating Environment of the Safety I/O Block

The Safety I/O Block effectively utilizes its security functions to protect the operations and assets of equipment and the Safety I/O Block itself.
Segmenting the network, such as by separating it into a production area and office area, as shown in the figure below is effective in minimizing the scope of the impact when an attack is received from outside. Also implement security measures for the peripheral devices of the Safety I/O Block. Refer to the manuals of the peripheral devices for the specific procedures.



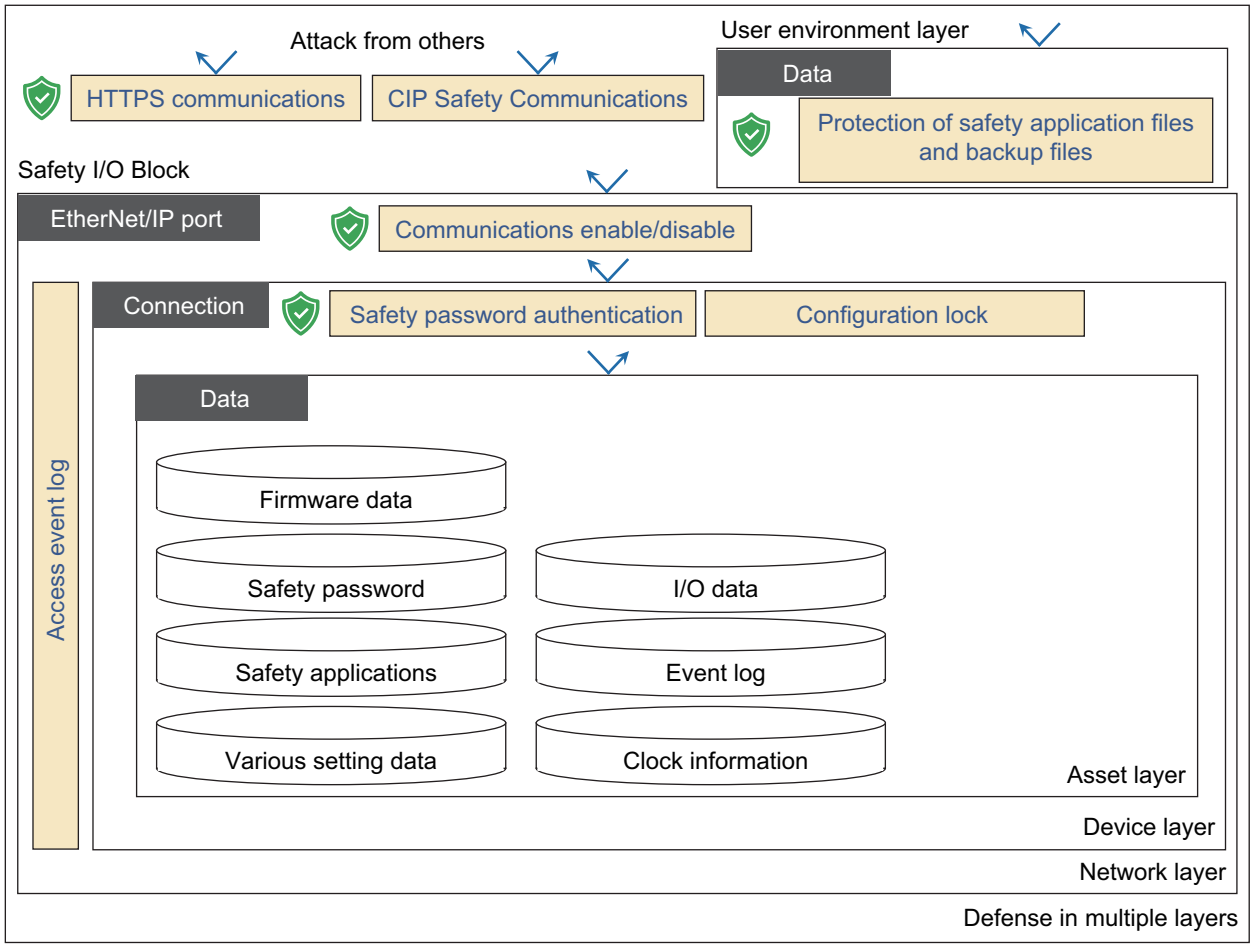
10-1-2 Security Measures for the Technical Layer Using the Safety I/O Block

The Safety I/O Block provides security functions to enable protection of your assets by defense in depth. Even if an attacker breaks through one layer, the security functions in the layer closest to the assets will be able to protect the assets.

Depending on the purpose and the type of threat, provide defense in depth by combining the measures described in the *Security Guideline for Factory Automation System (Cat. No. P162)* and the multiple security functions described in this section.

In this section, the things that you should do in particular using the security functions are described. Read the section in conjunction and take necessary measures.

In addition, be sure to check that each security function is operating as intended yourself.



The table below shows the functions provided in each layer.

Layer to protect assets	Purpose	Function that the Safety I/O Block provides	Reference
Network layer	Protecting data on communication lines	HTTPS communications function (Web UI)	*HTTPS Communications Function (Web UI)* on page 10-5
		CIP Safety communications function	*CIP Safety Communications Function* on page 10-5
	Blocking external attacks on the Safety I/O Block	Communications enable/disable setting function	*Communications Enable/Disable Settings* on page 10-7
Device layer	Preventing unauthorized operations on the Safety I/O Block	Safety password authentication function	*Safety Password Authentication Function* on page 10-9

Layer to protect assets	Purpose	Function that the Safety I/O Block provides	Reference
	Preventing tampering of the assets of the Safety I/O Block	Configuration lock function	*Configuration Lock Function* on page 10-10
User environment layer	Protecting safety application files and backup files	Protection of safety application files and backup files	*Protecting Safety Application Files and Backup Files* on page 10-11
Common to all layers	Preventing repudiation	Access event log function	*Access Event Log Function* on page 10-12

10-2 Security Functions of Safety I/O Block to Protect Assets

This section describes the security functions that the Safety I/O Block provides.

10-2-1 Protecting Data on Communication Lines

Equipment connected to a network is subject to the risk of cyberattacks over the network. Use the following functions to prevent information disclosure from data flowing over communication lines, tampering, and denial of service.

HTTPS Communications Function (Web UI)

The HTTPS communications function is intended to improve the security of communications between the Web browser and the Safety I/O Block.
Since it encrypts and then adds hash values to communications data before sending and receiving, it is useful to prevent eavesdropping and tampering by a third party.
Refer to *7-2 Overview of the Web UI* on page 7-17 for details on the HTTPS communications function.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
○	○		○	○	

● Things That You Should Do

- To enhance security, use the Web UI with the latest version of your Web browser.
- Install a firewall (blocking unused communications ports and restricting communications hosts) for the networks of control systems and equipment to isolate them from IT networks, and make sure that the connections to the safety control system of the Web UI are established inside the firewall.
- Use a virtual private network (VPN) for remote access to control systems and equipment from the Web UI.
- A CA certificate is required to use the HTTPS communications function. Download the CA certificate from the OMRON website, and then install it in the Web browser. If an attempt is made to access the Safety I/O Block while the CA certificate is not installed, an error occurs in the Web browser. Refer to *8-3 HTTPS Communications Function* on page 8-8 for details.
- To start up the Web UI, there is the method to enter an IP address and the method to enter a domain name. When using the method to enter an IP address, take measures to ensure that an unauthorized device does not intercept communications between the PC and the Safety I/O Block. Refer to *7-2-5 Web UI Startup Procedure* on page 7-21 for details on measures.

CIP Safety Communications Function

The CIP Safety communications function is a safety function for exchanging data cyclically between the CIP Safety originator (safety controller) and CIP Safety target (Safety I/O Block). The reliability of communications is guaranteed by mechanisms such as TUNID, SCCRC, and SCTS.

Refer to *6-2 CIP Safety Communications* on page 6-4 for details on the CIP Safety communications function.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
○	○			○	

10-2-2 Blocking External Attacks on the Safety I/O Block

Equipment connected to the Internet is subject to the risk of cyberattacks over the network. Block external attacks to prevent malfunctions of production equipment and accidents.

Communications Enable/Disable Settings

The communications enable/disable setting function allow you to enable or disable each communications function of the Safety I/O Block. Prevent information leakage and attacks by disabling unused communications functions to reduce the number of access routes to the Safety I/O Block from the outside.
The communications enable/disable setting function can be configured for the following targets.

Target	Description
EtherNet/IP port	The Ethernet communications function of EtherNet/IP ports 1 and 2 can be set to enable or disable for each port. Both of the ports are enabled by default.
DHCP (IP address settings)	The function to obtain the IP address from a DHCP server can be set to enable or disable. It is disable by default.
SNTP (automatic clock adjustment)	The function to obtain the clock information from an SNTP server can be set to enable or disable. It is disable by default.

● EtherNet/IP Port Communications Enable/Disable Settings

Configure the communications enable/disable setting of an EtherNet/IP port by using explicit message communications.
The commands to send are as follows.

Implementation details	Send command item	Send command value
EtherNet/IP port communications enable/disable settings	Service code	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01 hex: Port1 02 hex: Port2
	Attribute ID	30 (Communication Port Enable)
	Service data	TRUE: Enabled FALSE: Disabled

Refer to *Explicit Message Server Function* on page 6-7 for the method to access CIP objects through an explicit message.

● DHCP Communications Enable/Disable Setting

To set the DHCP communications enable/disable setting using Sysmac Studio, set **Obtain from DHCP server** on the screen for setting the IP address as follows.
To set the DHCP communications enable/disable setting using the Web UI, set **Obtain from DHCP server** for the IP address on the TCP/IP Settings screen of the Web UI as follows.

DHCP communications	Obtain from DHCP server
Enable	Select the check box.
Disable	Clear the check box.

Refer to *7-10-3 Setting by Sysmac Studio* on page 7-74 for the procedure to set the IP address with Sysmac Studio.
Refer to *7-10-4 Setting by Web UI* on page 7-76 for details on the TCP/IP Settings screen of the Web UI.

● SNTP Communications Enable/Disable Setting

To set the SNTP communications enable/disable setting using Sysmac Studio, set **SNTP Settings** on the screen for setting automatic clock adjustment as follows.
To set the SNTP communications enable/disable setting using the Web UI, set **NTP/SNTP server IP address** on the Automatic Clock Adjustment Settings screen of the Web UI as follows.

SNTP communications	Setting
Active	Set the IP address.
Inactive	Do not set the IP address.

Refer to *Procedure Using Sysmac Studio* on page 7-91 for the procedure to configure automatic clock adjustment in Sysmac Studio.
Refer to *Procedure Using the Web UI* on page 7-92 for details on the Automatic Clock Adjustment Settings screen of the Web UI.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
○	○		○	○	

● Things That You Should Do

- Security measures have not been taken for DHCP and SNTP protocols. When you use the DHCP and SNTP protocols, use your application to ensure security.
- Use the function in combination with other measures, such as installing a firewall to prevent unauthorized packets from reaching the Safety I/O Block.

10-2-3 Preventing Unauthorized Operations on the Safety I/O Block

Prevent unauthorized operations on the Safety I/O Block to protect safety applications and equipment, which are your important intellectual property, from theft, unauthorized utilization, production equipment malfunctions, and accidents.

Safety Password Authentication Function

Changes to setting data and operations of the Safety I/O Block carry the risk of causing personal injury or property damage. Prevent operation from operators without authority by restricting the functions that operators can operate based on their authority. The safety password authentication functions of the Safety I/O Block are as follows.

Function	Description
Restriction of operations affecting function safety	Authentication by safety password is required when executing the memory all clear, restart, configuration lock and unlock, change operation mode, and safety password functions.
Restriction of Web UI operations	The Web UI has the operation authorities of administrator and observer. Only an administrator can change the setting data. Authentication by safety password is required to use the Web UI as an administrator.

Refer to the page of each function for details on the restriction of operations affecting function safety. Refer to *7-2-2 Operation Authorities of the Web UI* on page 7-17 for a details on the restriction of Web UI operations. Refer to *7-18 Setting the Safety Password* on page 7-104 for details on setting the safety password.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
○	○	○	○	○	○

● Things That You Should Do

- Be sure to set a safety password for the Safety I/O Block.
- Change the safety password yourself on a periodic basis.
- Set and manage the safety password appropriately to prevent unauthorized use by a third party.
- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- To enhance the confidentiality of the safety password, do not set the same password as other devices.
- CIP Safety, which this product complies with, is a safety communications mechanism for the purpose of achieving device safety in FA applications in factories and other industrial environments. To mitigate security risks such as unauthorized operation of this product, implement appropriate measures across the entire system in addition to the product's functions, including controlling access to the production area and restricting access to the network.

10-2-4 Preventing Tampering of the Assets of the Safety I/O Block

Prevent the tampering of the setting data, which is your important intellectual property, and unauthorized execution of safety applications that are not intended to be executed.

Configuration Lock Function

The configuration lock function prevents setting data related to the safety of the Safety I/O Block and safety applications that are executed from being changed unintentionally. The setting data cannot be changed for the Safety I/O Block while the configuration is locked. Furthermore, a selected safety application cannot be changed to execute another safety application.
Refer to *7-17 Configuration Lock* on page 7-99 for details on the configuration lock.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
	○				

● Things That You Should Do

- Be sure to lock the configuration before full operation of the Safety I/O Block.

10-2-5 Protecting Safety Application Files and Backup Files

Prevent the unauthorized use of your design assets, which are your important intellectual property.

Protecting Safety Application Files and Backup Files

The safety application files and backup files are protected with passwords to prevent unauthorized access to the files. The passwords that protect the files are the safety application file password and the backup file password, respectively.
Refer to *7-9-5 Exporting a Safety Application File* on page 7-68 for details on the safety application file password. Refer to *7-19 Backup* on page 7-108 for details on the backup file password.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
	○				

● Things That You Should Do

- Set and manage the safety application file password and backup file password appropriately to prevent unauthorized use by a third party.
- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.

10-2-6 Preventing Repudiation

To protect your assets, it is also important to grasp the fact that they have been subjected to unauthorized operations. In addition, in the event of a security incident, it is necessary to determine the cause and circumstances of the incident. Recording security breaches and cyberattacks allows you to confirm who did what and when, and can be used as a repudiation preventive measure when problems occur.

Access Event Log Function

The Safety I/O Block records the operations that the user performs on the Safety I/O Block using Sysmac Studio or the Web UI as access event logs. The access event logs can be read and cleared using Sysmac Studio or the Web UI.
Refer to *11-2-1 Event Log Function* on page 11-6 for details on the access event log function.

● Threats That Can Be Addressed

S: Spoofing	T: Tampering	R: Repudiation	I: Information leak	D: Denial of service	E: Elevation of privilege
		○			

● Things That You Should Do

- If the access event log is cleared, you cannot prevent repudiation. If the number of events exceeds the number of records permitted, the Safety I/O Block overwrites the access event log from older information. It is recommended to back up the logs periodically and keep them for a certain period of time.

10-3 Applying Security Patches

To protect your assets and production from cyberattacks progressing day by day, it is effective to keep your devices up-to-date for higher security strength.
This section describes the functions that the Safety I/O Block provides for updating.

10-3-1 Updating the Safety I/O Block

To add functionality, improve operability, and enhance security, always keep the Safety I/O Block updated to the latest version for use.

Firmware Update Function

The firmware update function is used to update the firmware used by the Safety I/O Block to the latest version.
Refer to *8-14 Firmware Update Function* on page 8-35 for details on the firmware update function.
When you update the firmware, an event is logged in the event log. When referring to the change history, check the events as described in *11-2-1 Event Log Function* on page 11-6.
Check the OMRON website for details on how to obtain the latest firmware file.

● Things That You Should Do

- Regularly check that the firmware of the Safety I/O Block is the latest version.
- If a backup file is restored after executing the firmware update function, set the safety password to enhance the security.

10-3-2 Updating the Sysmac Studio

To add functionality, improve operability, and enhance security, always keep Sysmac Studio updated to the latest version for use.
Refer to *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on auto-updating Sysmac Studio.

10-3-3 Updating the OS of Your PC

To avoid security risks arising from vulnerabilities in the OS, always keep the OS of your PC on which Sysmac Studio, Web UI, and its Support Software are running up-to-date.

10-4 Safely Disposing of Equipment

This section describes the functions that the Safety I/O Block provides for disposal.

10-4-1 Erasing Your Assets in the Safety I/O Block

Disposing of or transferring the Safety I/O Block carries the risk of information disclosure, allowing third parties to view setting data and other information saved in the Safety I/O Block.
Before disposal or transfer, erase the setting data at your own responsibility.

Clear All Memory Function

The clear all memory function is used to completely clear the setting data in the Safety I/O Block. To completely clear the setting data, select the clear all memory function in the Web UI to clear also the *event logs* and *safety applications set in the Web UI*. Note that the *event logs* and *safety applications set in the Web UI* are not cleared when the clear all memory function of Sysmac Studio is executed.
Refer to *8-2 Clear All Memory Function* on page 8-4 for details on the clear all memory function.
If the clear all memory function fails, the Safety I/O Block may be faulty. Contact your nearest OMRON branch or sales office.

11

Troubleshooting

This chapter describes how to check whether errors are occurring on the Safety I/O Block, and how to perform troubleshooting when errors occur.

11-1 Checking for Errors 11-2
11-1-1 How an Error Is Notified and What Information to Check 11-2
11-1-2 How to Check for Errors 11-2
11-1-3 Operating Status Monitor Function 11-3
11-2 Checking for Errors and Troubleshooting with the Event 11-6
11-2-1 Event Log Function 11-6
11-2-2 Checking Events Using Sysmac Studio 11-6
11-2-3 Checking Events Using the Web UI 11-9
11-2-4 Event Details and Troubleshooting 11-12

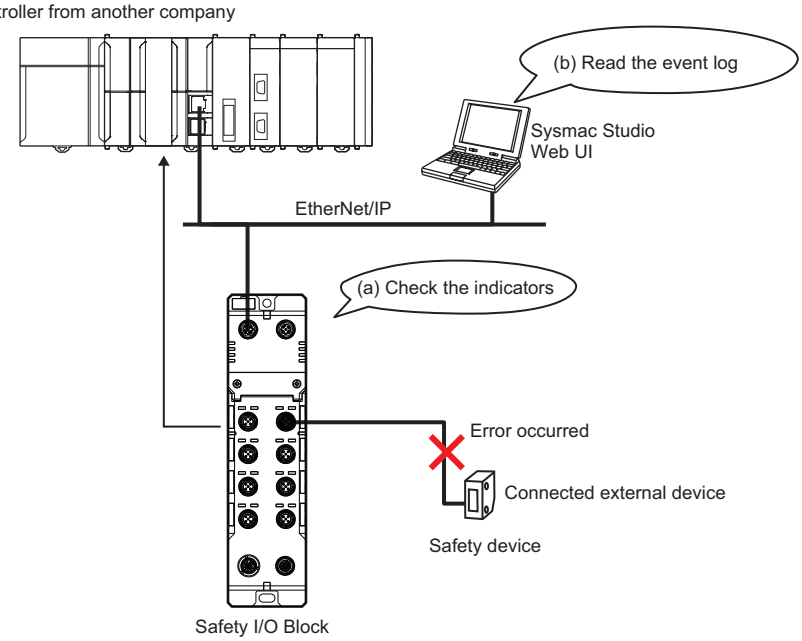
11-1 Checking for Errors

This section describes the error notification and check methods, and the basic procedure for checking errors.

11-1-1 How an Error Is Notified and What Information to Check

When the Safety I/O Block detects an error, you are notified in the following ways.
When an error is notified, check the status of the Unit and take corrective action.

Controller
· NJ/NX/NY-series CPU Unit
· NX-series Safety Control Unit
· Controller from another company



Letter	Notification method	Check method	Reference
(a)	Notify of Safety I/O Block error by indicator	Visually check status of each indicator on the Safety I/O Block.	*3-2-1 Status Indicators* on page 3-5 *3-2-2 I/O Indicators* on page 3-8
(b)	Notify of error occurrence on the Safety I/O Block and information about it by event	Read and check the events of the Safety I/O Block on the CIP Safety Monitor screen of Sysmac Studio or on the Operating Status Monitor screen of the Web UI.	*11-2 Checking for Errors and Troubleshooting with the Event* on page 11-6

11-1-2 How to Check for Errors

The following table shows the basic procedure to check for errors.

Step	Item	Description	Reference
1	Finding the occurrence of an error	Find whether or not an error occurred using the indicator lighting status.	*3-2-1 Status Indicators* on page 3-5 *3-2-2 I/O Indicators* on page 3-8

Step	Item	Description	Reference
		⇩	
2	Isolating the error cause	If there is an error, perform the following checks to isolate the cause.	-
		Check each status information of the Safety I/O Block.	*11-1-3 Operating Status Monitor Function* on page 11-3
		Check the event log of the Safety I/O Block.	*11-2 Checking for Errors and Troubleshooting with the Event* on page 11-6
		⇩	
3	Addressing the cause of the error	After you isolate the cause of the error, take the appropriate measure to address it.	-

11-1-3 Operating Status Monitor Function

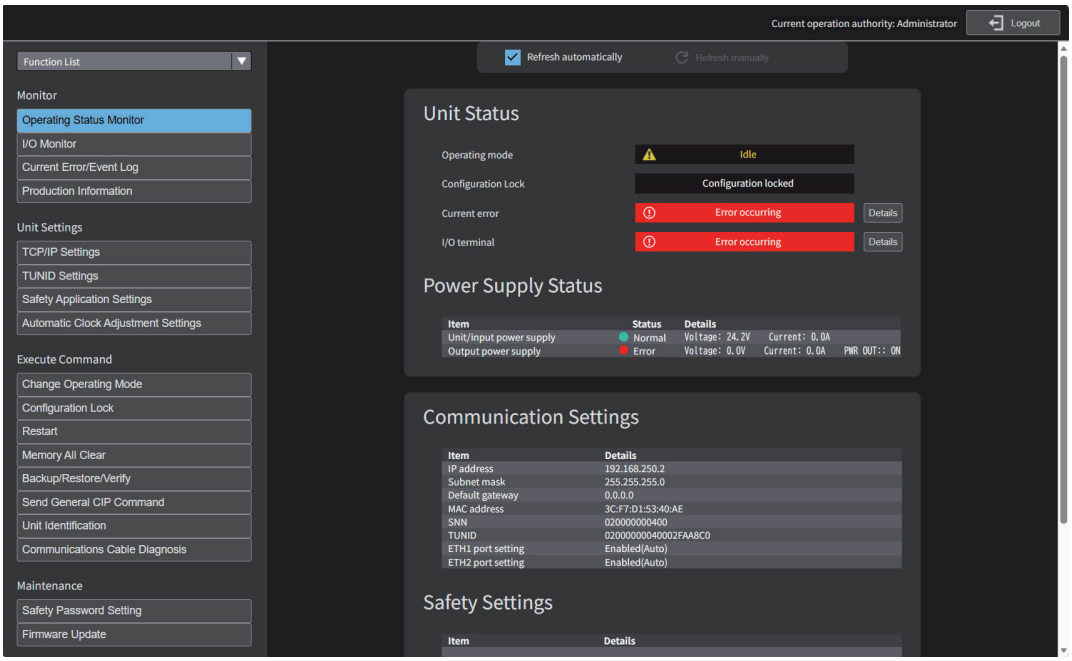
The operating status monitor function displays each status information of the Safety I/O Block.

Purpose of Operating Status Monitor Function

The purpose of the operating status monitor function is to understand the current status of the Safety I/O Block from each status information.

Procedure for Using Operating Status Monitor Function

Check the operating status of the corresponding Unit in the Operating Status Monitor screen of the Web UI.



Details on Operating Status Monitor Function

The operating status monitor function allows you to check **Unit Status**, **Power Supply Status**, **Connection Status**, **Communications Settings**, and **Safety Settings**.

● Unit Status

Operating mode, **Configuration lock**, **Current error**, or **I/O terminal** is displayed in **Unit Status**.

a. Operating mode
The current operating mode is displayed. Refer to *6-8 Operating Modes* on page 6-47 for details on operating modes.

b. Current errors
The information displayed as **Current error** is as follows.

Display	Description
Normal	Unit is in normal status
Error occurring	An error is occurring on the Unit

Clicking the **Details** button when **Error occurring** is displayed transitions to the *Current Error/Event Log screen*.

c. Configuration lock
The information displayed as **Configuration lock** is as follows.

Display	Description
Configuration locked	The configuration is locked.
Configuration unlocked	The configuration is unlocked.

Refer to *7-17 Configuration Lock* on page 7-99 for details on the configuration lock.

d. I/O terminal
The information displayed as **I/O terminal** is as follows.

Display	Description
Normal	The safety I/O terminal is normal.
Error occurring	An error has occurred in the safety I/O terminal.

Clicking the **Details** button when **Error occurring** is displayed transitions to the *I/O Monitor screen*.

● Power Supply Status

Power Supply Status displays the status and value of each power supply terminal. The following information is displayed.

Item	Description
Status	Normal or error*1
Details	Voltage value and current value

***1.** If the output power supply (PWR output port) is not used, OFF is displayed in the Status field of Output power supply (PWR output port).

● Communications Settings

Various communications setting information is displayed in **Communications Settings**. The following information is displayed.

- IP address
- Subnet mask
- Default gateway
- MAC address
- SNN (Safety Network Number)
- TUNID (Target Unit Network Identifier)
- Whether the ETH1 port is enabled or disabled, and the communications speed and communications mode
- Whether the ETH2 port is enabled or disabled, and the communications speed and communications mode

● Safety Settings

Various safety setting information is displayed in **Safety Settings**. The following information is displayed.

Item	Description
Configuration	Configured or not configured
Rotary switch (SETTING)	Values of rotary switches in SETTING
CFUNID	Values of configuration unique identification (CFUNID)
Application name	Names of set safety applications
Creator name	Name of the creator of the set safety application
Comment	Any comment
SCCRC	Values of safety configuration CRC (SCCRC)
SCTS	Values of safety configuration time stamp (SCTS)

In addition, the values of all configuration assembly data are displayed as a parameter list. Refer to *A-2-3 Configuration Assembly Data* on page A-7 for details on the configuration assembly data.

11-2 Checking for Errors and Troubleshooting with the Event

This section describes how to check for errors with the current error event and event logs, and perform troubleshooting.
Use Sysmac Studio or the Web UI for the event check.

11-2-1 Event Log Function

The event log function records events that are categorized into the following categories.

a. System event logs
These logs record events such as status changes that occurred internally in the Safety I/O Block, causes of safety stops, and communications errors.
They are intended to be used for checking whether the safety functions operate correctly, identifying the causes of errors and stops, and maintaining safety.

b. Access event logs
These logs record the settings configured and commands executed for the Safety I/O Block by the user or by another device.
They are intended to be used for identifying the person who performed certain actions in the event of security issues such as data tampering or information leaks, and to prevent the person denying the actions.

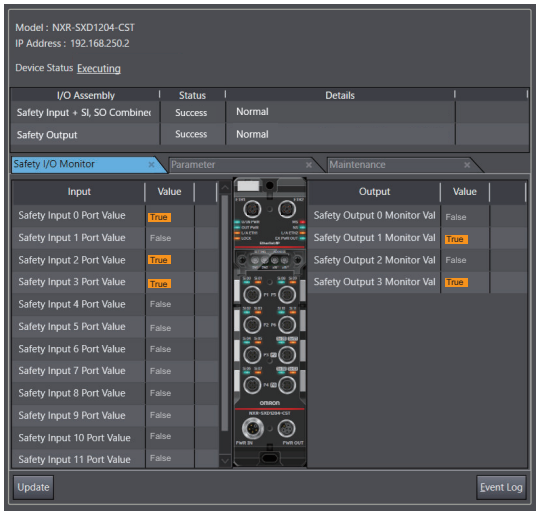
11-2-2 Checking Events Using Sysmac Studio

You can check the events on the Current Error screen and Event Log screen.

Current Error Screen and Event Log Screen Display Method

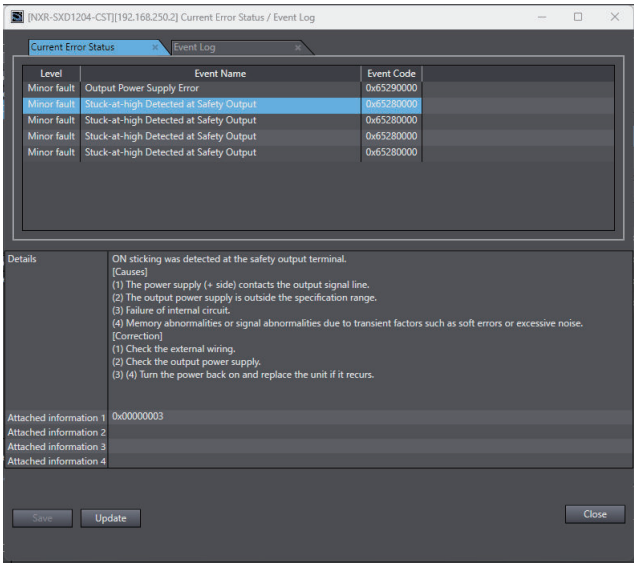
This section describes how to display the current errors and event logs with Sysmac Studio.

1 Click **Tools** - **CIP Safety Monitor** to open the CIP Safety Monitor screen.

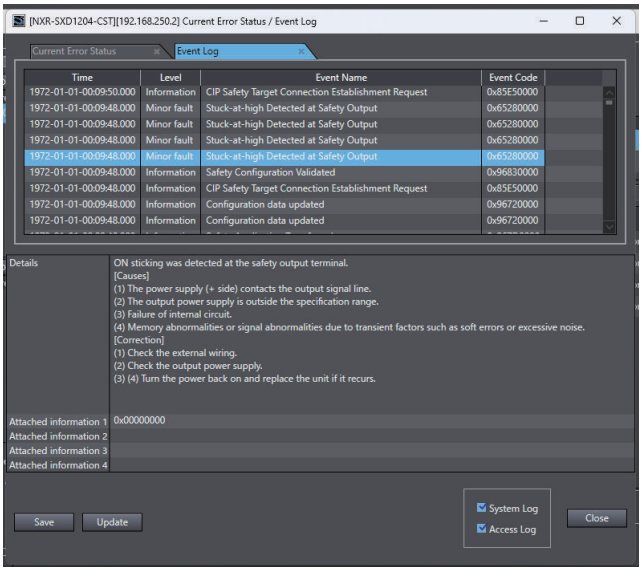


2 Select the Safety I/O Block from **CIP Safety Target List**.
The device status and current I/O assembly errors of the Safety I/O Block are displayed.

3 Click the **Event Log** button at the bottom right.
The current errors are displayed.

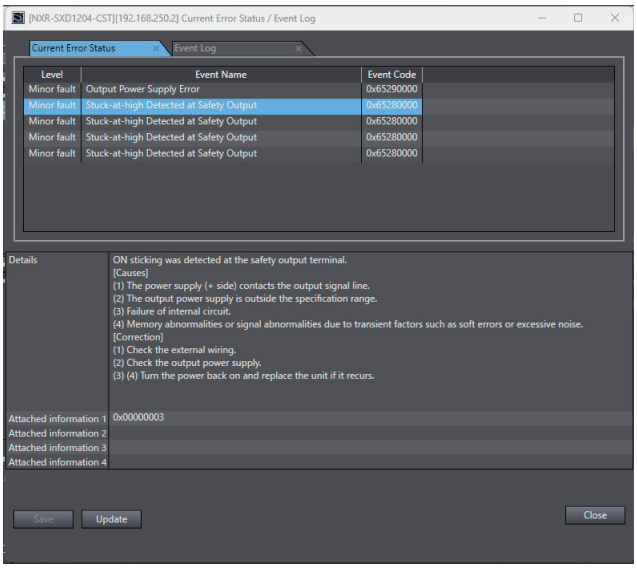


4 Click the **Event Log** tab.
The event logs are displayed.



Current Error Screen

This section describes the functions of the display items and operation buttons in the Current Error screen.



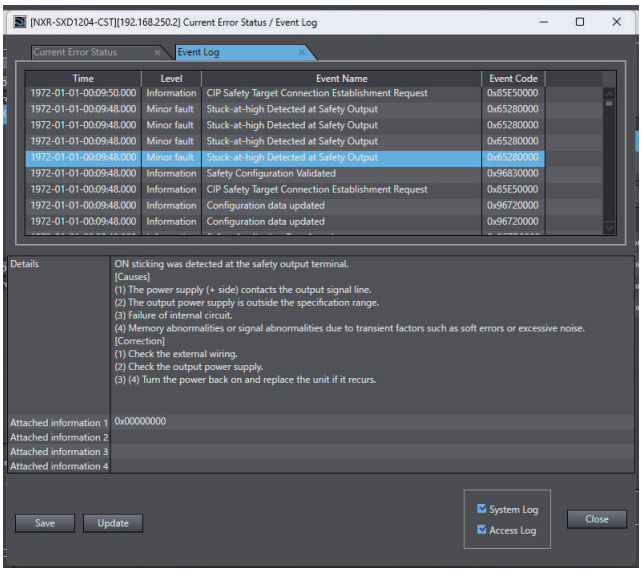
- Displayed item

Item	Description
Level	This indicates the level of influence that the error (event) has on control.
Event name	Displays the name of the event that occurred.
Event code	This is the code of the error (event) that occurred in the Safety I/O Block.
Details	Displays the cause, measure, and attached information for the selected event.
Attached information 1 to 4	

- Operation buttons
  a) Update
     Updates the information for the current error to the latest information.

Event Log Screen

The display items and details of the Event Log screen are as follows.



- Displayed item

Item	Description
Date/Time	Displays the date and time that the event occurred. *1
Level	This indicates the level of influence that the error (event) has on control.
Event name	Displays the name of the event that occurred. This Unit can display the most recent 100 events.
Event code	This is the code of the error (event) that occurred in the Safety I/O Block.
Details	Displays the cause, measure, and attached information for the selected event.
Attached information 1 to 4	

***1.** When this Unit does not have time information, "-----" is displayed.

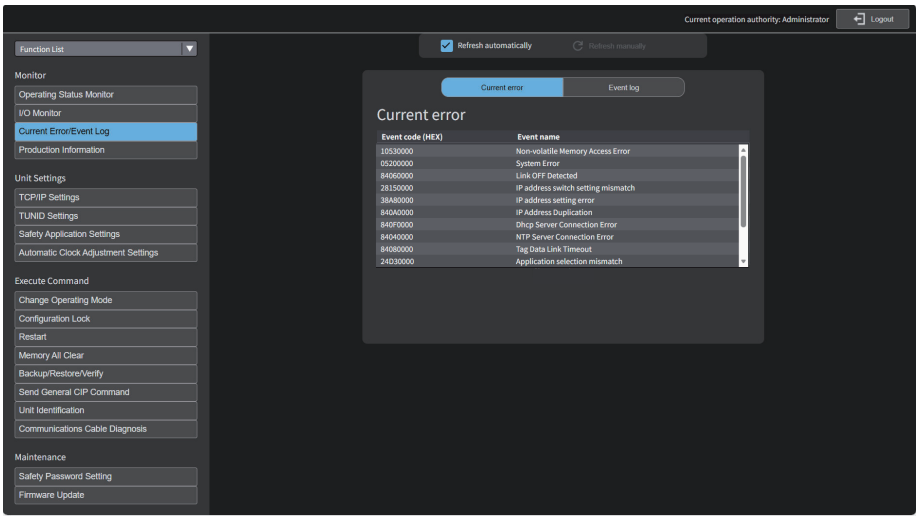
- Operation buttons
  a) Update
  Updates the data of the event log to the latest data.
  b) Save
  Saves the event log.
  c) Clear
  Clears the event log. The safety password is required for clearing.
  d) “System log” and “Access log” check boxes
  Displays the selected logs. Both of the check boxes are selected by default.

11-2-3 Checking Events Using the Web UI

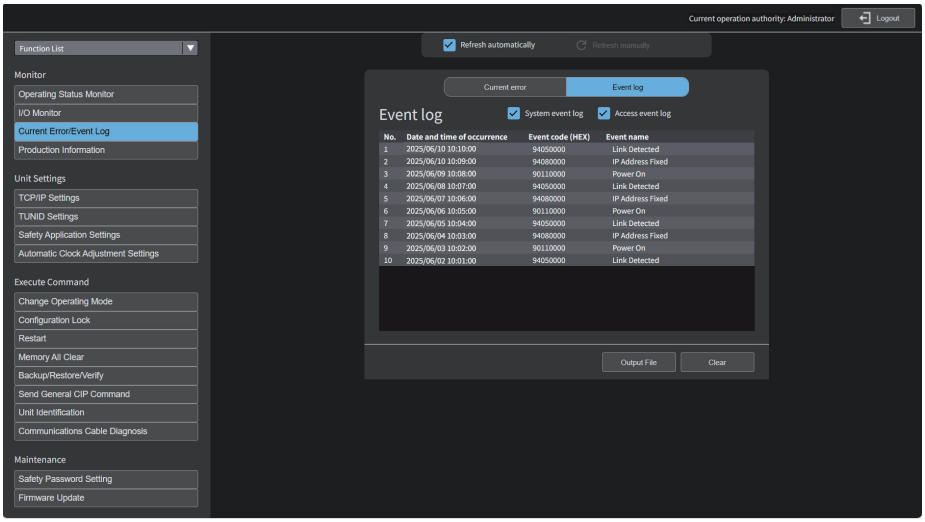
Check the events on the Current Error/Event Log screen of the Web UI.
The Current Error/Event Log screen displays the current error and event logs of the corresponding Unit.
The event logs can be saved to the PC in CSV format. Furthermore, the event logs can be cleared from the internal memory of the Safety I/O Block.

Current Error Screen and Event Log Screen Display Method

1 Click **Current Error/Event Log** from the left menu.
The following Current error screen is displayed.

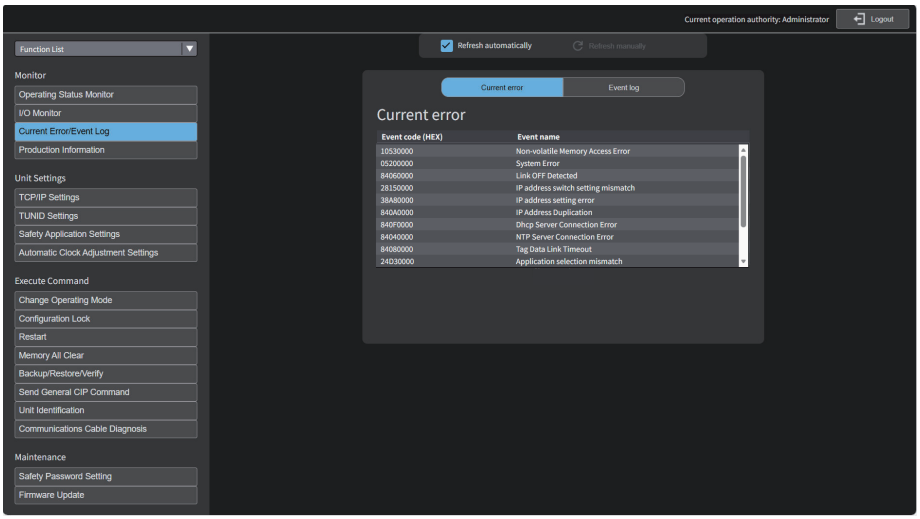


2 Click the **Event log** button.
The following Event log screen is displayed.



Current Error Screen

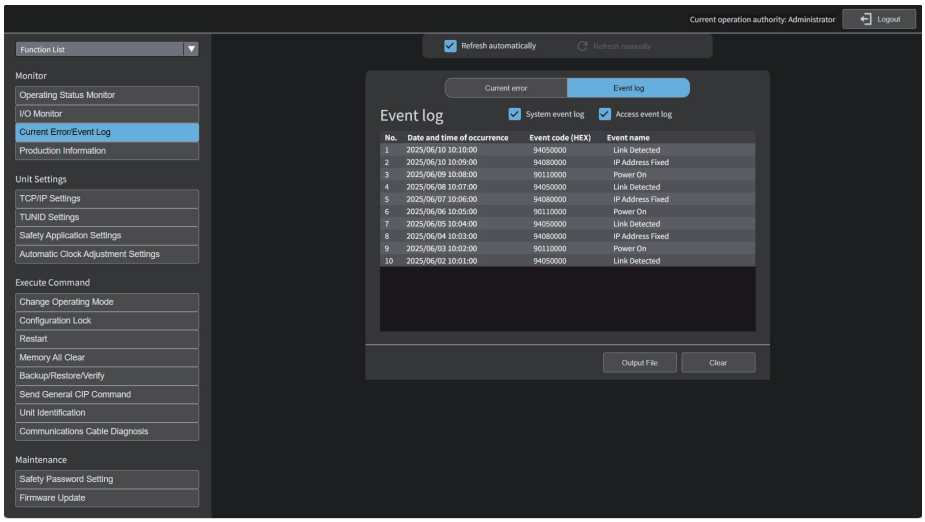
The **Current error** screen displays the following information about the current error.



Item	Description
Event code (Hex)	Event code of error that occurred
Event name	Event name of error that occurred
Attached information	Attached information for event that occurred

Event Log Screen

The **Event log** screen displays the following information about event logs that have occurred up until now.



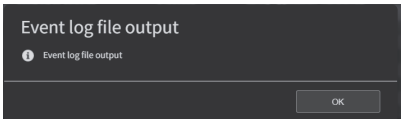
Item	Description
Date and time of occurrence	Time and date that event occurred
Level	Level of the event that occurred
Event name	Event name of event that occurred
Event code (Hex)	Event code of event that occurred
Attached information	Attached information of event that occurred

If you select the **System event log** check box, the system event log is displayed. If you select the **Access event log** check box, the access event log is displayed. Both of them can be displayed.

● Saving Event Log

With event log saving, both event logs are saved regardless of whether the **System event log** and **Access event log** check boxes are selected.

1 Click the **Output File** button on the Event Log screen.
A file containing the event logs is saved in CSV format to the Downloads folder on the PC. The file contains the system event and access event logs as well as the firmware version, product serial number, and IP address.
The following message is displayed.

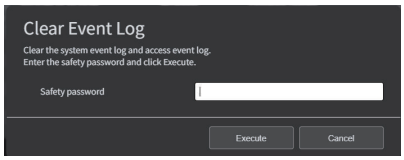


2 Click the **OK** button.

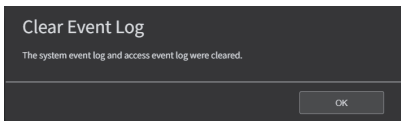
● Clearing Event Logs

With event log clearing, the event logs with the **System event log** and **Access event log** check boxes selected are cleared.

1 Click the **Clear** button on the Event Log tab page.
The following message is displayed.



2 Enter the safety password, and click the **Execute** button.
The event log is cleared, and the following message is displayed.



3 Click the **OK** button.

11-2-4 Event Details and Troubleshooting

This section describes how to check and troubleshoot events.
The current events are retained unless you reset them.
To reset an event, you must eliminate the cause of the current error. The same event will occur again if you reset the event but do not eliminate the cause of the error.

Event List

This section lists the events (errors) that may occur.
Refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for all of the event codes for an NJ/NX-series Controller.
Refer to *NY-series Troubleshooting Manual (Cat. No. W564)* for all of the event codes for an NY-series Controller.

● How to View the Event List

The contents of the event list are described below.

Item	Description
Event code	This is the code of the error (event) that occurred in the Safety I/O Block. It is displayed as eight hexadecimal digits.
Event name	This is the name of the error (event).
Description	This is a description of the error (event).
Cause (assumed cause)	This is the assumed cause of the error (event).

Item	Description
Level	This indicates the level of influence that the error (event) has on control. 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	This is the page that provides details on the error (event).

***1.** This symbol appears only for events for which the user can change the event level.

● Events List

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
05200000 hex	System Error	A hardware error was detected during self-diagnosis of the hardware.	• A memory error occurred due to a transient factor, such as a software error or excessive noise • Hardware failure		○			page 11-23
05210000 hex	Internal Circuit Error at Safety Input	A fault was detected in the internal circuit for the safety input terminal.	• Internal circuit for the safety input terminal is faulty. • Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise		○			page 11-23
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. • Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise		○			page 11-24
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. • Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise		○			page 11-24
155E0000 hex	Non-volatile Memory Access Error	Reading or writing from/to non-volatile memory failed.	• Incorrect setting data • Power interruption during writing of setting data • Non-volatile memory failure		○			page 11-25

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
24D30000 hex	Invalid Rotary Switch Setting for Safety Application	The rotary switch settings for the safety application are invalid.	The rotary switch settings for the safety application are invalid.		○			page 11-26
28150000 hex	Rotary switch settings changed after configuration was locked	The rotary switch settings when the configuration was locked and the current settings do not match.	The rotary switches were changed and the Unit was started up after the configuration was locked.		○			page 11-27
359E0000 hex	Check that the rotary switch settings for the safety application are invalid	The IP address was changed in an IP address non-settable state.	• The rotary switches for the IP address were changed in an IP address non-settable state and then the Unit was started up. • The DHCP server settings were changed and a different IP address was assigned in an IP address non-settable state.		○			page 11-28
38A80000 hex	IP Address Setting Error	An error was detected in the IP address settings.	• Incorrect setting data • Power interruption during writing of TCP/IP settings • The IP address obtained from the DHCP server is invalid. • Non-volatile memory access error		○			page 11-29
38A90000 hex	IP Address Changed after Setting TUNID	A TUNID setting error was detected.	• The rotary switches for the IP address were changed and the Unit was started up after setting the TUNID. • The DHCP server settings were changed and an IP address different from that when set the TUNID was assigned after setting the TUNID.		○			page 11-30
55030000 hex	Data error between dual channel outputs	The wrong safety output data was written.	Different values were written to the safety outputs set for the dual channels.		○			page 11-31
65210000 hex	Output Power Interrupt Circuit Error	An error was detected in the output power interruption test.	A wiring error or hardware failure.		○			page 11-31

Event code	Event name	Description	Assumed cause	Level				Reference
				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. • Failure of connected external device • Error is occurring with the test output terminal used in combination with the corresponding safety input terminal.		○			page 11-32
65230000 hex	Discrepancy Error at Safety Input	An error was detected in discrepancy evaluation of safety input terminals.	• There is a ground fault or break in the input signal line. • The connected device is faulty. • The setting of the discrepancy time is incorrect. • Chattering occurred in the input signal from an external input device, such as a safety door. • Error is occurring with the test output terminal used in combination with the corresponding safety input terminal.		○			page 11-33
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. • Failure of connected external device		○			page 11-33
65250000 hex	Stuck-at-high Detected at Test Output	A test output terminal that is stuck ON was detected.	• The positive power supply wire is in contact with the output signal line. • The internal circuit is faulty. • Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise • Error is occurring with the test output terminal used in combination with the corresponding safety input terminal.		○			page 11-34

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
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 11-34
65280000 hex	Stuck-at-high Detected at Safety Output	A safety output terminal that is stuck ON was detected.	• The positive power supply wire is in contact with the output signal line. • The output power supply is outside the specifications. • The internal circuit is faulty. • Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise		○			page 11-35
65290000 hex	Output Power Supply Error	An incorrect output power supply was detected.	• The output power is not connected. • The output power supply is shut off due to the voltage of the output power supply falling below the detection threshold value. • The output power supply is shut off due to the voltage of the output power supply rising above the detection threshold value. • The output power supply is shut off due to the current of the output power supply rising above the detection threshold value.		○			page 11-36
652B0000 hex	EDM Error	An error was detected in EDM.	• Output signal line is broken. • There is a ground fault on the output signal line. • Is the output signal line in contact with the power supply? • Welding of contactor and relay contacts, which are external wiring devices • Broken wire or ground fault of external wiring device		○			page 11-37
84040000 hex	NTP Server Connection Error	Connection with the NTP server failed.	• Incorrect setting data • Server is down. • An error occurred in the communications path.		○			page 11-38

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
840F0000 hex	DHCP Server Connection Error	Connection with the DHCP server failed.	• Server setting error • Server is down. • An error occurred in the communications path.		○			page 11-39
85E20000 hex	IP Address Duplication Error	The IP address is duplicated.	The IP address is duplicated with the IP address of another node.		○			page 11-40
85E30000 hex	Tag Data Link Timeout	A timeout occurred in a tag data link.	• The power supply of the originator node is OFF. • Communications of the originator node are stopped. • The Ethernet cable for EtherNet/IP is disconnected. • The Ethernet cable for EtherNet/IP is broken. • Link to the EtherNet/IP port is OFF. • Packet loss occurred on the path due to the network communications load. • Noise		○			page 11-41

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
85E40000 hex	CIP Safety Target Connection Timeout	A timeout occurred in the CIP Safety Target connection.	• Cable is broken. • The originator device entered a state where it could not accept a connection. • The timeout value in the communications settings is too short. • 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 in the communications path. • **CIP message server** 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. • Noise • **CIP Safety communications** is set to **Do not use** in the EtherNet/IP port settings.		○			page 11-42
652F0000 hex	Unit/Input Power Supply Voltage Out-of-Specification Detected	The voltage of the Unit/input power supply was detected to be outside the specification range.	The voltage of the Unit/input power supply was detected to be outside the specification range.			○		page 11-43
65300000 hex	Unit/Input Power Supply Current Out-of-Specification Detected	The current of the Unit/input power supply was detected to be outside the specification range.	The current of the Unit/input power supply was detected to be outside the specification range.			○		page 11-43
65310000 hex	Output Power Supply Voltage Out-of-Specification Detected	The voltage of the output power supply was detected to be outside the specification range.	The voltage of the output power supply was detected to be outside the specification range.			○		page 11-44

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
65320000 hex	Output Power Supply Current Out-of-Specification Detected	The current of the output power supply was detected to be outside the specification range.	The current of the output power supply was detected to be outside the specification range.			○		page 11-44
85E10000 hex	Link OFF Detected	An Ethernet link OFF was detected.	• An Ethernet cable is broken, disconnected, or loose. • The power supply of the Ethernet switch is turned OFF. • Baud rate mismatch. • Noise • Execute a restart or execute a memory all clear.			○		page 11-45
85E50000 hex	CIP Safety Target Connection Open Request	There was a request to open a connection from the CIP Safety originator.	There was a request to open a connection from the CIP Safety originator.				○	page 11-45
90110000 hex	Power Turned ON	The power supply was turned ON.	The power supply turned ON.				○	page 11-46
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 11-46
966C0000 hex	Configuration Locked	Configuration lock was executed.	Configuration lock execution				○	page 11-46
966D0000 hex	Configuration Unlocked	Configuration unlock was executed.	Configuration unlock execution				○	page 11-47
96710000 hex	Output Power Supply (PWR OUT) Turned Off	The output power supply that is supplied from the PWR OUT power supply connector was turned OFF.	Shutoff of the through-wiring output power supply was instructed by *through-wiring output power supply shutoff command*.				○	page 11-47
96720000 hex	Setting Data Changed	The setting data was changed.	The setting data was changed.				○	page 11-48
96730000 hex	Login	Logged in. (Web UI)	Logged in using the Web UI.				○	page 11-49
96750000 hex	Safety Application Deleted	Safety application data was deleted from the Unit.	Deletion was accepted from the Web UI.				○	page 11-49

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
96760000 hex	Safety Password Mismatch	Password mismatch was detected when executing a service that requires a safety password.	Password mismatch was detected when executing a service that requires a safety password.				○	page 11-49
96770000 hex	Output Power Supply (PWR OUT) Turned On	The output power supply that is supplied from the PWR OUT power supply connector was turned ON.	Recovery of the through-wiring output power supply was instructed by *through-wiring output power supply recovery command*.				○	page 11-50
96780000 hex	Firmware Update Executed	A firmware update was executed.	A firmware update was executed.				○	page 11-50
96790000 hex	Memory All Clear	Memory all clear was executed.	Memory all clear was executed.				○	page 11-51
967A0000 hex	Link Detected	Establishing of an Ethernet link was detected.	Establishing of an Ethernet link was detected.				○	page 11-51
967B0000 hex	Operating Mode Changed	Change operating mode was executed.	Change operating mode executed.				○	page 11-52
967C0000 hex	Safety Password Changed	The safety password was changed.	The safety password was changed.				○	page 11-52
967D0000 hex	Safety Application Transferred	The safety application data was transferred to the Unit.	• Transfer by the Web UI was accepted. • A Type 1 Safety Open request was accepted from the safety controller.				○	page 11-53
967E0000 hex	Event Log Cleared	The event log was cleared.	The event log was cleared.				○	page 11-53
967F0000 hex	Backup Executed	A backup was executed.	A backup was executed.				○	page 11-54
96800000 hex	Restore Executed	A restore was executed.	A restore was executed.				○	page 11-54
96810000 hex	OMRON Maintenance Executed	Maintenance by OMRON maintenance personnel was executed.	Maintenance by OMRON maintenance personnel was executed.				○	page 11-54
96820000 hex	Restarted	A restart was executed.	A restart was executed.				○	page 11-55
96830000 hex	Safety Configuration Validated	The safety configuration was validated.	The safety configuration was validated.				○	page 11-55

Event code	Event name	Description	Assumed cause	Level				Reference
				Prt	Min	Obs	Info	
96840000 hex	IP Address Indication Function Executed	The IP address indication function was executed.	Started up with SW1 = SW2 = 8 (IP address indication function).				○	page 11-56
96850000 hex	I/O Wiring Checking Function Executed	The I/O wiring checking function was executed.	Started up with SW1 = SW2 = E (I/O wiring checking function).				○	page 11-56

Details on Events

This section describes the details on each event.

● How to View Event Details

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>Description</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 rowspan="2">Error attributes</td><td>Level</td><td>Tells the level of influence on control. *1</td><td>Recovery method</td><td>Gives the recovery method. *2</td><td>Log category</td><td>Tells which log the error is saved in. *3</td></tr>
<tr><td>Effects</td><td>User program</td><td>Tells what will happen to execution of the user program. *4</td><td>Operation</td><td colspan="3">Provides special information on the operation that results from the error.</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 Sysmac Studio/HMI. *5</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 are 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.** Method to reset the error status of the Controller after corrections, and is one of the following:
- Automatic recovery: Normal status is restored automatically when the cause of the error is removed.
- Error reset: Normal status is restored when the error is reset after the cause of the error is removed.
- Cycle the power supply: Normal status is restored when the power supply to the Controller is turned OFF and then back ON after the cause of the error is removed.
- Controller reset: Normal status is restored when the Controller is reset after the cause of the error is removed.
- Depends on cause: The recovery method depends on the cause of the error.

***3.** One of the following:
- System: System event log
- Access: Access event log

***4.** 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.

***5.** Refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* or *NY-series Troubleshooting Manual (Cat. No. W564)* for the applicable range of the HMI Troubleshooter.

● Explanation of Events

Event name	System Error			**Event code**	05200000 hex	
Description	A hardware error was detected during self-diagnosis of the hardware.					
Source	-		**Source details**	-	**Detection timing**	Continuously
Error attributes	**Level**	Minor fault	**Recovery method**	Cycle the power supply	**Log category**	System
Effects	**User program**	Continues	**Operation**	The corresponding Unit stops operating and the I/O data changes to the safe state.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	• A memory error occurred due to a transient factor, such as a software error or excessive noise • Hardware failure		Cycle the power supply. Replace the Unit if the error occurs again.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
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	Internal Circuit Error at Safety Input			**Event code**	05210000 hex	
Description	A fault was detected in the internal circuit for the safety input terminal.					
Source	-		**Source details**	-	**Detection timing**	• During idle • When executing
Error attributes	**Level**	Minor fault	**Recovery method**	• Cycle the power supply • Execute a restart	**Log category**	System
Effects	**User program**	Continues	**Operation**	The corresponding safety input terminal is maintained in the safe state until the power supply is cycled.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Internal circuit for the safety input terminal is faulty. Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise		Cycle the power supply. Replace the Unit if the error occurs again.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

Event name	Internal Circuit Error at Test Output			**Event code**	05220000 hex	
Description	A fault was detected in the internal circuit for the test output terminal.					
Source	-		**Source details**	-	**Detection timing**	• During idle • When executing
Error attributes	**Level**	Minor fault	**Recovery method**	• Cycle the power supply • Execute a restart	**Log category**	System
Effects	**User program**	Continues	**Operation**	The corresponding test output terminal is maintained in the safe state until the power supply is cycled. Also, an *External Test Signal Failure at Safety Input* event (65220000 hex) occurs for the safety input terminal that uses the corresponding test output terminal as the test source.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The internal circuit for the test output terminal is faulty.		Cycle the power supply. Replace the Unit if the error occurs again.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
	Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise					
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

Event name	Internal Circuit Error at Safety Output			**Event code**	05230000 hex	
Description	A fault was detected in the internal circuit for the safety output terminal.					
Source	-		**Source details**	-	**Detection timing**	• During idle • When executing
Error attributes	**Level**	Minor fault	**Recovery method**	• Cycle the power supply • Execute a restart	**Log category**	System
Effects	**User program**	Continues	**Operation**	The corresponding safety output terminal is maintained in the safe state until the power supply is cycled.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The internal circuit for the safety output terminal is faulty.		Cycle the power supply. Replace the Unit if the error occurs again.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
	Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise					
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Non-volatile Memory Access Error</td><td>Event code</td><td colspan="2">155E0000 hex</td></tr>
<tr><td>Description</td><td colspan="6">Reading or writing from/to non-volatile memory failed.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>• Cycle the power supply
• Execute a restart
• Automatic recovery (after downloading the settings)</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 corresponding Unit stops operating and the I/O data changes to the safe state.</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">Incorrect setting data</td><td colspan="2" rowspan="3">Identify the cause of the error from the attached information.
• When attached information 1 = 01 hex
Cycle the power supply.
• When attached information 1 = 02 hex
Perform the following according to the value of attached information 2.
02xx to 05xx hex: Configure each setting again.
20xx hex:
- For a -CST model, execute a memory all clear and then configure the settings again.
- For an -EIT model, align the rotary switches to SW1 = SW2 = 0, then execute a memory all clear and configure the safety application settings again.
21xx hex: Configure the safety application again.
FExx hex: Update the firmware.

If operation is not recovered by the above, replace the Unit.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">Power interruption during writing of setting data</td><td colspan="2">Do not turn OFF the power supply of the corresponding Unit during writing of setting data.</td></tr>
<tr><td colspan="2">Non-volatile memory failure</td><td colspan="2">None</td></tr>
</table>

Attached information	Attached information 1: Cause 01 hex: Failure accessing non-volatile memory 02 hex: Data corrupt Attached information 2: Detection target 02xx hex: Link settings 03xx hex: Ethernet port enable/disable settings 04xx hex: SNTP settings 05xx hex: Power shut-off function for through-wiring output enable/disable settings 20xx hex: Other safety related data 21xx hex: Safety application data 80xx hex: QoS settings 81xx hex: LLDP function settings FExx hex: Firmware data Other than above: Other system data
Precautions/ Remarks	None

Event name	Invalid Rotary Switch Setting for Safety Application			**Event code**	24D30000 hex	
Description	The rotary switch settings for the safety application are invalid.					
Source	-		**Source details**	-	**Detection timing**	• When power is turned ON. • When execute a restart
Error attributes	**Level**	Minor fault	**Recovery method**	• Cycle the power supply • Execute a restart	**Log category**	System
Effects	**User program**	Continues	**Operation**	The corresponding Unit stops operating and the I/O data changes to the safe state.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The rotary switch settings for the safety application are invalid.		Check that the rotary switch settings for the safety application are invalid.		None	
Attached information	Attached information 1: Setting values of rotary switches for current safety application The display format is [SW1, SW2]. Example: When SW1 = 1 and SW2 = E → 1E					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Rotary switch settings changed after configuration was locked</td><td>Event code</td><td colspan="2">28150000 hex</td></tr>
<tr><td>Description</td><td colspan="6">The rotary switch settings when the configuration was locked and the current settings do not match.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>• When power is turned ON.
• When execute a restart</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>• Cycle the power supply
• Execute a restart</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 corresponding Unit stops operating and the I/O data changes to the safe state.</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 rotary switches were changed and the Unit was started up after the configuration was locked.</td><td colspan="2">• Return the setting values of the rotary switches to the setting values when the configuration was locked.
• Execute a memory all clear after the configuration has been unlocked, and then configure the settings again.
Cycle the power supply or execute a restart also after any of the corrections is performed.</td><td colspan="2">Do not change the setting values of the rotary switches after the configuration has been locked.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Current setting values of rotary switches
The display format is [SW1, SW2, $x16^{1}$, $x16^{0}$].
Example: When SW1=F, SW2=F, $x16^{1}$=0, $x16^{0}$=1
→ FF01 hex
Attached information 2: Setting values of rotary switches when configuration was locked
The display format is [SW1, SW2, $x16^{1}$, $x16^{0}$].
Example: When SW1=3, SW2=3, $x16^{1}$=0, $x16^{0}$=1
→ 3301 hex</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="2">Check that the rotary switch settings for the safety application are invalid</td><td>Event code</td><td colspan="2">359E0000 hex</td></tr>
<tr><td>Description</td><td colspan="5">The IP address was changed in an IP address non-settable state.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>• When power is turned ON.
• When execute a restart</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>• Cycle the power supply
• Execute a restart</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 corresponding Unit stops operating and the I/O data changes to the safe state.</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 rotary switches for the IP address were changed in an IP address non-settable state and then the Unit was started up.
• The DHCP server settings were changed and a different IP address was assigned in an IP address non-settable state.</td><td colspan="2">• Return the rotary switches for the IP address to the original values.
• Return the DHCP server settings to the original values.
• Execute a memory all clear and then set the IP address again.
If operation is not recovered by the above, replace the Unit.</td><td colspan="2">Do not operate the rotary switches for the IP address and change the DHCP server settings in the IP address non-settable state.</td></tr>
<tr><td>Attached information</td><td colspan="5">Attached information 1: Current IP address
Example: C0A8FA64 hex when the IP address is 192.168.250.100.
Attached information 2: IP address set in settable state
Example: C0A8FA64 hex when the IP address is 192.168.250.100.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="5">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="3">IP Address Setting Error</td><td>Event code</td><td colspan="2">38A80000 hex</td></tr>
<tr><td>Description</td><td colspan="6">An error was detected in the IP address settings.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>• When power is turned ON.
• When execute a restart</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>• Cycle the power supply
• Execute a restart</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">EtherNet/IP communications will not operate.
CIP Safety communications will not operate.</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">Incorrect setting data</td><td colspan="2" rowspan="3">The IP address will be the default value of 192.168.250.1. Perform one of the following corrections.
• Identify the cause of the error from the attached information and then set the correct values again.
• Execute a memory all clear or write the settings again.
• Correct the setting for the IP address provided by the DHCP server so that it is within the range specified for the corresponding Unit.
Cycle the power supply or execute a restart also after any of the corrections is performed.
If operation is not recovered by the above, replace the Unit.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">Power interruption during writing of TCP/IP settings</td><td colspan="2">Do not turn OFF the power supply of the corresponding Unit during writing of TCP/IP settings.</td></tr>
<tr><td colspan="2">The IP address obtained from the DHCP server is invalid.</td><td colspan="2">Correct the setting for the IP address provided by the DHCP server so that it is within the range specified for the corresponding Unit.</td></tr>
<tr><td colspan="2">Non-volatile memory access error</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 (when attached information 1 is 02 hex)
11 hex: IP address invalid
12 hex: Subnet mask invalid
13 hex: Default gateway invalid</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="3">IP Address Changed after Setting TUNID</td><td>Event code</td><td colspan="2">38A90000 hex</td></tr>
<tr><td>Description</td><td colspan="6">A TUNID setting error was detected.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>• When power is turned ON.
• When execute a restart</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>• Cycle the power supply
• Execute a restart</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 corresponding Unit stops operating and the I/O data changes to the safe state.</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 rotary switches for the IP address were changed and the Unit was started up after setting the TUNID.</td><td colspan="2">Return the rotary switches for the IP address to the values when the TUNID was set.</td><td colspan="2" rowspan="3">Do not operate the rotary switches for the IP address and change the DHCP server settings after setting the TUNID.</td></tr>
<tr><td colspan="2">The DHCP server settings were changed and an IP address different from that when set the TUNID was assigned after setting the TUNID.</td><td colspan="2">Return the DHCP server settings to the values when the TUNID was set.</td></tr>
<tr><td colspan="2"></td><td colspan="2">Alternatively, execute a memory all clear and then set the TUNID again.
If operation is not recovered by the above, replace the Unit.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Current IP address
Example: C0A8FA01 hex when the IP address is 192.168.250.1.
Attached information 2: IP address when TUNID was set (IP address part of TUNID)
Example: C0A8FA64 hex when the IP address is 192.168.250.100.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Data error between dual channel outputs			Event code	55030000 hex	
Description	The wrong safety output data was written.					
Source	—		Source details	-	Detection timing	• During idle • When executing
Error attributes	Level	Minor fault	Recovery method	Recover by inactivating the safety output terminal	Log category	System
Effects	User program	Continues	Operation	>The corresponding safety output terminal is maintained in the safe state until the error is cleared.		
Cause and correction	Assumed cause		Correction		Prevention	
	Different values were written to the safety outputs set for the dual channels.		Check the safety program, and write the same value to the safety outputs set for the dual channels.		Design the safety program considering the corrections that are given on the left.	
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

Event name	Output Power Interrupt Circuit Error			Event code	65210000 hex	
Description	An error was detected in the output power interruption test.					
Source	-		Source details	-	Detection timing	• When power is turned ON. • When execute a restart
Error attributes	Level	Minor fault	Recovery method	• Cycle the power supply • Execute a restart	Log category	System
Effects	User program	Continues	Operation	The corresponding Unit continues to operate, but the safe state is maintained for the I/O data.		
Cause and correction	Assumed cause		Correction		Prevention	
	A wiring error or hardware failure.		Check the following and then supply the rated power. • Is the power supply voltage within the specifications? • Is there no wiring error or break? • Is 24 VDC 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 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>Description</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">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>• During idle
• When executing</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>Recover by inactivating the safety input terminal</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 corresponding safety input terminal is maintained in the safe state until the error is cleared.</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">Failure of connected external device</td><td colspan="2">Replace the connected external device.</td></tr>
<tr><td colspan="2">Error is occurring with the test output terminal used in combination with the corresponding safety input terminal.</td><td colspan="2">Check the error occurring with the test output terminal and try the solutions specified in Correction.</td><td colspan="2">Try the solutions specified in Prevention for the error occurring with 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	
Description	An error was detected in discrepancy evaluation of safety input terminals.					
Source	-		Source details	-	Detection timing	• During idle • When executing
Error attributes	Level	Minor fault	Recovery method	Recover by inactivating the safety input terminal	Log category	System
Effects	User program	Continues	Operation	The corresponding safety input terminal is maintained in the safe state until the error is cleared.		
Cause and correction	Assumed cause		Correction		Prevention	
	There is a ground fault or break 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 connected external device.			
	The setting of the discrepancy time is incorrect.		Correct the discrepancy evaluation 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 an external input device, such as a safety door.					
	Error is occurring with the test output terminal used in combination with the corresponding safety input terminal.		Check the error occurring with the test output terminal and try the solutions specified in Correction.		Try the solutions specified in Prevention for the error occurring with the test output terminal.	
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

Event name	Overload Detected at Test Output			Event code	65240000 hex	
Description	An overcurrent was detected at the test output terminal.					
Source	-		Source details	-	Detection timing	• During idle • When executing
Error attributes	Level	Minor fault	Recovery method	Automatic recovery	Log category	System
Effects	User program	Continues	Operation	The safety input terminal that uses the corresponding test output terminal as the test source is maintained in the safe state until the error is cleared.		
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.	
	Failure of connected external device		Replace the connected external device.			
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	None					

Event name	Stuck-at-high Detected at Test Output		Event code	65250000 hex	
Description	A test output terminal that is stuck ON was detected.				
Source	-	Source details	-	Detection timing	• During idle • When executing
Error attributes	Level: Minor fault	Recovery method	Automatic recovery	Log category	System
Effects	User program: Continues	Operation	The safety input terminal that uses the corresponding test output terminal as the test source is maintained in the safe state until the error is cleared.		
Cause and correction	**Assumed cause**	**Correction**		**Prevention**	
	The positive power supply wire 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. Replace the Unit if the error occurs again.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
	Memory abnormality or signal abnormality due to a transient factor, 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	
Description	A ground fault was detected on the safety output terminal.				
Source	-	Source details	-	Detection timing	• During idle • When executing
Error attributes	Level: Minor fault	Recovery method	Recover by inactivating the safety output terminal	Log category	System
Effects	User program: Continues	Operation	The corresponding safety output terminal is maintained in the safe state until the error is cleared.		
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	If an abnormality occurs in the output power supply, this error may be registered even when there is no ground fault at the safety output terminal.				

Event name	Stuck-at-high Detected at Safety Output			Event code	65280000 hex	
Description	A safety output terminal that is stuck ON was detected.					
Source	-		Source details	-	Detection timing	• During idle • When executing
Error attributes	Level	Minor fault	Recovery method	Recover by inactivating the safety output terminal	Log category	System
Effects	User program	Continues	Operation	The corresponding safety output terminal is maintained in the safe state until the error is cleared.		
Cause and correction	Assumed cause		Correction		Prevention	
	The positive power supply wire 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. Replace the Unit if the error occurs again.		If cycling the power supply restores normal operation, there may be excessive noise near the Unit. Implement noise countermeasures.	
	Memory abnormality or signal abnormality due to a transient factor, such as a software error or excessive noise					
Attached information	Attached information 1: Terminal number					
Precautions/ Remarks	If an abnormality occurs in the output power supply, this error may be registered even when the safety output terminals are not stuck ON.					

<table>
<tr><td>Event name</td><td colspan="2">Output Power Supply Error</td><td>Event code</td><td colspan="2">65290000 hex</td></tr>
<tr><td>Description</td><td colspan="5">An incorrect output power supply was detected.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</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="2">The corresponding Unit continues to operate, but the safe state is maintained for the output data.</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">• The output power is not connected.
• The output power supply is shut off due to the voltage of the output power supply falling below the detection threshold value.
• The output power supply is shut off due to the voltage of the output power supply rising above the detection threshold value.
• The output power supply is shut off due to the current of the output power supply rising above the detection threshold value.</td><td colspan="2">Check the following and then supply the rated power.
• Is the power supply voltage within the specifications?
• Is there no wiring error or break?
• Is there no overcurrent occurring due to shorting of the power supply wires?
If the voltage that is measured is correct, the Unit may be faulty. In that case, replace the Unit.</td><td>Design the system considering the corrections that are given on the left.</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>

Event name	EDM Error			Event code	652B0000 hex	
Description	An error was detected in EDM.					
Source	-		Source details	-	Detection timing	When executing
Error attributes	Level	Minor fault	Recovery method	Recover by inactivating the relationship of the output and feedback input of the FB.	Log category	System
Effects	User program	Continues	Operation	The corresponding safety output terminal is maintained in the safe state until the error is cleared.		
Cause and correction	Assumed cause		Correction		Prevention	
	Check for the following items. • Output signal line is broken. • There is a ground fault on the output signal line. • Is the output signal line in contact with the power supply? • Welding of contactor and relay contacts, which are external wiring devices • Broken wire or ground fault of external wiring device		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: Output terminal number of EDM for which error occurred 0: So00 to 3: So03					
Precautions/ Remarks	None					

Event name	NTP Server Connection Error			**Event code**	84040000 hex	
Description	Connection with the NTP server failed.					
Source	-		**Source details**	-	**Detection timing**	During NTP operation
Error attributes	**Level**	Minor fault	**Recovery method**	Automatic recovery When the server specification is corrected and downloading is performed again, cycle the power supply or execute a restart.	**Log category**	System
Effects	**User program**	Continues	**Operation**	Time cannot be acquired via NTP.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Incorrect setting data		If there is a mistake with the specification for the connection destination server, correct the server specification and then download the setting data again.		Check if the connection destination server setting is correct.	
	Server is down.		Check if the connection destination server is operating normally and set it to operate normally if it is not.		Check if the connection destination server 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	If **TCP Server Run** is recorded in the event log after the correction is made, then the CPU Unit is correctly connected to the DNS server.					

Event name	DHCP Server Connection Error			**Event code**	840F0000 hex	
Description	Connection with the DHCP server failed.					
Source	-		**Source details**	-	**Detection timing**	During DHCP operation
Error attributes	**Level**	Minor fault	**Recovery method**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues	**Operation**	EtherNet/IP communications will not operate. Requests to the DHCP server will continue until there is a response from the DHCP server.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Server setting error		Server is down.		Check if the connection destination server setting is correct.	
	Server is down.		Check if the connection destination server is operating normally and set it to operate normally if it is not.		Check if the connection destination server 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">IP Address Duplication Error</td><td>Event code</td><td colspan="2">85E20000 hex</td></tr>
<tr><td>Description</td><td colspan="6">The IP address is duplicated.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>When IP address determined</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</td><td>• Cycle the power supply
• Execute a restart</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">EtherNet/IP communications will not operate
CIP Safety communications will not operate</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 IP address is duplicated with the IP address of another node.</td><td colspan="2">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.
Cycle the power supply or execute a restart also after any of the corrections is performed.</td><td colspan="2">Assign an IP address to each node within the network so that they do not duplicate each other.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Duplicated IP address
Example: C0A8FA01 hex when the IP address is 192.168.250.1.</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">A duplicated address error occurs if an ARP is sent using the set IP address and there is an ARP response.</td></tr>
</table>

<table>
<tr><td>Event name</td><td colspan="3">Tag Data Link Timeout</td><td>Event code</td><td colspan="2">85E30000 hex</td></tr>
<tr><td>Description</td><td colspan="6">A timeout occurred in a tag data link.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>Continuously</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Minor fault</td><td>Recovery method</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 corresponding Unit continues to operate.</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="2">The power supply of the originator node is OFF.</td><td colspan="2" rowspan="2">Check the status of the originator node and start it normally.</td><td colspan="2" rowspan="2">Use the tag data link after confirming that the originator node is running normally.</td></tr>
<tr><td colspan="2">Communications of the originator node are stopped.</td></tr>
<tr><td colspan="2">The Ethernet cable for EtherNet/IP is disconnected.</td><td colspan="2">Reconnect the connector and make sure it is mated correctly.</td><td colspan="2">Connect the connector securely.</td></tr>
<tr><td colspan="2">The Ethernet cable for EtherNet/IP is broken.</td><td colspan="2">Replace the Ethernet cable.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">Link to the EtherNet/IP port is OFF.</td><td colspan="2">Refer to the Link OFF Detected error (85E10000 hex) for the assumed causes and other information on link OFF. Allow CIP communications in the originator node and the Firewall and Packet Filter functions of the devices in the communications path.</td><td colspan="2">Refer to the Link OFF Detected error (85E10000 hex) for the assumed causes and other information on link OFF. Allow CIP communications in the originator node and the Firewall and Packet Filter functions of the devices in the communications path.</td></tr>
<tr><td colspan="2">Packet loss occurred on the path due to the network communications load.</td><td colspan="2">Increase the connection timeout value or RPI. Or, review the network environment and network devices.</td><td colspan="2">Design the network so that it will not become overloaded.</td></tr>
<tr><td colspan="2">Noise</td><td colspan="2">Implement noise countermeasures if there is excessive noise.</td><td colspan="2">Implement noise countermeasures if there is excessive noise.</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Originator IP address
Example: C0A8FA01 hex when the IP address is 192.168.250.1.
Attached information 2: Assembly Instance No
025C hex: Input Assembly 1
03C0 hex: Input Assembly 2
03C1 hex: Input Assembly 3</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">If multiple connection errors are occurring on the same node, only one occurring error is recorded in the event log.</td></tr>
</table>

Event name	CIP Safety Target Connection Timeout			**Event code**	85E40000 hex	
Description	A timeout occurred in the CIP Safety Target connection.					
Source	-		**Source details**	-	**Detection timing**	When executing
Error attributes	**Level**	Minor fault	**Recovery method**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues	**Operation**	The corresponding Unit continues to operate, but the safe state is maintained for the I/O data of the safety connection where the error was detected.		

	Assumed cause	**Correction**	**Prevention**
Cause and correction	Cable is broken.	Check the cable to see if it is broken.	Build the system considering the corrections that are given on the left.
	The originator device entered a state where it could not accept a connection.	Check if the originator device is in a state where it can accept a connection.	
	The timeout value in the communications settings is too short.	Check if the timeout value in the communications settings is appropriate.	
	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 in the communications path.	Check if CIP Safety packets from the originator node are allowed by the Packet Filter (Simple) or Packet Filter functions in the EtherNet/IP port settings or on the devices in the communications path.	
	CIP message server for the originator node is set to **Do not use**.	Check if **CIP message server** for the originator node is set to **Use**.	
	When the Packet Filter function of the originator node is enabled, CIP Safety packets from the target node are not allowed.	Check if CIP Safety packets from the target node are allowed in the Packet Filter settings of the originator node.	
	Noise	Check if communications are affected by noise.	
	CIP Safety communications is set to **Do not use** in the EtherNet/IP port settings.	Check if **CIP Safety communications** is set to **Use** in the EtherNet/IP port settings.	

Attached information	Attached information 1: Assembly Instance No
Precautions/ Remarks	None

Event name	Unit/Input Power Supply Voltage Out-of-Specification Detected			Event code	652F0000 hex	
Description	The voltage of the Unit/input power supply was detected to be outside the specification range.					
Source	-		Source details	-	Detection timing	Continuously
Error attributes	Level	Observation	Recovery method	Automatic recovery	Log category	System
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	The voltage of the Unit/input power supply was detected to be outside the specification range.		Adjust the voltage of the Unit/input power supply to a normal value within the specification range.		None	
Attached information	Attached information 1 Voltage monitor values of Unit/input power supply 100 mV increments					
Precautions/ Remarks	None					

Event name	Unit/Input Power Supply Current Out-of-Specification Detected			Event code	65300000 hex	
Description	The current of the Unit/input power supply was detected to be outside the specification range.					
Source	-		Source details	-	Detection timing	Continuously
Error attributes	Level	Observation	Recovery method	Automatic recovery	Log category	System
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	The current of the Unit/input power supply was detected to be outside the specification range.		Adjust the current of the Unit/input power supply to a normal value within the specification range.		None	
Attached information	Attached information 1 Current monitor values of Unit/input power supply 100 mA increments					
Precautions/ Remarks	None					

Event name	Output Power Supply Voltage Out-of-Specification Detected			Event code	65310000 hex	
Description	The voltage of the output power supply was detected to be outside the specification range.					
Source	-		Source details	-	Detection timing	Continuously
Error attributes	Level	Observation	Recovery method	Automatic recovery	Log category	System
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	The voltage of the output power supply was detected to be outside the specification range.		Adjust the voltage of the output power supply to a normal value within the specification range.		None	
Attached information	Attached information 1: Voltage monitor values of output power supply 100 mV increments					
Precautions/ Remarks	None					

Event name	Output Power Supply Current Out-of-Specification Detected			Event code	65320000 hex	
Description	The current of the output power supply was detected to be outside the specification range.					
Source	-		Source details	-	Detection timing	Continuously
Error attributes	Level	Observation	Recovery method	Automatic recovery	Log category	System
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	The current of the output power supply was detected to be outside the specification range.		Adjust the current of the output power supply to a normal value within the specification range.		None	
Attached information	Attached information 1: Current monitor values of output power supply 100 mA increments					
Precautions/ Remarks	None					

Event name	Link OFF Detected			Event code	85E10000 hex	
Description	An Ethernet link OFF was detected.					
Source	-		Source details	-	Detection timing	Continuously
Error attributes	Level	Observation	Recovery method	Automatic recovery	Log category	System
Effects	User program	Continues	Operation	EtherNet/IP communications will not operate.		
Cause and correction	Assumed cause		Correction		Prevention	
	An Ethernet cable is broken, disconnected, or loose.		Connect the Ethernet cable securely. If the cable is broken, replace it.		Connect the Ethernet cable securely. Check the cable to make sure that it is not broken.	
	The power supply of the Ethernet switch is turned OFF.		Turn ON the power supply to the Ethernet switch. Replace the Ethernet switch if it fails.		Do not turn OFF the power supply to the Ethernet switch.	
	Baud rate mismatch.		Correct the settings so that the same baud rate is used as for the remote communications nodes.		Set the same baud rate as for the remote communications nodes.	
	Noise		Implement noise countermeasures if there is excessive noise.		Implement noise countermeasures.	
	Execute a restart or execute a memory all clear.		None. This event occurs when the operation on the left are performed.		None. This event occurs when the operation on the left are performed.	
Attached information	Attached information 1: EtherNet/IP communications connector for which link OFF detected 1: EtherNet/IP communications connector 1 (ETH1) 2: EtherNet/IP communications connector 2 (ETH2)					
Precautions/ Remarks	None					

Event name	CIP Safety Target Connection Open Request			Event code	85E50000 hex	
Description	There was a request to open a connection from the CIP Safety originator.					
Source	-		Source details	-	Detection timing	• During idle • When executing
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	There was a request to open a connection from the CIP Safety originator.		—		—	
Attached information	Attached information 1: Reserved Attached information 2: Assembly Instance No Attached information 3: General Status defined in CIP specifications Attached information 4: Extended Status defined in CIP specifications					
Precautions/ Remarks	None					

Event name	Power Turned ON			Event code	90110000 hex	
Description	The power supply was turned ON.					
Source	-		Source details	-	Detection timing	When power is turned ON.
Error attributes	Level	Information	Recovery method	-	Log category	System
Effects	User program	Continues	Operation	Operation starts.		
Cause and correction	Assumed cause		Correction		Prevention	
	The power supply turned ON.		None		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	IP Address Fixed			Event code	94080000 hex	
Description	The correct IP address has been determined and Ethernet communications can start.					
Source	-		Source details	-	Detection timing	• When power is turned ON. • When execute a restart
Error attributes	Level	Information	Recovery method	-	Log category	System
Effects	User program	Continues	Operation	Not affected.		
Cause and correction	Assumed cause		Correction		Prevention	
	The correct IP address has been determined and Ethernet communications can start.		None		None	
Attached information	Attached information 1: IP address Example: C0A8FA01 hex when the IP address is 192.168.250.1.					
Precautions/ Remarks	None					

Event name	Configuration Locked			Event code	966C0000 hex	
Description	Configuration lock was executed.					
Source	-		Source details	-	Detection timing	When configuration lock executed
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	Configuration lock execution		None		None	
Attached information	Attached information 1: Reserved Attached information 2: SCCRC Attached information 3: Setting values of rotary switches when configuration was locked The display format is [SW1, SW2, $x16^{1}$,$x16^{0}$]. Example: When SW1=3, SW2=3, $x16^{1}$=0, $x16^{0}$=1					
Precautions/ Remarks	None					

Event name	Configuration Unlocked			Event code	966D0000 hex	
Description	Configuration unlock was executed.					
Source	-		Source details	-	Detection timing	When configuration unlock executed
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	Configuration unlock execution		None		None	
Attached information	Attached information 1: Reserved					
Precautions/ Remarks	None					

Event name	Output Power Supply (PWR OUT) Turned Off			Event code	96710000 hex	
Description	The output power supply that is supplied from the PWR OUT power supply connector was turned OFF.					
Source	-		Source details	-	Detection timing	When turn output power supply (PWR OUT) OFF
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	The output power supply that is supplied from the PWR OUT power supply connector will turn OFF.		
Cause and correction	Assumed cause		Correction		Prevention	
	Shutoff of the through-wiring output power supply was instructed by *through-wiring output power supply shutoff command*.		None		None	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td>Event name</td><td colspan="3">Setting Data Changed</td><td>Event code</td><td colspan="2">96720000 hex</td></tr>
<tr><td>Description</td><td colspan="6">The setting data was changed.</td></tr>
<tr><td>Source</td><td colspan="2">-</td><td>Source details</td><td>-</td><td>Detection timing</td><td>When settings are changed.</td></tr>
<tr><td>Error attributes</td><td>Level</td><td>Information</td><td>Recovery method</td><td>-</td><td>Log category</td><td>Access</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">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 setting data was changed.</td><td colspan="2">None</td><td colspan="2">None</td></tr>
<tr><td>Attached information</td><td colspan="6">Attached information 1: Reserved
Attached information 2: Change target
0100 hex: TCP/IP settings (IP determination method)
0101 hex: TCP/IP settings (IP address)
0102 hex: TCP/IP settings (Encapsulation Inactivity Timeout)
0200 hex: LINK settings
0300 hex: Communications port enable/disable function setting
0400 hex: Automatic clock adjustment setting (NTP/SNTP Server IP Address)
0401 hex: Automatic clock adjustment setting (time zone)
0500 hex: Power shut-off function setting for through-wiring output
2000 hex: Safety password
2006 hex: Configuration lock state
2008 hex: Restore active flag
2001 hex: TUNID
2002 hex: Alarm Enable
2003 hex: Warning Enable
2004 hex: Output Connection Owner
2005 hex: CFUNID
21*1 hex: Configuration data
21*2 hex: SCID
21*5 hex: Application name
21*6 hex: Version
21*7 hex: Creator
(* is a value from 0 to F indicating the application number)
8000 hex: QoS setting (DSCP Urgent)
8001 hex: QoS setting (DSCP Scheduled)
8002 hex: QoS setting (DSCP High)
8003 hex: QoS setting (DSCP Low)
8004 hex: QoS setting (DSCP Explicit)
8100 hex: LLDP setting (LLDP Enable)
8101 hex: LLDP setting (LLDP Tx Interval)
8102 hex: LLDP setting (LLDP Tx Hold)</td></tr>
<tr><td>Precautions/ Remarks</td><td colspan="6">None</td></tr>
</table>

Event name	Login		Event code	96730000 hex		
Description	Logged in. (Web UI)					
Source	-		Source details	-	Detection timing	When operated by user (Web UI)
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected.		
Cause and correction	Assumed cause		Correction		Prevention	
	Logged in using the Web UI.		None		None	
Attached information	Attached information 1: Connection source IP address Example: C0A8FA64 hex when the IP address is 192.168.250.100. Attached information 2: Login right type 0: Login with administrator right 1: Login with observer right					
Precautions/ Remarks	None					

Event name	Safety Application Deleted		Event code	96750000 hex		
Description	Safety application data was deleted from the Unit.					
Source	-		Source details	-	Detection timing	When command (deletion) from user
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	Deletion was accepted from the Web UI.		None		None	
Attached information	Attached information 1: Reserved Attached information 2: Application number					
Precautions/ Remarks	None					

Event name	Safety Password Mismatch		Event code	96760000 hex		
Description	Password mismatch was detected when executing a service that requires a safety password.					
Source	-		Source details	-	Detection timing	When executing a service that requires a password
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	The corresponding Unit continues to operate.		
Cause and correction	Assumed cause		Correction		Prevention	
	Password mismatch was detected when executing a service that requires a safety password.		Enter the correct safety password and execute the service again.		None	
Attached information	Attached information 1: Reserved					
Precautions/ Remarks	None					

Event name	Output Power Supply (PWR OUT) Turned On			Event code	96770000 hex	
Description	The output power supply that is supplied from the PWR OUT power supply connector was turned ON.					
Source	-		Source details	-	Detection timing	When turn output power supply (PWR OUT) ON
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	The output power supply that is supplied from the PWR OUT power supply connector will turn ON.		
Cause and correction	Assumed cause		Correction		Prevention	
	Recovery of the through-wiring output power supply was instructed by *through-wiring output power supply recovery command*.		None		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	Firmware Update Executed			Event code	96780000 hex	
Description	A firmware update was executed.					
Source	-		Source details	-	Detection timing	When firmware updated
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected.		
Cause and correction	Assumed cause		Correction		Prevention	
	A firmware update was executed.		None		None	
Attached information	Attached information 1: Connection source IP address Example: C0A8FA64 hex when the IP address is 192.168.250.100. Attached information 2: Execution result 0000 hex: Successful 0001 hex: Failed Attached information 3: Version of written firmware (BCD) Example: For Ver. 1.10.01, it will be 01100100 hex.					
Precautions/ Remarks	None					

Event name	Memory All Clear			**Event code**	96790000 hex	
Description	Memory all clear was executed.					
Source	-		**Source details**	-	**Detection timing**	When memory all clear is executed
Error attributes	**Level**	Information	**Recovery method**	-	**Log category**	Access
Effects	**User program**	Continues	**Operation**	Operation is started after a reset is executed.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Memory all clear was executed.		None		None	
Attached information	Attached information 1: Reserved Attached information 2: Reset type 1: Memory all clear (all data of attached information 3 is cleared) 2: Memory all clear (some data of attached information 3 is cleared) Attached information 3: Uninitialized data (data for which the value of the corresponding bit is 1 is not initialized)*1 Bit 0: IP Address Bit 2: TUNID Bit 3: Password Bit 4: CFUNID Bit 5: Output Connection Owner					
Precautions/ Remarks	None					

***1.** This is valid only when attached information 2 is **2**.

Event name	Link Detected			**Event code**	967A0000 hex	
Description	Establishing of an Ethernet link was detected.					
Source	-		**Source details**	-	**Detection timing**	When a link is established.
Error attributes	**Level**	Information	**Recovery method**	-	**Log category**	System
Effects	**User program**	Continues	**Operation**	Not affected.		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Establishing of an Ethernet link was detected.		None		None	
Attached information	Attached information 1: EtherNet/IP communications connector for which link ON detected 1: EtherNet/IP communications connector 1 (ETH1) 2: EtherNet/IP communications connector 2 (ETH2)					
Precautions/ Remarks	None					

Event name	Operating Mode Changed		Event code	967B0000 hex	
Description	Change operating mode was executed.				
Source	-	Source details	-	Detection timing	When change operating mode executed
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected	
Cause and correction	Assumed cause		Correction	Prevention	
	Change operating mode executed.		None	None	
Attached information	Attached information 1: Reserved Attached information 2: New operating mode 2: Idle 3: Executing				
Precautions/ Remarks	None				

Event name	Safety Password Changed		Event code	967C0000 hex	
Description	The safety password was changed.				
Source	-	Source details	-	Detection timing	When command (transfer) from user
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected.	
Cause and correction	Assumed cause		Correction	Prevention	
	The safety password was changed.		None	None	
Attached information	Attached information 1: Reserved				
Precautions/ Remarks	None				

Event name	Safety Application Transferred			Event code	967D0000 hex	
Description	The safety application data was transferred to the Unit.					
Source	-		Source details	-	Detection timing	• When command (transfer) from user • When Type1 Safety Open accepted
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	• Transfer by the Web UI was accepted. • A Type 1 Safety Open request was accepted from the safety controller.		None		None	
Attached information	Attached information 1: Reserved Attached information 2: Application number Attached Information 3: SCCRC Attached Information 4: Setting method 1: Type1 Safety Open 2: Setting by Web UI function					
Precautions/ Remarks	None					

Event name	Event Log Cleared			Event code	967E0000 hex	
Description	The event log was cleared.					
Source	-		Source details	-	Detection timing	Continuously
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected.		
Cause and correction	Assumed cause		Correction		Prevention	
	The event log was cleared.		None		None	
Attached information	Attached information 1: Connection source IP address Example: C0A8FA01 hex when the IP address is 192.168.250.1. Attached information 2: Events that were cleared. 0: Logs for all categories were cleared. 1: The system event log was cleared. 2: The access event log was cleared.					
Precautions/ Remarks	None					

Event name	Backup Executed			Event code	967F0000 hex	
Description	A backup was executed.					
Source	-		Source details	-	Detection timing	When a backup was executed.
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	A backup was executed.		None		None	
Attached information	Attached information 1: Connection source IP address Example: C0A8FA64 hex when the IP address is 192.168.250.100. Attached information 2: Execution result 0000 hex: Successful 0001 hex: Failed					
Precautions/ Remarks	None					

Event name	Restore Executed			Event code	96800000 hex	
Description	A restore was executed.					
Source	-		Source details	-	Detection timing	When a restore was executed.
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	A restore was executed.		None		None	
Attached information	Attached information 1: Connection source IP address Example: C0A8FA64 hex when the IP address is 192.168.250.100. Attached information 2: Execution result 0000 hex: Successful 0001 hex: Failed					
Precautions/ Remarks	None					

Event name	OMRON Maintenance Executed			Event code	96810000 hex	
Description	Maintenance by OMRON maintenance personnel was executed.					
Source	-		Source details	-	Detection timing	When OMRON maintenance was executed.
Error attributes	Level	Information	Recovery method	-	Log category	Access
Effects	User program	Continues	Operation	Not affected		
Cause and correction	Assumed cause		Correction		Prevention	
	Maintenance by OMRON maintenance personnel was executed.		None		None	
Attached information	Attached information 1: Connection source IP address Example: C0A8FA64 hex when the IP address is 192.168.250.100.					
Precautions/ Remarks	None					

Event name	Restarted			**Event code**	96820000 hex	
Description	A restart was executed.					
Source	-		**Source details**	-	**Detection timing**	When execute a restart
Error attributes	**Level**	Information	**Recovery method**	-	**Log category**	Access
Effects	**User program**	Continues	**Operation**	Not affected		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	A restart was executed.		None		None	
Attached information	Attached information 1: Reserved					
Precautions/ Remarks	None					

Event name	Safety Configuration Validated			**Event code**	96830000 hex	
Description	The safety configuration was validated.					
Source	-		**Source details**	-	**Detection timing**	• When power is turned ON. • When execute a restart
Error attributes	**Level**	Information	**Recovery method**	-	**Log category**	System
Effects	**User program**	Continues	**Operation**	Not affected		
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The safety configuration was validated.		None		None	
Attached information	Attached information 1: Application number Attached information 2: SCCRC Attached information 3: Configuration locked state 0: Unlocked 1: Locked Attached information 4: Startup mode 0: Idle 1: Executing					
Precautions/ Remarks	None					

Event name	IP Address Indication Function Executed		Event code	96840000 hex	
Description	The IP address indication function was executed.				
Source	-	Source details	-	Detection timing	• When power is turned ON. • When execute a restart
Error attributes	Level	Information	Recovery method	-	Log category	System
Effects	User program	Continues	Operation	Not affected	
Cause and correction	Assumed cause		Correction	Prevention	
	Started up with SW1 = SW2 = 8 (IP address indication function).		None	None	
Attached information	None				
Precautions/ Remarks	None				

Event name	I/O Wiring Checking Function Executed		Event code	96850000 hex	
Description	The I/O wiring checking function was executed.				
Source	-	Source details	-	Detection timing	• When power is turned ON. • When execute a restart
Error attributes	Level	Information	Recovery method	-	Log category	System
Effects	User program	Continues	Operation	Not affected	
Cause and correction	Assumed cause		Correction	Prevention	
	Started up with SW1 = SW2 = E (I/O wiring checking function).		None	None	
Attached information	None				
Precautions/ Remarks	None				

12

Inspection and Maintenance

This chapter describes inspection and maintenance of the Safety I/O Block.

12-1 Cleaning and Inspection 12-2
12-1-1 Cleaning 12-2
12-1-2 Inspection Procedure 12-2

12-2 Replacing Units 12-4
12-2-1 Unit Replacement Precautions 12-4
12-2-2 Unit Replacement Using the Backup Function 12-4
12-2-3 Unit Replacement Without Using the Backup Function 12-5

12-1 Cleaning and Inspection

This section describes daily device maintenance such as cleaning and inspection.
Inspect the Safety I/O Block daily or periodically in order to keep it in optimal operating condition.

12-1-1 Cleaning

Clean the device regularly as described below in order to keep it in optimal operating condition.

- Wipe the device 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 device from gum, vinyl, or tape that was left on for a long time. Remove such items during regular cleaning.

Precautions for Correct Use

Never use volatile solvents, such as paint thinner, benzene, or chemical wipes. They may deteriorate the engraved or printed surfaces of the product.

12-1-2 Inspection Procedure

Be sure to perform periodic inspections to ensure the Unit is maintained in the optimal operating condition.
Inspections should be performed once every 6 to 12 months (once every month for safety validation testing).
When you operate the device in a location subject to extremely high temperatures and high humidity or dust, perform inspections more frequently.
Take immediate steps to correct the situation if any of the conditions in the following table are not met. Refer to *Inspection Items* on page 12-3 for information about the conditions.

- 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.
- Operate this product continuously for at least eight hours to complete all diagnostics because part of the diagnostic processing is executed in segments during the idle time of normal processing.

Tools Required for Inspections

● Tools Always Required

- Phillips screwdriver
- Torque handle
- Voltage tester or digital voltmeter
- Industrial alcohol and pure cotton cloth

● Tools Required Occasionally

- Oscilloscope

- Thermometer and hygrometer

Inspection Items

Inspect the following items to check if the results meet the criteria.
If the results do not meet the criteria, improve the environment or adjust the device so that the inspection results meet the criteria.

Inspection item	Inspection details	Criteria	Inspection means
Environment	Check the ambient temperature and the temperature inside the panel	-10 to 55°C	Thermometer
	Check the ambient humidity and the humidity inside the panel	25% to 85% (with no condensation)	Hygrometer
	Check for accumulation of dust	No accumulation of dust	Inspect visually
Installation condition	Check that the Unit is securely fixed	No looseness	Phillips screwdriver
	Check that the waterproof covers of the cables are tightened to an appropriate torque on the connectors of the Unit	The covers are tightened to the specified torque	Torque handle
	The rotary switch cover is tight	No looseness	Phillips screwdriver
	Check for damaged connecting cables	No visible damage	Inspect visually
Safety validation testing (user testing)	Check to be sure that all safety functions operate correctly	All functions must operate as intended	Perform operation to operate the safety functions.

12-2 Replacing Units

This section describes how to replace a running Safety I/O Block due to a failure or for maintenance or other reasons.
There are the following two Unit replacement methods.
With Unit replacement using the backup function, the setting data of all the safety applications and non-safety functions that the customer configured can be set simultaneously.
When not using the backup function, set the necessary settings individually.

- Unit replacement using the backup function
- Unit replacement without using the backup function

12-2-1 Unit Replacement Precautions

When you find a fault during inspection and replace the device, keep in mind the following:

- 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.).
- The Safety I/O Block is a network component. Note that a failure in the Unit may affect the entire network. If the Unit fails, repair it immediately. To restore the functionality of the network as soon as possible, it is recommended to prepare a spare.
- After replacement, check that there are no problems with the new device.
- When you return a faulty device for repair, send the device to your OMRON representative with a note describing your problem in as much detail as possible.
- For poor contact, take a clean cotton cloth, soak the cloth in industrial alcohol, and carefully wipe the contacts.

12-2-2 Unit Replacement Using the Backup Function

This section describes the replacement of the Safety I/O Block Unit using the backup function.
Creating a backup file using the backup function in advance will allow you to recover the setting data easily. This reduces the amount of work required for recovery. We recommend making a backup when locking the configuration. Refer to *7-19 Backup* on page 7-108 for details on the backup function, and *Restore* on page 7-109 for details on the restore procedure.

The replacement procedure is shown below.

Step	Item	Description	Tool to use
1	Execute backup*1	Execute a backup. Perform this procedure in advance of performing the replacement work. We recommend performing this procedure when starting up the device.	Web UI
2	Installation and wiring	Remove the Safety I/O Block to be replaced and install the Safety I/O Block. Set the rotary switch settings to the same settings as the previous Unit. Connect the Ethernet, power supply, and I/O cables. Connect the PC to the Safety I/O Block.	Not required
3	Set the safety password*1	Set the safety password of the Safety I/O Block.	Web UI

Step	Item	Description	Tool to use
4	Execute restore*1	Execute restoring to the Safety I/O Block.	Web UI
5	Cycle the power supply	Cycle the power supply to the Safety I/O Block or perform a restart.	Not required
6	Establish EtherNet/IP connection and CIP Safety connection	The CIP Safety originator and EtherNet/IP originator establish a connection with the Safety I/O Block.	Not required

***1.** The safety password is required for the work.

12-2-3 Unit Replacement Without Using the Backup Function

This section describes how to replace the Safety I/O Block Unit without using the backup function.

- When configuration for the safety controller to perform control (configuration using Type 1 Safety Open)
  Configure only the settings for the Safety I/O Block of *7-1-1 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using Type 1 Safety Open)* on page 7-3.
  A remote I/O safety application is configured by the safety controller when a Type1 Safety Open connection is established between the safety controller and the Safety I/O Block.

- When configuration for the safety controller to perform control (configuration using the Web UI)
  Configure only the settings for the Safety I/O Block of *7-1-2 Setting Procedure of Configuration for the Safety Controller to Perform Control (Configuration Using the Web UI)* on page 7-6.
  A remote I/O safety application is configured by using the Web UI to download a safety application file to the Safety I/O Block.

- When configuration for the Safety I/O Block to perform control using a preset safety application
  Configure only the settings for the Safety I/O Block of *7-1-3 Setting Procedure of Configuration for the Safety I/O Block to Perform Control Using a Preset Safety Application* on page 7-9.
  A fixed application of the Safety I/O Block can be set with SETTING rotary switches SW1 and SW2.

- When configuration (centralized management type) for the Safety I/O Block to perform control using a safety application designed by a user
  Configure only the settings for the Safety I/O Block of *7-1-4 Setting Procedure of Configuration (Centralized Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 7-11.
  A user-defined application is configured by the safety controller when a Type1 Safety Open connection is established between the safety controller and the Safety I/O Block.

- When configuration (distributed management type) for the Safety I/O Block to perform control using a safety application designed by a user
  Configure only the settings for the Safety I/O Block of *7-1-5 Setting Procedure of Configuration (Distributed Management Type) for the Safety I/O Block to Perform Control Using a Safety Application Designed by a User* on page 7-14.
  An add-on application is configured by using the Web UI to download a safety application file to the Safety I/O Block.

A

Appendices

The appendices provide the dimensions, safety I/O assembly data, and other supplemental information for the Safety I/O Block.

A-1 Dimensions A-2

A-2 Safety I/O Assembly Data A-4

A-2-1 Safety Input Assembly Data A-4
A-2-2 Safety Output Assembly Data A-6
A-2-3 Configuration Assembly Data A-7

A-3 I/O Assembly Ports and Corresponding Safety I/O Assembly Data Elements A-14

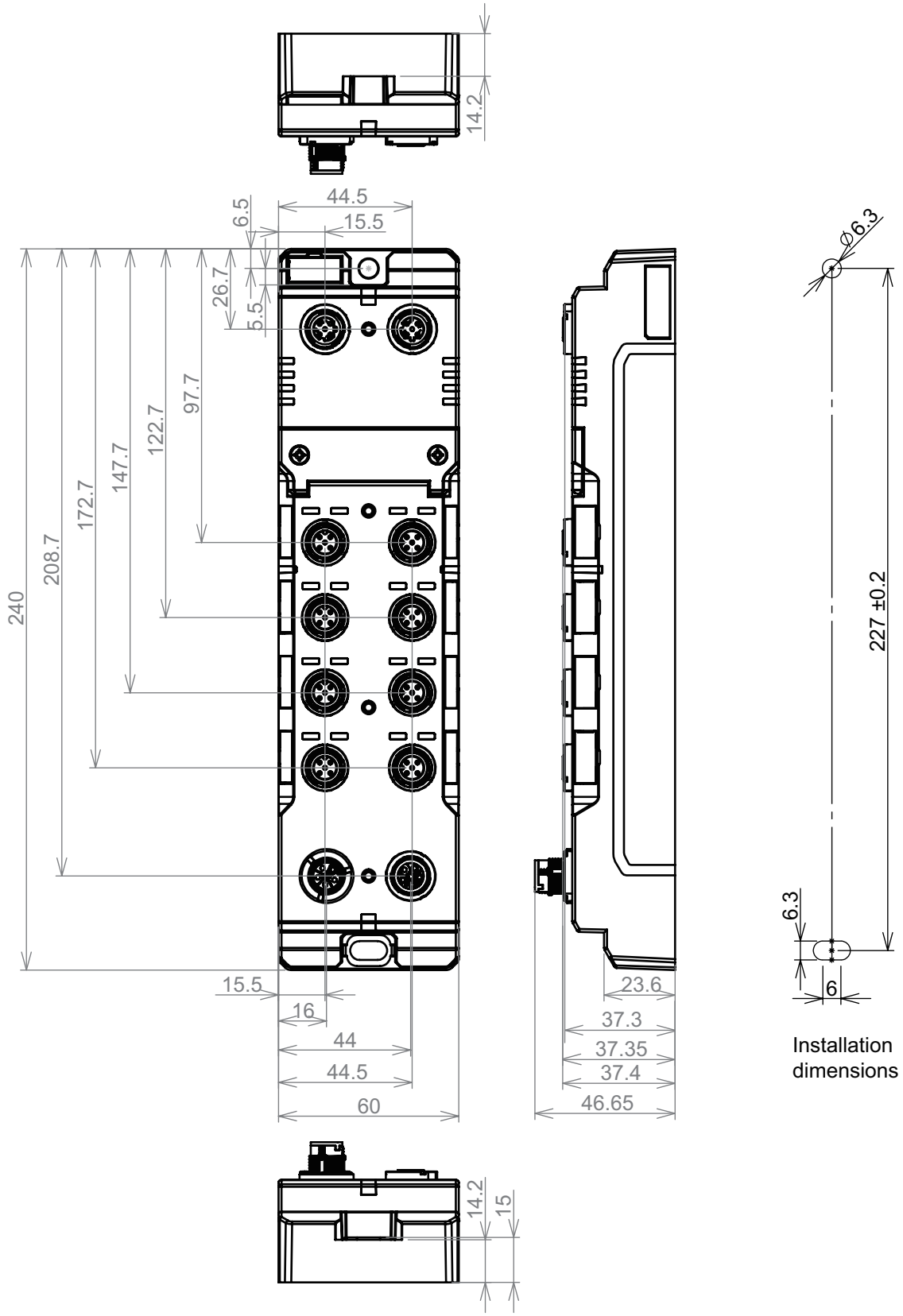
A-4 Supported CIP Objects A-16

A-4-1 Identity Object (Class ID: 01 Hex) A-17
A-4-2 Assembly Object (Class ID: 04 Hex) A-19
A-4-3 Unit Manager Object (Class ID: 380 Hex) A-22
A-4-4 Event History Log Object (Class ID: 34B Hex) A-27
A-4-5 Error Event Object (Class ID: 34C Hex) A-30
A-4-6 Safety Discrete Input Point (SDIP) Object (Class ID: 3D Hex) A-33
A-4-7 Safety Discrete Output Point (SDOP) Object (Class ID: 3B Hex) A-35
A-4-8 Device Level Ring (DLR) Object (Class ID: 47 Hex) A-37
A-4-9 QoS Object (Class ID: 48 Hex) A-39
A-4-10 TCP/IP Interface Object (Class ID: F5 Hex) A-41
A-4-11 Ethernet Link Object (Class ID: F6 Hex) A-45
A-4-12 LLDP Management Object (Class ID: 109 Hex) A-51
A-4-13 LLDP Data Table Object (Class ID: 10A Hex) A-53
A-4-14 Logic Process Object (Class ID: 309 Hex) A-58

A-5 Declaration of Conformity A-60

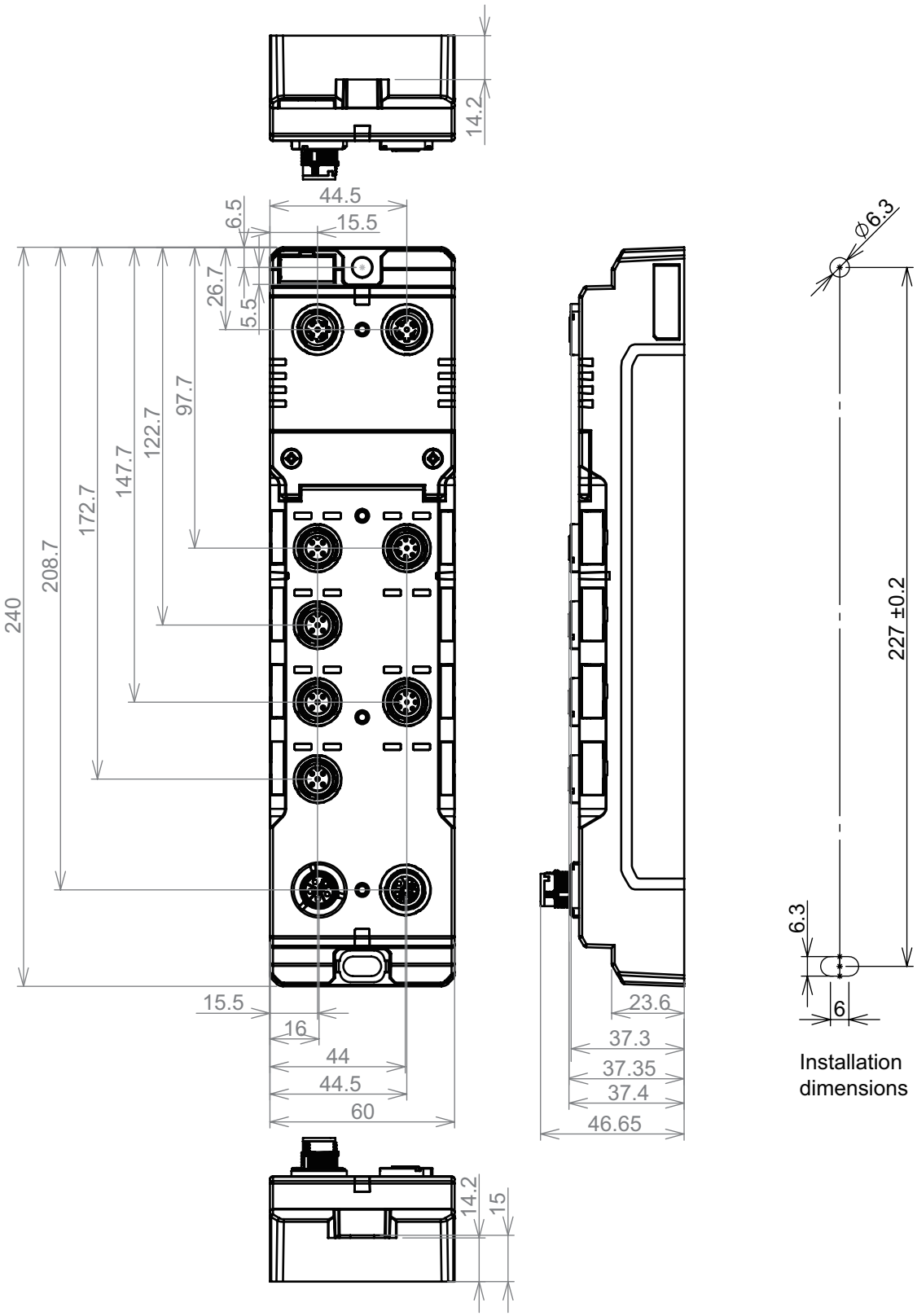
A-1 Dimensions

NXR-SXD1204-CST



Installation dimensions

NXR-SXD1204B-CST



Installation dimensions

A-2 Safety I/O Assembly Data

The I/O assembly data of the Safety I/O Block consists of the following.

A-2-1 Safety Input Assembly Data

This section shows the safety input assembly data.
The meaning of each element in the data is as follows.

Element	Meaning	Attribute
Safety Input N	Value of safety input terminal Si N 0: Safety input terminal is OFF or an error is occurring 1: Safety input terminal is ON	Safety
Safety Input N Status	Status information of safety input terminal Si N 0: Error is occurring 1: Normal (no errors)	Safety
Safety Input Status	Status information of safety input terminals (aggregate) 0: There is an error on one of the safety input terminals 1: All of the safety input terminals are normal	Safety
Test Output N Monitor	Value of test output terminal T N 0: Test output terminal is OFF or an error is occurring 1: Test output terminal is ON	Not Safety
Test Output N Status	Status information of test output terminal T N 0: Error is occurring 1: Normal (no errors)	Not Safety
Safety Output N Monitor	Value actually output to safety output terminal So N 0: Safety output terminal is OFF 1: Safety output terminal is ON	Not Safety
Safety Output N Status	Status information of safety output terminal So N 0: Error is occurring 1: Normal (no errors)	Safety
Safety Output Status	Status information of safety output terminals (aggregate) 0: There is an error on one of the safety output terminals 1: All of the safety output terminals are normal	Safety
Output Power Supply Error Flag	Output power supply error flag 0: Output power supply is normal 1: Output power supply is abnormal or power supply is OFF	Not Safety
Application Number	Safety application number	Not Safety
Cnxn Status	Connection status information 0: Connections are not established. 1: Connections are established.	Not Safety

Input Data (Assembly 604 to 25C Hex), Size 2 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0

Byte	Bit							
	7	6	5	4	3	2	1	0
1	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8

Input Data (Assembly 960 to 3C0 Hex), Size 5 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input 3 Status	Safety Input 2 Status	Safety Input 1 Status	Safety Input 0 Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8
2	Safety Input 11 Status	Safety Input 10 Status	Safety Input 9 Status	Safety Input 8 Status	Safety Input 7 Status	Safety Input 6 Status	Safety Input 5 Status	Safety Input 4 Status
3	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	Reserved	Reserved	Reserved	Reserved
4	Application Number							

Input Data (Assembly 961 to 3C1 Hex), Size 9 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input 3 Status	Safety Input 2 Status	Safety Input 1 Status	Safety Input 0 Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8
2	Safety Input 11 Status	Safety Input 10 Status	Safety Input 9 Status	Safety Input 8 Status	Safety Input 7 Status	Safety Input 6 Status	Safety Input 5 Status	Safety Input 4 Status
3	Safety Output 3 Monitor	Safety Output 2 Monitor	Safety Output 1 Monitor	Safety Output 0 Monitor	Safety Output 3 Status	Safety Output 2 Status	Safety Output 1 Status	Safety Output 0 Status
4	Test Output 7 Status	Test Output 6 Status	Test Output 5 Status	Test Output 4 Status	Test Output 3 Status	Test Output 2 Status	Test Output 1 Status	Test Output 0 Status
5	Test Output 3 Monitor	Test Output 2 Monitor	Test Output 1 Monitor	Test Output 0 Monitor	Test Output 11 Status	Test Output 10 Status	Test Output 9 Status	Test Output 8 Status
6	Test Output 11 Monitor	Test Output 10 Monitor	Test Output 9 Monitor	Test Output 8 Monitor	Test Output 7 Monitor	Test Output 6 Monitor	Test Output 5 Monitor	Test Output 4 Monitor
7	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	Reserved	Reserved	Reserved	Reserved
8	Application Number							

A-2-2 Safety Output Assembly Data

This section shows the safety output assembly data.
The meaning of each element in the data is as follows.

Element	Meaning	Attribute
Safety Output N	ON/OFF to safety output terminal So N 0: Safety output OFF 1: Safety output ON	Safety
Standard Output N	ON/OFF of standby output to test output terminal T N 0: Standard output OFF 1: Standard output ON	Not Safety
Remote N Output M	ON/OFF of remote outputs Ro N - M 0: Remote output OFF 1: Remote output ON	Safety

Output Data (Assembly 563 to 233 Hex), Size 1 Byte

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Reserved	Reserved	Reserved	Reserved	Safety Output 3	Safety Output 2	Safety Output 1	Safety Output 0

Output Data (Assembly 881 to 371 Hex), Size 3 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Remote1 Output 1	Remote1 Output 0
1	Standard Output 7	Standard Output 6	Standard Output 5	Standard Output 4	Standard Output 3	Standard Output 2	Standard Output 1	Standard Output 0
2	Reserved	Reserved	Reserved	Reserved	Standard Output 11	Standard Output 10	Standard Output 9	Standard Output 8

Output Data (Assembly 882 to 372 Hex), Size 1 Byte

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Remote2 Output 1	Remote2 Output 0

Output Data (Assembly 883 to 373 Hex), Size 1 Byte

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Remote3 Output 1	Remote3 Output 0

Output Data (Assembly 896 to 380 Hex), Size 3 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Reserved	Reserved	Reserved	Reserved	Safety Output 3	Safety Output 2	Safety Output 1	Safety Output 0
1	Standard Output 7	Standard Output 6	Standard Output 5	Standard Output 4	Standard Output 3	Standard Output 2	Standard Output 1	Standard Output 0
2	Reserved	Reserved	Reserved	Reserved	Standard Output 11	Standard Output 10	Standard Output 9	Standard Output 8

A-2-3 Configuration Assembly Data

This section shows the configuration assembly data.
The meaning of each element in the data is as follows.

Element	Meaning
Power-on Mode	Startup mode 0: Stopped (idle) 1: Executing
Test Output N Mode	Mode used for test output terminal T N 0: Not Used 1: Standard Output 2: Test Output 3: Power Supply Output
Safety Output Error Latch Time	Output error latch time of the safety output terminal
Safety Output N Channel Mode	Mode used for safety output terminal So N 0: Not used 1: Used without test pulse 2: Used with test pulse
Safety Output N/N+1 Dual Channel Mode	Mode used for safety output terminals So N and So N+1 0: Single channel 1: Dual channel
Safety Input Error Latch Time	Input error latch time of the safety input terminal
Safety Input N Off_On_Delay	OFF→ON delay time of safety input terminal Si N
Safety Input N On_Off_Delay	ON→OFF delay time of safety input terminal Si N
Safety Input N Channel Mode	Mode used for safety input terminal Si N 0: Not used 1: Used together with test output terminal 2: Used without test pulse as semiconductor input device 3: Used without test pulse as standard input
Safety Input N Test Source	Number of test output terminal to use connected with safety input terminal Si N
Safety Input N/N+1 Dual Channel Mode	Mode used for safety input terminals Si N and Si N+1 0: Single channel 1: Dual-channel equivalent input 2: Dual-channel complementary input
Safety Input N/N+1 Discrepancy Time	Discrepancy time
Output Logic N Off_On_Delay	OFF→ON delay time of safety output terminal So N
Output Logic N On_Off_Delay	ON→OFF delay time of safety output terminal So N
Output Logic N Output Condition	Output value condition of logic for safety output terminal So N

Element	Meaning
Output Logic N EDM Feedback	Number of safety input terminal to use to input the EDM feedback value to safety output terminal So N
Input Logic N Input Condition1	Condition of input condition calculation of logic of safety input terminal Si N and remote output
Input Logic N Reset Condition	Condition of reset calculation of logic of safety input terminal Si N and remote output
Input Logic N Reset Minimum ON Pulse Width	Minimum ON pulse width of reset signal for safety input terminal Si N and remote output
Input Logic N Reset Maximum ON Pulse Width	Maximum ON pulse width of reset signal for safety input terminal Si N and remote output

Configuration (Assembly 864 to 360 Hex), Size 340 Bytes

Data	Size (byte)	Offset (byte)
Power-on Mode	1	0
Padding	1	1
Test Output 0 Mode	1	2
Test Output 1 Mode	1	3
Test Output 2 Mode	1	4
Test Output 3 Mode	1	5
Test Output 4 Mode	1	6
Test Output 5 Mode	1	7
Test Output 6 Mode	1	8
Test Output 7 Mode	1	9
Test Output 8 Mode	1	10
Test Output 9 Mode	1	11
Test Output 10 Mode	1	12
Test Output 11 Mode	1	13
Safety Output Error Latch Time	2	14
Safety Output 0 Channel Mode	1	16
Safety Output 1 Channel Mode	1	17
Safety Output 2 Channel Mode	1	18
Safety Output 3 Channel Mode	1	19
Safety Out 0/1 Dual Channel Mode	1	20
Safety Out 2/3 Dual Channel Mode	1	21
Safety Input Error Latch Time	2	22
Safety Input 0 Off_On_Delay	2	24
Safety Input 0 On_Off_Delay	2	26
Safety Input 0 Channel Mode	1	28
Safety Input 0 Test Source	1	29
Safety Input 1 Off_On_Delay	2	30
Safety Input 1 On_Off_Delay	2	32
Safety Input 1 Channel Mode	1	34
Safety Input 1 Test Source	1	35
Safety Input 2 Off_On_Delay	2	36
Safety Input 2 On_Off_Delay	2	38
Safety Input 2 Channel Mode	1	40

Data	Size (byte)	Offset (byte)
Safety Input 2 Test Source	1	41
Safety Input 3 Off_On_Delay	2	42
Safety Input 3 On_Off_Delay	2	44
Safety Input 3 Channel Mode	1	46
Safety Input 3 Test Source	1	47
Safety Input 4 Off_On_Delay	2	48
Safety Input 4 On_Off_Delay	2	50
Safety Input 4 Channel Mode	1	52
Safety Input 4 Test Source	1	53
Safety Input 5 Off_On_Delay	2	54
Safety Input 5 On_Off_Delay	2	56
Safety Input 5 Channel Mode	1	58
Safety Input 5 Test Source	1	59
Safety Input 6 Off_On_Delay	2	60
Safety Input 6 On_Off_Delay	2	62
Safety Input 6 Channel Mode	1	64
Safety Input 6 Test Source	1	65
Safety Input 7 Off_On_Delay	2	66
Safety Input 7 On_Off_Delay	2	68
Safety Input 7 Channel Mode	1	70
Safety Input 7 Test Source	1	71
Safety Input 8 Off_On_Delay	2	72
Safety Input 8 On_Off_Delay	2	74
Safety Input 8 Channel Mode	1	76
Safety Input 8 Test Source	1	77
Safety Input 9 Off_On_Delay	2	78
Safety Input 9 On_Off_Delay	2	80
Safety Input 9 Channel Mode	1	82
Safety Input 9 Test Source	1	83
Safety Input 10 Off_On_Delay	2	84
Safety Input 10 On_Off_Delay	2	86
Safety Input 10 Channel Mode	1	88
Safety Input 10 Test Source	1	89
Safety Input 11 Off_On_Delay	2	90
Safety Input 11 On_Off_Delay	2	92
Safety Input 11 Channel Mode	1	94
Safety Input 11 Test Source	1	95
Safety Input 0/1 Dual Channel Mode	1	96
padding	1	97
Safety Input 0/1 Discrepancy Time	2	98
Safety Input 2/3 Dual Channel Mode	1	100
padding	1	101
Safety Input 2/3 Discrepancy Time	2	102
Safety Input 4/5 Dual Channel Mode	1	104
padding	1	105
Safety Input 4/5 Discrepancy Time	2	106
Safety Input 6/7 Dual Channel Mode	1	108

Data	Size (byte)	Offset (byte)
padding	1	109
Safety Input 6/7 Discrepancy Time	2	110
Safety Input 8/9 Dual Channel Mode	1	112
padding	1	113
Safety Input 8/9 Discrepancy Time	2	114
Safety Input 10/11 Dual Channel Mode	1	116
padding	1	117
Safety Input 10/11 Discrepancy Time	2	118
Output Logic 0 Off_On_Delay	2	120
Output Logic 0 On_Off_Delay	2	122
Output Logic 0 Output Condition	4	124
Output Logic 0 EDM Feedback	1	128
Padding	1	129
Output Logic 1 Off_On_Delay	2	130
Output Logic 1 On_Off_Delay	2	132
Output Logic 1 Output Condition	4	134
Output Logic 1 EDM Feedback	1	138
Padding	1	139
Output Logic 2 Off_On_Delay	2	140
Output Logic 2 On_Off_Delay	2	142
Output Logic 2 Output Condition	4	144
Output Logic 2 EDM Feedback	1	148
Padding	1	149
Output Logic 3 Off_On_Delay	2	150
Output Logic 3 On_Off_Delay	2	152
Output Logic 3 Output Condition	4	154
Output Logic 3 EDM Feedback	1	158
Padding	1	159
Input Logic 0 Input Condition	4	160
Input Logic 0 Reset Condition	1	164
Padding	1	165
Input Logic 0 Reset Minimum ON Pulse Width	2	166
Input Logic 0 Reset Maximum ON Pulse Width	2	168
Input Logic 1 Input Condition	4	170
Input Logic 1 Reset Condition	1	174
Padding	1	175
Input Logic 1 Reset Minimum ON Pulse Width	2	176
Input Logic 1 Reset Maximum ON Pulse Width	2	178
Input Logic 2 Input Condition	4	180
Input Logic 2 Reset Condition	1	184
Padding	1	185
Input Logic 2 Reset Minimum ON Pulse Width	2	186

Data	Size (byte)	Offset (byte)
Input Logic 2 Reset Maximum ON Pulse Width	2	188
Input Logic 3 Input Condition	4	190
Input Logic 3 Reset Condition	1	194
Padding	1	195
Input Logic 3 Reset Minimum ON Pulse Width	2	196
Input Logic 3 Reset Maximum ON Pulse Width	2	198
Input Logic 4 Input Condition	4	200
Input Logic 4 Reset Condition	1	204
Padding	1	205
Input Logic 4 Reset Minimum ON Pulse Width	2	206
Input Logic 4 Reset Maximum ON Pulse Width	2	208
Input Logic 5 Input Condition	4	210
Input Logic 5 Reset Condition	1	214
Padding	1	215
Input Logic 5 Reset Minimum ON Pulse Width	2	216
Input Logic 5 Reset Maximum ON Pulse Width	2	218
Input Logic 6 Input Condition	4	220
Input Logic 6 Reset Condition	1	224
Padding	1	225
Input Logic 6 Reset Minimum ON Pulse Width	2	226
Input Logic 6 Reset Maximum ON Pulse Width	2	228
Input Logic 7 Input Condition	4	230
Input Logic 7 Reset Condition	1	234
Padding	1	235
Input Logic 7 Reset Minimum ON Pulse Width	2	236
Input Logic 7 Reset Maximum ON Pulse Width	2	238
Input Logic 8 Input Condition	4	240
Input Logic 8 Reset Condition	1	244
Padding	1	245
Input Logic 8 Reset Minimum ON Pulse Width	2	246
Input Logic 8 Reset Maximum ON Pulse Width	2	248
Input Logic 9 Input Condition	4	250
Input Logic 9 Reset Condition	1	254
Padding	1	255
Input Logic 9 Reset Minimum ON Pulse Width	2	256

Data	Size (byte)	Offset (byte)
Input Logic 9 Reset Maximum ON Pulse Width	2	258
Input Logic 10 Input Condition	4	260
Input Logic 10 Reset Condition	1	264
Padding	1	265
Input Logic 10 Reset Minimum ON Pulse Width	2	266
Input Logic 10 Reset Maximum ON Pulse Width	2	268
Input Logic 11 Input Condition	4	270
Input Logic 11 Reset Condition	1	274
Padding	1	275
Input Logic 11 Reset Minimum ON Pulse Width	2	276
Input Logic 11 Reset Maximum ON Pulse Width	2	278
Input Logic 12 Input Condition	4	280
Input Logic 12 Reset Condition	1	284
Padding	1	285
Input Logic 12 Reset Minimum ON Pulse Width	2	286
Input Logic 12 Reset Maximum ON Pulse Width	2	288
Input Logic 13 Input Condition	4	290
Input Logic 13 Reset Condition	1	294
Padding	1	295
Input Logic 13 Reset Minimum ON Pulse Width	2	296
Input Logic 13 Reset Maximum ON Pulse Width	2	298
Input Logic 14 Input Condition	4	300
Input Logic 14 Reset Condition	1	304
Padding	1	305
Input Logic 14 Reset Minimum ON Pulse Width	2	306
Input Logic 14 Reset Maximum ON Pulse Width	2	308
Input Logic 15 Input Condition	4	310
Input Logic 15 Reset Condition	1	314
Padding	1	315
Input Logic 15 Reset Minimum ON Pulse Width	2	316
Input Logic 15 Reset Maximum ON Pulse Width	2	318
Input Logic 16 Input Condition	4	320
Input Logic 16 Reset Condition	1	324
Padding	1	325
Input Logic 16 Reset Minimum ON Pulse Width	2	326

Data	Size (byte)	Offset (byte)
Input Logic 16 Reset Maximum ON Pulse Width	2	328
Input Logic 17 Input Condition	4	330
Input Logic 17 Reset Condition	1	334
Padding	1	335
Input Logic 17 Reset Minimum ON Pulse Width	2	336
Input Logic 17 Reset Maximum ON Pulse Width	2	338

A-3 I/O Assembly Ports and Corresponding Safety I/O Assembly Data Elements

The following shows the I/O assemblies of the Safety I/O Block, and the port names when the I/O assemblies are expanded in the I/O map.
Each port corresponds one-to-one with an element of the safety I/O assembly data.
Refer to *A-2 Safety I/O Assembly Data* on page A-4 for the meaning of elements of the safety I/O assembly data.

I/O Assembly	Port	Data type	R/W	Size (bit)	Element of corresponding safety I/O assembly data
Safety Input 1	Safety Input 0-11 Logical Value	SAFEBOOL	R	12	Safety Input N
	Safety Cnxn Status	SAFEBOOL	R	1	Cnxn Status
	Output Power Status	SAFEBOOL	R	1	Output Power Supply Error Flag
	Combined Safety Output Status	SAFEBOOL	R	1	Safety Output Status
	Combined Safety Input Status	SAFEBOOL	R	1	Safety Input Status
Safety Input 2	Safety Input 0-11 Logical Value	SAFEBOOL	R	12	Safety Input N
	Safety Input 0-11 Status	SAFEBOOL	R	12	Safety Input N Status
	Safety Cnxn status	SAFEBOOL	R	1	Cnxn Status
	Output Power Status	SAFEBOOL	R	1	Output Power Supply Error Flag
	Combined Safety Output Status	SAFEBOOL	R	1	Safety Output Status
	Combined Safety Input Status	SAFEBOOL	R	1	Safety Input Status
	Application Number	SAFEINT	R	8	Application Number
Safety Input 3	Safety Input 0-11 Logical Value	SAFEBOOL	R	12	Safety Input N
	Safety Input 0-11 Status	SAFEBOOL	R	12	Safety Input N Status
	Safety Output 0-3 Status	SAFEBOOL	R	4	Safety Output N Status
	Safety Output 0-3 Monitor Value	SAFEBOOL	R	4	Safety Output N Monitor
	Test Output 0-11 Status	SAFEBOOL	R	12	Test Output N Status
	Test Output 0-11 Value	SAFEBOOL	R	12	Test Output N Monitor
	Safety Cnxn status	SAFEBOOL	R	1	Cnxn Status
	Output Power Status	SAFEBOOL	R	1	Output Power Supply Error Flag
	Combined Safety Output Status	SAFEBOOL	R	1	Safety Output Status
	Combined Safety Input Status	SAFEBOOL	R	1	Safety Input Status
	Application Number	SAFEINT	R	8	Application Number
Safety Output	Safety Output 0-3 Value	SAFEBOOL	W	4	Safety Output N

I/O Assembly	Port	Data type	R/W	Size (bit)	Element of corresponding safety I/O assembly data
Safety Remote Output 1 + Standard Output	Remote 1 Output 0-1	SAFEBOOL	W	2	Remote N Output M
	Test Output 0-11 Value	SAFEBOOL	W	12	Standard Output N
Safety Remote Output 2	Remote 2 Output 0-1	SAFEBOOL	W	2	Remote N Output M
Safety Remote Output 3	Remote 3 Output 0-1	SAFEBOOL	W	2	Remote N Output M
Safety Output + Standard Output	Safety Output 0-3 Value	SAFEBOOL	W	4	Safety Output N
	Test Output 0-11 Value	SAFEBOOL	W	12	Standard Output N

A-4 Supported CIP Objects

The supported CIP objects are listed below.
To access CIP objects in the Safety I/O Block, use an explicit message. Refer to *Explicit Message Server Function* on page 6-7 for information on the method to access CIP objects through an explicit message.

Object name	Function	Reference
Identity object	Reads the product information of the Safety I/O Block.	*A-4-1 Identity Object (Class ID: 01 Hex)* on page A-17
Assembly object	Binds the I/O data of the external devices connected to the Safety I/O Block.	*A-4-2 Assembly Object (Class ID: 04 Hex)* on page A-19
Unit Manager object	Aggregates the unit Information on the Safety I/O Block.	*A-4-3 Unit Manager Object (Class ID: 380 Hex)* on page A-22
Event History Log object	Manages the event logs.	*A-4-4 Event History Log Object (Class ID: 34B Hex)* on page A-27
Error Event object	Manages the currently occurring error events.	*A-4-5 Error Event Object (Class ID: 34C Hex)* on page A-30
Safety Discrete Input Point (SDIP) object	Manages the safety input terminals individually, one terminal at a time.	*A-4-6 Safety Discrete Input Point (SDIP) Object (Class ID: 3D Hex)* on page A-33
Safety Discrete Output Point (SDOP) object	Manages the safety output terminals individually, one terminal at a time.	*A-4-7 Safety Discrete Output Point (SDOP) Object (Class ID: 3B Hex)* on page A-35
Device Level Ring (DLR) object	Indicates the status of the DLR network.	*A-4-8 Device Level Ring (DLR) Object (Class ID: 47 Hex)* on page A-37
QoS object	Sets the value of the IPv4 DiffServ Code Point (DSCP) under Ethernet frame priority control.	*A-4-9 QoS Object (Class ID: 48 Hex)* on page A-39
TCP/IP Interface object	Configures the TCP/IP interface settings.	*A-4-10 TCP/IP Interface Object (Class ID: F5 Hex)* on page A-41
Ethernet Link object	Gets various information on an Ethernet link.	*A-4-11 Ethernet Link Object (Class ID: F6 Hex)* on page A-45
LLDP Management object	Manages the LLDP function.	*A-4-12 LLDP Management Object (Class ID: 109 Hex)* on page A-51
LLDP Data Table object	Manages the data of the LLDP function.	*A-4-13 LLDP Data Table Object (Class ID: 10A Hex)* on page A-53
Logic Process object	Reads the number of the application that is operating.	*A-4-14 Logic Process Object (Class ID: 309 Hex)* on page A-58

Precautions for Correct Use

For the above CIP objects, if the data type of parameter data is INT, UINT, UDINT, ULINT, WORD, or DWORD, store the data to write in little endian format. The read data is also stored in little endian format.
Note that notations in this manual follow the standard hexadecimal format, with high-order digits on the left and low-order digits on the right.

A-4-1 Identity Object (Class ID: 01 Hex)

The Identity object is used to read the product information from the Safety I/O Block.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	01	-
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0002

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name		Description	Attribute	Data	
					Data type	Value
1	Vendor ID		Vendor ID	Reading	UINT	002F hex
2	Device Type		Device type	Reading	UINT	0308 hex (Safety IO and Logic Device)
3	Product Code		Product code	Reading	UINT	NXR-SXD1204-CST: 0BF9 hex NXR-SXD1204B-CST: 0BFA hex
4	Revision		Device CIP revision	Reading	STRUCT	–
		Major Revision	Major revision		USINT	01 hex
		Minor Revision	Minor revision		USINT	01 hex
5	Status		Status of Safety I/O Block	Reading	WORD	Refer to *Values of Status* on page A-18 below.
6	Serial Number		Serial number	Reading	UDINT	Unique number for each product unit
7	Product Name		Product name	Reading	SHORT STRING	Refer to *Value of Product Name* on page A-18 below.

● Values of Status

Bit	Name	Description
0	Owned	Indicates that the Safety I/O Block opened a connection as the target. • TRUE: Opened • FALSE: Not opened
1	Reserved	Always FALSE
2	Configured	Indicates that the Safety I/O Block is configured. • TRUE: Configured • FALSE: Not configured
3	Reserved	Always FALSE
4 to 7	Extended Device Status	*1
8	Reserved	Always FALSE
9	Reserved	Always FALSE
10	Major Recoverable Fault	• TRUE: An error for which the MS indicator flashes in red is occurring. • FALSE: An error for which the MS indicator flashes in red is not occurring.
11	Major Unrecoverable Fault	• TRUE: An error for which the MS indicator lights in red is occurring. • FALSE: An error for which the MS indicator lights in red is not occurring.
12 to 15	Reserved	Always FALSE

***1.** The meaning of the values of Extended Status is as follows.

- 0 to 1: Reserved
- 2: One or more timeouts are occurring with a class 1 communications (tag data link) connection.
- 3: A class 1 communications (tag data link) connection is not established.
- 4-5 : Reserved
- 6: One or more class 1 communications (tag data link) connections are communicating normally in RUN mode.
- 7: One or more class 1 communications (tag data link) connections are established, and they are all in Idle mode.
- 8 to 15: Reserved

● Value of Product Name

Model	Value (hex)
NXR-SXD1204-CST	0F 4E 58 52 2D 53 58 44 31 32 30 34 2D 43 53 54
NXR-SXD1204B-CST	10 4E 58 52 2D 53 58 44 31 32 30 34 42 2D 43 53 54

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
01	Get_Attribute_All	Reads the values of all attributes.	Not possible	Possible
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible

A-4-2 Assembly Object (Class ID: 04 Hex)

The Assembly object is used to bind the I/O data of the external devices connected to the Safety I/O Block.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	04	–
Instance ID	00	Specifies the class itself.
	25C, 3C0, 3C1	Safety input assembly data
	233, 371, 372, 373, 380	Safety output assembly data
	360	Configuration assembly data

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0003

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.
Writing is possible when the assigned instance is Standard Output only.

Attribute ID for instance ID 25C hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Input Data (Assembly 604 to 25C Hex), Size 2 Bytes* on page A-4.

Attribute ID for instance ID 3C0 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Input Data (Assembly 960 to 3C0 Hex), Size 5 Bytes* on page A-5.

Attribute ID for instance ID 3C1 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Input Data (Assembly 961 to 3C1 Hex), Size 9 Bytes* on page A-5.

Attribute ID for instance ID 233 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Output Data (Assembly 563 to 233 Hex), Size 1 Byte* on page A-6.

Attribute ID for instance ID 371 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Output Data (Assembly 881 to 371 Hex), Size 3 Bytes* on page A-6.

Attribute ID for instance ID 372 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Output Data (Assembly 882 to 372 Hex), Size 1 Byte* on page A-6.

Attribute ID for instance ID 373 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Output Data (Assembly 883 to 373 Hex), Size 1 Byte* on page A-6.

Attribute ID for instance ID 380 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	Refer to *Output Data (Assembly 896 to 380 Hex), Size 3 Bytes* on page A-7.

Attribute ID for instance ID 360 hex

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
03	Data	Input/output data	Reading	ARRAY OF BYTE	*Configuration (Assembly 864 to 360 Hex), Size 340 Bytes* on page A-8

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible

A-4-3 Unit Manager Object (Class ID: 380 Hex)

The Unit Manager object aggregates Unit information on the Safety I/O Block.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	380	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Unit Version	Unit version	Reading	DWORD	Refer to *Values of Unit Version and Hardware Version* on page A-25 below.
2	Hardware Version	Hardware version	Reading	DWORD	Refer to *Values of Unit Version and Hardware Version* on page A-25 below.
3	Firmware Version	Firmware version	Reading	DWORD	Refer to *Values of Firmware Version* on page A-25 below.
5	Unit/Input Power Voltage	Unit/input power supply voltage	Reading	UINT	Present value of the Unit/input power supply voltage *1 The value is in 100 mV units. For example, the value is 241 in the case of 24.1 V.
6	Max Unit/ Input Power Voltage	Maximum Unit/input power supply voltage	Reading	UINT	Maximum value of the Unit/input power supply voltage *1 The value is in 100 mV units.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
7	Min Unit/ Input Power Voltage	Minimum Unit/ input power supply voltage	Reading	UINT	Minimum value of the Unit/input power supply voltage *1 The value is in 100 mV units.
8	Output Power Voltage	Output power supply voltage	Reading	UINT	Present value of the output power supply voltage *1 The value is in 100 mV units.
9	Max Output Power Voltage	Maximum output power supply voltage	Reading	UINT	Maximum value of the output power supply voltage *1 The value is in 100 mV units.
10	Min Output Power Supply Voltage	Minimum output power supply voltage	Reading	UINT	Minimum value of the output power supply voltage *1 The value is in 100 mV units.
11	Operate Hours	Unit total operating hours	Reading	UDINT	Total operating hours of Unit (Unit: h)
12	SNTP server IP address	IP address of SNTP server	Reading/ writing	UDINT	"0": Automatic clock adjustment disabled Other than "0": IP address of SNTP server The setting is enabled after restarting the Unit. The following values cannot be set. • IP addresses that start with 0, 127, or 255 • Class-D IP addresses (224.0.0.0 to 239.255.255.255) • Class-E IP addresses (240.0.0.0 to 255.255.255.255) • Link local addresses (169.254.0.0 to 169.254.255.255)
20	Unit/Input Power Current	Unit/input power supply current	Reading	UINT	Present value of the Unit/input power supply current *1 The value is in 100 mA units. For example, the value is 51 in the case of 5.1 A.
21	Max Unit/ Input Power Current	Maximum Unit/input power supply current	Reading	UINT	Maximum value of the Unit/input power supply current *1 The value is in 100 mA units.
22	Min Unit/ Input Power Current	Minimum Unit/ input power supply current	Reading	UINT	Minimum value of the Unit/input power supply current *1 The value is in 100 mA units.
23	Output Power Current	Output power supply current	Reading	UINT	Present value of the output power supply current *1 The value is in 100 mA units.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
24	Max Output Power Current	Maximum output power supply current	Reading	UINT	Maximum value of the output power supply current *1 The value is in 100 mA units.
25	Min Output Power Current	Minimum output power supply current	Reading	UINT	Minimum value of the output power supply current *1 The value is in 100 mA units.
26	Unit/Input Power Supply Error Flag	Unit/input power supply error flag	Reading	BOOL	TRUE: Voltage value is outside normal range FALSE: Voltage value is inside normal range
27	Output Power Supply Error Flag	Output power supply error flag	Reading	BOOL	TRUE: Voltage value is outside normal range FALSE: Voltage value is inside normal range
28	Cross-Wiring Output Power Shut-off Control	Through-wiring output power supply	Reading/ writing	BOOL	TRUE: Through-wiring output power is supplied (default value). FALSE: Through-wiring output power is not supplied. However, this is enabled only when the value of Cross-Wiring Output Shut-off Enable is TRUE.
29	Cross-Wiring Output Power Shut-off Enable	Enable or disable the power shut-off function for through-wiring output	Reading/ writing	BOOL	TRUE: The power shut-off function for through-wiring output is used (default value). FALSE: The power shut-off function for through-wiring output is not used. The new settings are applied immediately.
30	Communication Port Enable	Communications enable/ disable setting	Reading/ writing	USINT	0: Ports 1 and 2 are both enabled (default value) 1: Port 1 is enabled and port 2 is disabled 2: Port 1 is disabled and port 2 is enabled This setting is enabled after restarting.
100	Time	Current time	Reading	DATE_AND_TIME	Local time according to the time zone. When the time information is obtained through automatic clock adjustment (SNTP), it becomes the time corrected by SNTP. When SNTP is not used, it becomes the time counted from 00:00:00 on January 1, 1972. The default value is DT#1972-01-01-00:00:00.000.
102	Time Zone Offset - Minutes	Difference in minutes between Coordinated Universal Time (UTC) and Time	Reading/ writing	INT	-720 to 840 Indicates the difference in minutes between Coordinated Universal Time (UTC) and Time. For example if UTC is 0:00 AM and Time is 2:30 AM, the value of Time Zone Offset - Minutes will be 150. The default value is 0. The setting is enabled after restarting the Unit.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
104	Firmware Hash Value	Firmware hash value	Reading	ARRAY OF USINT	Firmware hash value 32 bytes

***1.** When the Unit is restarted, the value is reset.

● Values of Unit Version and Hardware Version

Bit	Name	Description
0 to 15	Reserved	Always FALSE
16 to 23	Minor version number field	The minor version is expressed as BCD. 0 to 99
24 to 31	Major version number field	The major version is expressed as BCD. 0 to 9

For example, if the Unit version is 1.01, the value of the Unit version is 01010000 hex. If the Unit version is 7.12, the value of the Unit version is 07120000 hex.

● Values of Firmware Version

Bit	Name	Description
0 to 7	Reserved	Always FALSE
8 to 15	Revision number field	The revision number is expressed as BCD. 0 to 99
16 to 23	Minor version number field	The minor version is expressed as BCD. 0 to 99
24 to 31	Major version number field	The major version is expressed as BCD. 0 to 9

For example, if the firmware version is 1.01.02, the value of the firmware version is 01010200 hex. If the firmware version is 7.00.10, the value of the firmware version is 07001000 hex.

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible
4B	Execute_WhereAmI	Executes the Unit identification function.	Not possible	Possible

Execute_WhereAmI (Service Code: 4B Hex)

Execute the Unit identification function. The request format is as follows.

● Request Format

Parameter name	Description	Data type	Value
Service	Service code	USINT	4B hex
Request Path Size	Size of request path	USINT	03
Request Path	Request path	Padded EPATH	210080032401 hex
Blink Duration	Unit identification function execution duration	UINT	0: Stops the Unit identification function. 5 to 1,800: Executes the Unit identification function for the specified duration only. The unit is seconds. The Unit identification indicators light up or turn off repeatedly as shown below for the duration specified in Blink Duration. • The indicators light up for a period of 100 ms each in a clockwise direction, and this is repeated four times. • The indicators all turn off for 500 ms.

A-4-4 Event History Log Object (Class ID: 34B Hex)

The Event History Log object is used to manage the event logs.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	34B	
Instance ID	01 to 02	Specifies the instance. 01: System event log (common for all MPU) 02: Access event log (common for all MPU)

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum instance number	Reading	UINT	0005
3	Number of Instance	Number of instances	Reading	UINT	0005

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Max Number of Record	Number of records that can be registered	Reading	UINT	The number differs as follows depending on the value of the instance ID. 01 hex: 100 records 02 hex: 100 records
2	Number of Record	Number of registered records	Reading	UINT	0 to Max Number of Record
3	Undate Counter	Counter	Reading	UINT	1 to 65,535
4	Size of Record	Byte size of record to read	Reading	UINT	40

Service Codes

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
01	Get_Attribute_All	Reads the values of all attributes.	Possible	Possible

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
34	Get Event Log	Reads the contents of the specified event log.	Not possible	Possible

Get_Event_Log (Service Code: 34 Hex)

Reads the contents of the specified event log. The request format and response format are as follows.

● Request Format

Parameter name	Description	Data type	Value
Service	Service code	USINT	34 hex
Request Path Size	Size of request path	USINT	03
Request Path	Request path	Padded EPATH	21004B032401 to 21004B032402 hex
Start Number of Read	Record number to start reading First number is 0.	UINT	
Number of Read	Number of records to read*1	UINT	
Update Counter	Value of attribute ID 3 *Update Counter* for instance read in advance*2 0: Record update detection disabled Other than 0: Record update detection enabled	UINT	

***1.** If the specified number of records does not exist, the number of records actually read is stored in *Actual Number of Read* of the response.

***2.** If the value differs from that of the current *Update Counter*, *Object state conflict* (0C hex) is returned.

● Response Format

Parameter name	Description	Data type	Value
Reply Service	Reply to Get Event Log service	USINT	B4 hex
Reserved	Reserved	octet	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00
Start Number of Read	Number of first record actually read	UINT	
Actual Number of Read	Number of records actually read	UINT	
Update Counter	Counter	UINT	
Number of Record	Number of registered records	UINT	
Record	Event log record	ARRAY OF STRUCT OF*1	

Parameter name	Description	Data type	Value
Index	Index of record*2	UDINT	0 to 4,294,967,295 The value is incremented for each record, and returned to 0 once the maximum value is reached.
Time	Time when event occurred	DATE_AND_TIME	
Product Code	Product code	DWORD	
Event Code	Event code*3	DWORD	
Event Priority	Event levels	WORD	3: Minor fault 4: Observation 5: Information
Additional Info Data Type1	Data type of additional information 1 of event	BYTE	
Additional Info Data Type2	Data type of additional information 2 of event	BYTE	
Additional Info Data Type3	Data type of additional information 3 of event	BYTE	
Additional Info Data Type4	Data type of additional information 4 of event	BYTE	
Additional Info1	Additional information 1 of event*3	Data type specified in Additional Info Data Type1 (4 octets)	
Additional Info2	Additional information 2 of event*3	Data type specified in Additional Info Data Type2 (4 octets)	
Additional Info3	Additional information 3 of event*3	Data type specified in Additional Info Data Type3 (4 octets)	
Additional Info4	Additional information 4 of event*3	Data type specified in Additional Info Data Type4 (4 octets)	

***1.** The size of the structure is 40 bytes.

***2.** Numbers are assigned through the instance ID = 01 hex (system event log) and instance ID = 02 hex (access event log).

***3.** Refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details on the description.

A-4-5 Error Event Object (Class ID: 34C Hex)

The Error Event object is used to manage the currently occurring error events.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	34C	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum instance number	Reading	UINT	0001
3	Number of Instance	Number of instances	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Max Number of Record	Number of records that can be registered	Reading	UINT	
2	Number of Record	Number of registered records	Reading	UINT	0 to Max Number of Record
3	Undate Counter	Counter	Reading	UINT	1 to 65,535
4	Size of Record	Byte size of record to read	Reading	UINT	34

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
01	Get_Attribute_All	Reads the values of all attributes.	Possible	Possible
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
34	Get Error Event	Gets the currently occurring error events.	Not possible	Possible

Get_Error_Event (Service Code: 34 Hex)

Gets the currently occurring error events. The request format and response format are as follows.

● Request Format

Parameter name	Description	Data type	Value
Service	Service code	USINT	34 hex
Request Path Size	Size of request path	USINT	03
Request Path	Request path	Padded EPATH	21004C032401 hex
Start Number of Read	Record number to start reading First number is 0.	UINT	
Number of Read	Number of records to read*1	UINT	
Update Counter	Value of attribute ID 3 *Update Counter* for instance read in advance*2 0: Record update detection disabled Other than 0: Record update detection enabled	UINT	

***1.** If the specified number of records does not exist, the number of records actually read is stored in *Actual Number of Read* of the response.

***2.** If the value differs from that of the current *Update Counter*, *Object state conflict* (0C hex) is returned.

● Response Format

Parameter name	Description	Data type	Value
Reply Service	Reply to Get Error Event service	USINT	B4 hex
Reserved	Reserved	octet	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00
Start Number of Read	Number of first record actually read	UINT	
Actual Number of Read	Number of records actually read	UINT	
Update Counter	Counter	UINT	
Number of Record	Number of registered records	UINT	
Record	Event record of error	ARRAY OF STRUCT OF*1	

Parameter name	Description	Data type	Value
Index	Index of record*2	UDINT	0 to 4,294,967,295 The value is incremented for each record, and returned to 0 once the maximum value is reached.
Product Code	Product code	DWORD	
Event Code	Event code*3	DWORD	
Event Priority	Event levels	WORD	3: Minor fault
Additional Info Data Type1	Data type of additional information 1 of event	BYTE	
Additional Info Data Type2	Data type of additional information 2 of event	BYTE	
Additional Info Data Type3	Data type of additional information 3 of event	BYTE	
Additional Info Data Type4	Data type of additional information 4 of event	BYTE	
Additional Info1	Additional information 1 of event*3	Data type specified in Additional Info Data Type1 (4 octets)	
Additional Info2	Additional information 2 of event*3	Data type specified in Additional Info Data Type2 (4 octets)	
Additional Info3	Additional information 3 of event*3	Data type specified in Additional Info Data Type3 (4 octets)	
Additional Info4	Additional information 4 of event*3	Data type specified in Additional Info Data Type4 (4 octets)	

***1.** The size of the structure is 34 bytes.

***2.** This object targets currently occurring error events. Since *Index* is assigned at the point in time when an error event occurs, the values will become discontinuous if there are error events that have recovered later.

***3.** Refer to *11-2-4 Event Details and Troubleshooting* on page 11-12 for details on the description.

A-4-6 Safety Discrete Input Point (SDIP) Object (Class ID: 3D Hex)

The Safety Discrete Input Point (SDIP) object is used to manage the safety input terminals individually, one terminal at a time.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	3D	
Instance ID	00	Specifies the class itself.
	01-0C	Specifies the instance of each safety input terminal. 01: Safety input terminal Si00 02: Safety input terminal Si01 03: Safety input terminal Si02 04: Safety input terminal Si03 05: Safety input terminal Si04 06: Safety input terminal Si05 07: Safety input terminal Si06 08: Safety input terminal Si07 09: Safety input terminal Si08 0A: Safety input terminal Si09 0B: Safety input terminal Si10 0C: Safety input terminal Si11

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum instance number	Reading	UINT	000C
3	Number of Instance	Number of instances	Reading	UINT	000C
8	Latch Input Error Time	Latch time for the Alarm state of the Safety Status in the Instance Attribute	Reading *1	UINT	0 to 65,530 The default value is 1000 (DEC). The unit is ms. Settable in 10 ms steps.

***1.** This can be written when the configuration is unlocked.

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
102	Maintenance Counter	Current value of Maintenance Counter	Reading/ Writing	UDINT	Current value of Maintenance Counter This indicates the contact operation count of the safety input terminal (unit: times). To clear the value, write 0.

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible

A-4-7 Safety Discrete Output Point (SDOP) Object (Class ID: 3B Hex)

The Safety Discrete Output Point (SDOP) object is used to manage the safety output terminals individually, one terminal at a time.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	3B	
Instance ID	00	Specifies the class itself.
	01 to 04	Specifies the instance of each safety output terminal.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum instance number	Reading	UINT	0004
3	Number of Instance	Number of instances	Reading	UINT	0004
8	Latch Output Error Time	Latch time of the alarm status for Safety Status of the instance attribute	Reading	UINT	0 to 65,530 The default value is 1000 (DEC). The unit is ms. Settable in 10 ms steps.

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
102	Maintenance Counter	Current value of Maintenance Counter	Reading/ Writing	UDINT	Current value of Maintenance Counter This indicates the contact operation count of the safety output terminal (unit: times). To clear the value, write 0.

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible

A-4-8 Device Level Ring (DLR) Object (Class ID: 47 Hex)

The Device Level Ring (DLR) object indicates the status of the DLR network.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	47	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0003
2	Max Instance	Maximum instance number	Reading	UINT	0001
3	Number of Instance	Number of instances	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Network Topology	Mode of current network topology	Read	USINT	0: Linear 1: Ring If a ring supervisor is present on the network, this always indicates 1: Ring. If a ring supervisor is not present on the network or the set ring parameters are not supported by the running ring supervisor, this becomes 0: Linear, and subsequently transitions between Ring and Linear depending on the status of the network.
2	Network Status	Current state of network as seen from the device	Read	USINT	Refer to *Values of Network Status* on page A-38 below.
3-9	Reserved 41 octets				

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
10	Active Supervisor Address	IP address and MAC address of the active ring supervisor	Read	STRUCT	
	Supervisor IP Address	IP address of the active ring supervisor		UDINT	IP address of the active ring supervisor of the device*1
	Supervisor MAC Address	MAC address of the active ring supervisor		ARRAY OF 6 USINTs	MAC address of the active ring supervisor of the device*1
12	Capability Flags	Function on DLR retained by device	Read	DWORD	Fixed to 00000082 hex This means that the ring function is beacon frame-based and supports Flush_Table frames.

***1.** The default value is All0. When the active ring supervisor is determined, the value is updated to its value.

● Values of Network Status

Value	Name	Description
0	Normal	Normal status
1	Ring Fault	A ring fault was detected. This is valid only when the network topology is ring.
2	Unexpected Loop Detected	A loop was detected on the network. This is valid only when the network topology is linear.

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
01	Get_Attribute_All	Reads the values of all attributes.	Not possible	Possible
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible

A-4-9 QoS Object (Class ID: 48 Hex)

The QoS object sets the value of the IPv4 DiffServ Code Point (DSCP) under Ethernet frame priority control.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	48	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum instance number	Reading	UINT	0001
3	Number of Instance	Number of instances	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
4	DSCP Urgent	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Urgent.	Reading/ writing*1	USINT	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Urgent. The default value is 55 (‘110111’).
5	DSCP Scheduled	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Scheduled.	Reading/ writing*1	USINT	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Scheduled. The default value is 47 (‘101111’).
6	DSCP High	DSCP value when the priority of CIP Transport Class 0/1 messages is set to High.	Reading/ writing*1	USINT	DSCP value when the priority of CIP Transport Class 0/1 messages is set to High. The default value is 43 (‘101011’).
7	DSCP Low	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Low.	Reading/ writing*1	USINT	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Low. The default value is 31 (‘011111’).

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
8	DSCP Explicit	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Explicit.	Reading/ writing*1	USINT	DSCP value when the priority of CIP Transport Class 0/1 messages is set to Explicit. The default value is 27 (‘011011’).

***1.** The setting is enabled after restarting.

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible

A-4-10 TCP/IP Interface Object (Class ID: F5 Hex)

The TCP/IP Interface object is used to configure the TCP/IP interface settings.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	F5	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Supported revisions of TCP/IP Interface object	Reading	UINT	0004
2	Max Instance	Maximum instance number	Reading	UINT	0001
3	Number of Instance	Number of instances	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Status	Status of TCP/IP interface	Reading	DWORD	Refer to *Values of Status* on page A-43 below.
2	Configuration Capability	Bitmap of various functions supported by the TCP/IP interface	Reading	DWORD	Refer to *Values of Configuration Capability* on page A-43 below.
3	Configuration Control	Configuration determination method for the TCP/IP interface	Reading/ writing	DWORD	Refer to *Values of Configuration Control* on page A-44 below.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
4	Physical Link Object	Path to physical layer link object	Reading	STRUCT	
	Path size	Path size in words		UINT	0000
	Path	Fixed path to physical layer link object		Padded EPATH	All0 hex
5	Interface Configuration*1	Interface settings	Reading/ writing	STRUCT	
	IP Address	IP address		UDINT	IP address The default value is 192.168.250.1. The following values cannot be set. • IP addresses with a host ID that is all 0's or all 1's • IP addresses that start with 0, 127, or 255 • Class-D IP addresses (224.0.0.0 to 239.255.255.255) • Class-E IP addresses (240.0.0.0 to 255.255.255.255) • Link local addresses (169.254.0.0 to 169.254.255.255)
	Network Mask	Network mask		UDINT	Network mask The default value is 255.255.255.0. The enable conditions are as follows. • Bits must be contiguous from the beginning. • This must be within the range of 192.0.0.0 to 255.255.255.252.
	Gateway Address	Default gateway		UDINT	Gateway address The default value is 0.0.0.0 (indicates that there is no gateway). The following values cannot be set. • Value that does not satisfy the setting conditions of *IP Address*. • IP address of a segment that is different from the network address specified in *IP Address*.
	Name Server	Primary name server of DNS server		UDINT	Always 0.0.0.0.
	Name Server 2	Secondary name server of DNS server		UDINT	Always 0.0.0.0.
	Domain Name	Domain name		STRING	Domain name The default value is "" (NULL).

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
6	Host Name	Host name	Reading/ writing	STRING	Set the host name of the device with 64 ASCII characters or less. If there are less than 64 characters, padding will be used for the remaining number of characters.
7	Safety Network Number	Safety Network Number (SNN)	Reading	6 octets	Safety Network Number
13	Encapsulation Inactivity Timeout	Encapsulation inactivity timeout time	Reading/ writing	UINT	0 to 3,600 If there are no communications via EtherNet/IP during the time set for Encapsulation Inactivity Timeout, the TCP connection is closed. If Encapsulation Inactivity Timeout = 0, the TCP connection is not closed. The unit is seconds. The default value is 120.

***1.** If the IP address setting method is direct setting by rotary switch, writing to this attribute cannot be executed.

● Values of Status

Bit	Name	Description
0 to 3	Interface Configuration Status	Configuration status of the instance attribute ID 05 hex (Interface Configuration) 0: Not set or initializing 1: IP address already set by a method other than directly setting the IP address with hardware switches 2: IP address already set by directly setting with hardware switches 3 to 15: Reserved
4	Reserved	Always FALSE
5	Interface Configuration Pending	TRUE: The setting of the instance attribute ID 05 hex (Interface Configuration) was changed. The Safety I/O Block must be restarted to enable the change. FALSE: The setting of the instance attribute ID 05 hex (Interface Configuration) was not changed.
6	AcdStatus	TRUE: An IP address duplication was detected. However, this IP address can be used to continue CIP communications. FALSE: No IP address duplication was detected.
7	AcdFault	TRUE: This IP address cannot be used to continue CIP communications. FALSE: No IP address duplication was detected. Or, although an IP address duplication was detected, this IP address can be used to continue CIP communications.
8 to 31	Reserved	Always FALSE

● Values of Configuration Capability

Bit	Name	Description
0	BOOTP Client	Always FALSE BOOTP client function cannot be used
1	DNS Client	Always FALSE DNS client function cannot be used

Bit	Name	Description
2	DHCP Client	Always TRUE DHCP client function can be used
3	DHCP-DNS Update	Always FALSE DHCP-DNS Update function cannot be used
4	Configuration Settable	Always TRUE Interface configuration attribute can be set
5	Hardware Configuration	Always TRUE IP address can be set from hardware
6	Interface Configuration Change Requires Reset	Always TRUE The device must be restarted to enable a change of this attribute.
7	AcdCapable	Always FALSE IP address duplication detection function cannot be used
8 to 31	Reserved	Always FALSE

● Values of Configuration Control

Bit	Name	Description
0 to 3	Configuration Method	Setting method for IP address of Safety I/O Block 0: Uses the setting that is saved in non-volatile memory (default value). 1: Sets the IP address by the BOOTP server. 2: Sets the IP address by the DHCP server. 3 to 15: Reserved
4	DNS Enable	Always FALSE DNS client function cannot be used
5 to 31	Reserved	Always FALSE

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible

A-4-11 Ethernet Link Object (Class ID: F6 Hex)

The Ethernet Link object is used to obtain various information of an Ethernet link.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	F6	
Instance ID	00	Specifies the class itself.
	01 to 02	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Supported revisions of Ethernet Link object	Reading	UINT	0004
2	Max Instance	Maximum instance number	Reading	UINT	0002
3	Number of Instance	Number of instances	Reading	UINT	0002

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Interface Speed	Interface communications speed	Reading	UDINT	000A hex: 10 Mbps 0064 hex: 100 Mbps
2	Interface Flags	Interface status	Reading	DWORD	Refer to *Values of Interface Flags* on page A-49 below.
3	Physical Address	Interface MAC address	Reading	ARRAY OF USINT*1	Interface MAC address

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
4	Interface Counters	Interface communications statistical information	Reading	STRUCT	
	In Octets	Number of bytes of receive data		UDINT	Number of bytes of receive data
	In Ucast Packets	Number of received unicast packets		UDINT	Number of received unicast packets
	In NUcast Packets	Number of received non-unicast packets		UDINT	Number of received non-unicast packets
	In Discards	Number of discarded received packets		UDINT	Number of discarded received packets
	In Errors	Number of received error packets		UDINT	Number of received error packets However, this excludes those of *In Discards*.
	In Unknown Protos	Number of received unsupported protocol packets		UDINT	Number of received unsupported protocol packets
	Out Octets	Number of bytes of send data		UDINT	Number of bytes of send data
	Out Ucast Packets	Number of sent unicast packets		UDINT	Number of sent unicast packets
	Out NUcast Packets	Number of sent non-unicast packets		UDINT	Number of sent non-unicast packets
	Out Discards	Number of discarded sent packets		UDINT	Number of discarded sent packets
	Out Errors	Number of sent error packets		UDINT	Number of sent error packets

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
5	Media Counters	Interface media statistical information	Reading	STRUCT	
	Alignment Errors	Number of received alignment error frames		UDINT	Number of received alignment error frames
	FCS Errors	Number of times FCS error received		UDINT	Number of times FCS error received
	Single Collisions	Number of successfully sent frames with a collision detected		UDINT	Number of successfully sent frames with a collision detected
	Multiple Collisions	Number of successfully sent frames with more than one collision detected		UDINT	Number of successfully sent frames with more than one collision detected
	SQE Test Errors	Number of SQE test error occurrences		UDINT	Number of SQE test error occurrences
	Deferred Transmissions	Number of frames with a send delay		UDINT	Number of frames with a send delay
	Late Collisions	Number of times collisions detected in 512 bit time after packet transmission		UDINT	Number of times collisions detected in 512 bit time after packet transmission
	Excessive Collisions	Number of unsuccessfully sent frames due to excessive collisions		UDINT	Number of unsuccessfully sent frames due to excessive collisions
	MAC Transmit Errors	Number of unsuccessfully sent frames due to a MAC layer transmission error		UDINT	Number of unsuccessfully sent frames due to a MAC layer transmission error
	Carrier Sense Errors	Number of times carrier sensor error detected		UDINT	Number of times carrier sensor error detected
	Frame Too Long	Number of frames that exceeded the maximum frame size		UDINT	Number of frames that exceeded the maximum frame size
	MAC Receive Errors	Number of unsuccessfully received frames due to a MAC layer reception error		UDINT	Number of unsuccessfully received frames due to a MAC layer reception error
6	Interface Control	Interface configuration	Reading/ writing*2	STRUCT	
	Control Bits	Method to determine communications speed		WORD	Refer to *Values of Control Bits* on page A-49 below. The default value is 0001 hex.
	Forced Interface Speed	Communications speed when Auto-Negotiation is disabled		UINT	0064 hex: 100 Mbps The default value is 0000 hex. *3*4
7	Interface Type	Type of physical interface for this instance	Reading	USINT	Fixed to 02 hex: Twisted pair

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
8	Interface State	Interface state	Reading	USINT	00 hex: Status unclear 01 hex: Ready to send/ receive 02 hex: Disabled 03 hex: Testing 04 to FF hex: Reserved
10	Interface Label	Interface identification text string	Reading	SHORT STRING	Instance 1: Fixed to "Ethernet Port 1" Instance 2: Fixed to "Ethernet Port 2"
11	Interface Capability	Interface communications performance	Reading	STRUCT	-
	Capability Bits	Communications performance setting		DWORD	Refer to *Values of Capability Bits* on page A-49 below.
	Speed/Duplex Options	Combinations of communication speed and duplex mode allowed by the interface		STRUCT	
	Speed/Duplex Array Count	Communications speed/ bidirectional array size		USINT	Always 2
	Speed/Duplex Array	Communications speed/ bidirectional array		ARRAY OF STRUCT	
	Interface Speed	Interface communications speed		UINT	0064 hex: 100 Mbps
	Interface Duplex Mode	Interface bidirectional mode		USINT	00 hex: Half Duplex
	Speed/Duplex Array	Communications speed/ bidirectional array		ARRAY OF STRUCT	
	Interface Speed	Interface communications speed		UINT	0064 hex: 100 Mbps
	Interface Duplex Mode	Interface bidirectional mode		USINT	01 hex: Full Duplex
14	Ethernet Errors	Total value of interface counters, media counters, and HC media counters	Reading	UDINT	Total value of interface counters, media counters, and HC media counters The default value is 0.
15	Link Down Counter	Number of times the Ethernet port transitioned from the link up state to link down state	Reading	UDINT	Number of times the Ethernet port transitioned from the link up state to link down state The default value is 0.
100	Communication Cable Diagnosis	Communications cable diagnosis result	Reading	UINT	Refer to *Values of Communication Cable Diagnosis* on page A-50 below.

***1.** The array size is 6.

***2.** The setting is enabled after restarting.

***3.** In the following cases, the 09 hex (Invalid Attribute Value) error occurs.
- When any of bits 2 to 15 (reserved bits) of *Control Bits* is TRUE.
- When bit 0 (Auto-negotiate) is FALSE and bit 1 (Forced Duplex Mode) is TRUE of *Control Bits*, and an attempt is made to set a value outside the setting range for *Forced Interface Speed*.

***4.** In the following case, the 0C hex (Object State Conflict) error occurs.
- When bit 0 (Auto-negotiate) is TRUE and bit 1 (Forced Duplex Mode) is FALSE of *Control Bits*, and an attempt is made to set some value for *Forced Interface Speed*.

● Values of Interface Flags

Bit	Name	Description
0	Link Status	TRUE: An Ethernet link is established. FALSE: No Ethernet link is established.
1	Half/Full Duplex***1**	TRUE: Full Duplex FALSE: Half Duplex
2 to 4	Negotiation Status	0: Auto-negotiation execution is in progress. 1: Auto-negotiation failed. Operates in half duplex at communications speed of 10 Mbps. 2: Auto-negotiation failed. Operates in half duplex at set communications speed. 3: Auto-negotiation was successful. 4: Auto-negotiation disabled.
5	Manual Setting Requires Reset	TRUE: A device reset is required after the Interface Control Attribute is changed. FALSE: A device reset is not required after the Interface Control Attribute is changed.
6	Local Hardware Fault	TRUE: Hardware fault FALSE: No hardware fault
7 to 31	Reserved	Always FALSE

***1.** When Link Status = 0, it has no meaning.

● Values of Control Bits

Bit	Name	Description
0	Auto-negotiate	TRUE: Auto-negotiate is enabled. FALSE: Auto-negotiate is disabled. Operating according to the Forced Duplex Mode and Forced Interface Speed settings.
1	Forced Duplex Mode	TRUE: Full Duplex FALSE: Half Duplex This bit is used when Auto-negotiate is FALSE. If this bit is set when Auto-negotiate is TRUE, the error code 0C hex (Object State Conflict) is returned.
2-15	Reserved	Always FALSE

● Values of Capability Bits

Bit	Name	Description
0	Manual Setting Requires Reset	Always TRUE: Indicates that a device reset is required after the Interface Control Attribute is changed.
1	Auto-negotiate	Always TRUE: Auto-negotiation is supported.
2	Auto-MDIX	Always TRUE: Auto-MDIX is supported.
3	Manual Speed/Duplex	Always TRUE: Manual speed/duplex setting is supported.
4 to 31	Reserved	Always FALSE

● Values of Communication Cable Diagnosis

Bit	Description
0 to 7	Error occurrence location from the port Unit: m For diagnostic result error, 0
8 to 15	00 hex: Not executed 01 hex: Normal 02 hex: Short-circuit 03 hex: Break 04 hex: Port disabled F1 hex: Diagnosis in progress F2 hex: Diagnostic result error F3 hex: PHY read error

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible
3A	Exec_Cable_Diagnosis	Executes communications cable diagnosis.*1	Not possible	Possible
4C	Get_and_Clear	Reads and then clears a specified attribute value.*2*3	Not possible	Possible

***1.** If this service is executed in an instance for a communications port where a link is already established, communications cable diagnosis is not executed, and there will always be no failure. Furthermore, if this service is executed in an instance for a communications port with communications cable diagnosis currently in progress, the 0C hex (Object State Conflict) error occurs.

***2.** This service is supported by the following instance attributes.

- Interface Counters (04)
- Media Counters (05)
- Link_Down Counter (15)

When other than an attribute above is specified, 09 hex (invalid attribute value) is returned as the response code.

***3.** In the following combinations, when this service is executed for one of them, the value is read for one of them only, and both of them are reset.

- Interface Counters (04 hex) and HC Interface Counters (12 hex)
- Media Counters (05 hex) and HC Media Counters (13 hex)

A-4-12 LLDP Management Object (Class ID: 109 Hex)

The LLDP Management object is used to manage the LLDP function.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	109	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum instance number	Reading	UINT	0001
3	Number of Instance	Number of instances	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	LLDP Enable	LLDP enable	Reading/ writing	STRUCT	
	LLDP Enable Array length	Number of ports to set in LLDP Enable Array		UINT	This becomes the EthernetLink Object instance + 1 because it also includes the settings of the entire LLDP function. Always 3
	LLDP Enable Array	LLDP enable/disable setting of entire LLDP function or each port		ARRAY OF BYTE	Refer to *Values of LLDP Enable Array* on page A-52 below.
2	msgTxInterval	Send interval of LLDP frames	Reading/ writing	UINT	Send interval of LLDP frames 1 to 3,600 The unit is seconds. The default value is 30.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
3	msgTxHold	Multiplier for determining LLDP frame TTL value	Reading/ writing	USINT	1 to 100 The TTL value is obtained by msgTxInterval × msgTxHold. The default value is 4. Therefore, the default value of the TTL value is 30 × 4 = 120 seconds. If the result of msgTxInterval × msgTxHold exceeds 65,535, the TTL value is 65,535 seconds.
4	LLDP Datastore	Method to obtain LLDP database	Reading	WORD	Fixed to 1: Obtain by SNMP
5	Last Change	Value of sysUpTime obtained when an entry in the local LLDP database was last changed	Reading	UDINT	Value of sysUpTime obtained when an entry in the local LLDP database was last changed sysUpTime represents the time since the network management portion of the system was last initialized. The unit is 0.01 seconds.

● Values of LLDP Enable Array

Bit	Name	Description
0	Global Enable	TRUE: LLDP sending and receiving are enabled (default value). FALSE: LLDP sending and receiving are disabled. If the value is changed from TRUE to FALSE, all existing table entries are deleted.
1	Port 1 Enable	TRUE: LLDP sending from port 1 is enabled (default value). FALSE: LLDP sending from port 1 is disabled.
2	Port 2 Enable	TRUE: LLDP sending from port 2 is enabled (default value). FALSE: LLDP sending from port 2 is disabled.
3 to 7	Reserved	Always FALSE

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible

A-4-13 LLDP Data Table Object (Class ID: 10A Hex)

The LLDP Data Table object is used to manage the data of the LLDP function.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	10A	
Instance ID	00	Specifies the class itself.
	01-30	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001
2	Max Instance	Maximum value of instance IDs presently generated	Reading	UINT	0000-0030
3	Number of Instance	Number of instances presently generated	Reading	UINT	0000-0030

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
1	Ethernet Link Instance Number	Instance number of Ethernet Link object (F6 hex) that links with the Ethernet port that received the LLDP frame	Reading	UINT	Instance number of Ethernet Link object (F6 hex) that links with the Ethernet port that received the LLDP frame If unknown, it is 0.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
2	MAC Address	MAC address of the adjacent device that transmitted the received LLDP frame	Reading	ETH_MAC_ADDR	The stored value is determined in the following priority order. Priority 1: When TLV Type = 127 and Subtype = 2, CIP MAC address Priority 2: When TLV Type = 1 and Subtype = 4, Chassis ID Priority 3: When TLV Type = 2 and Subtype = 3, Port ID Priority 4: All 0
3	Interface Label	Interface label of the adjacent device that transmitted the received LLDP frame	Reading	SHORT STRING	The stored value is determined in the following priority order. Priority 1: When TLV Type = 127 and Subtype = 3, CIP Interface Label Priority 2: When TLV Type = 1 and Subtype = 6, Chassis ID Priority 3: When TLV Type = 2 and Subtype = 5, Port ID Priority 4: Null
4	Time to Live	Time that information of adjacent device is enabled.	Reading	UINT	Time that information of adjacent device is enabled. The unit is seconds. When Time to Live = 0, it means that this instance needs to be deleted.
5	System Capabilities TLV	Functions supported by adjacent device	Reading	STRUCT	
	System Capabilities	Functions that can be supported by adjacent device		WORD	Refer to *Values of System Capabilities and Enabled Capabilities* on page A-56 below.
	Enabled Capabilities	Functions currently enabled on adjacent device		WORD	Refer to *Values of System Capabilities and Enabled Capabilities* on page A-56 below.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
6	IPv4 Management Addresses	Management address of the adjacent device	Reading	STRUCT	
	Management Address Count	Number of management addresses to store		USINT	Number of management addresses to store 255 max.
	Management Address	Value of management address		ARRAY OF UDINT	Value of management address Enabled when Class A, B, or C. This value is not stored when all 0 or loopback address.
7	CIP Identification	CIP Identity of adjacent device	Reading	STRUCT	
	Vendor ID	Vendor ID		UINT	Vendor ID If the TLV corresponding to the received LLDP frame is not included, the value is 0.
	Device Type	Device type		UINT	Device type If the TLV corresponding to the received LLDP frame is not included, the value is 0.
	Product Code	Product code		UINT	Product code If the TLV corresponding to the received LLDP frame is not included, the value is 0.
	Major Revision	Major revision		BYTE	Major revision If the TLV corresponding to the received LLDP frame is not included, the value is 0.
	Minor Revision	Minor revision		USINT	Minor revision If the TLV corresponding to the received LLDP frame is not included, the value is 0.
	CIP Serial Number	CIP serial number		UDINT	CIP serial number If the TLV corresponding to the received LLDP frame is not included, the value is 0.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
8	Additional Ethernet Capabilities	Ethernet Preemption function status	Reading	STRUCT	
	Preemption Support	Support status of Preemption (TSN function) of adjacent node		BOOL	TRUE: Supported FALSE: Not supported
	Preemption Status	Enable/disable of Preemption (TSN function) of adjacent node		BOOL	TRUE: Enabled FALSE: Disabled
	Preemption Active	Whether Preemption (TSN function) of adjacent node is active		BOOL	TRUE: Active FALSE: Inactive
	Additional Fragment Size	Number of octets that must be sent in a frame before Preemption (TSN function) of the adjacent node occurs		USINT	0: 64 octets 1: 128 octets 2: 192 octets 3: 256 octets 4 to 255: Reserved
9	Last Change	Value of sysUpTime obtained when this instance was last changed	Reading	UDINT	Value of sysUpTime obtained when this instance was last changed sysUpTime represents the time since the network management portion of the system was last initialized. The unit is 0.01 seconds.

● Values of System Capabilities and Enabled Capabilities

Bit	Description
0	Other
1	Repeater
2	Bridge
3	Access Point
4	Router
5	Telephone
6	DOCSIS Cable Device
7	End Station
8	C-VLAN component
9	S-VLAN component
10	Two-port MAC Relay Component
11 to 15	Reserved

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
11	Find_Next_Object_Instance	This searches for the next object.	Possible	Possible

Find_Next_Object_Instance (Service Code: 11 Hex)

This searches for the next object. The request format and response format are as follows.

● Request Format

Parameter name	Description	Data type	Value
Service	Service code	USINT	11 hex
Maximum Returned Values	Maximum number of instance ID members in Instance ID List	USINT	

● Response Format

Parameter name	Description	Data type	Value
Reply Service	Reply to Find_Next_Object_Instance service	USINT	91 hex
Number Of List Members	Number of members	USINT	
Instance ID List	Instance ID list	ARRAY OF UINT	

A-4-14 Logic Process Object (Class ID: 309 Hex)

The Logic Process object is used to read the number of the application that is operating.

Class ID and Instance ID

The class ID and instance ID are given in the following table.

ID type	Value (hex)	Description
Class ID	309	
Instance ID	00	Specifies the class itself.
	01	Specifies the instance.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value (hex)
1	Revision	Revision of the object	Reading	UINT	0001

● Instance Attribute ID

The instance attribute ID specifies the attribute ID of the instance.

Attribute ID	Parameter name	Description	Attribute	Data	
				Data type	Value
101	Application Number	Application number	Reading	USINT	Refer to *Values of Application Number* on page A-58 below.

● Values of Application Number

Value	Description
0	Remote I/O mode application
1	Fixed application 1 Partial stop + entire stop application
2	Fixed application 2 Partial stop + entire stop application (with EDM)
3	Fixed application 3 Worker and robot automatic switching application
4 to 7	Reserved
8	Reserved
9 to 13	Add-on application 1 to 5
14	Reserved
15	User-defined application

If the value of a rotary switch is invalid or reading fails, the value when locked is returned if in the locked state. FF hex is returned if in the unlocked state.

Service Code

The service code specifies the service to execute.

Service code (hex)	Parameter name	Description	Supported service range	
			Class	Instance
0E	Get_Attribute_Single	Reads the value of the specified attribute.	Possible	Possible
10	Set_Attribute_Single	Writes the value of a specified attribute.	Not possible	Possible

A-5 Declaration of Conformity

No. EUSP0001B

Original

OMRON

EU DECLARATION OF CONFORMITY

1. **Product Models/Products:**
   NXR-S series
2. **Name and address of the manufacturer:**
   OMRON Corporation
   Shiokoji Horikawa, Shimogyo-Ku, Kyoto, 600-8530 Japan
3. **This declaration of conformity is issued under the sole responsibility of the manufacturer.**
4. **Objects of the declaration:**
   NXR-S series, Simple Logic Safety I/O Block
5. **The objects of the declaration described above are in conformity with the relevant Union harmonisation legislation:**
   2014/30/EU EMC Directive
   2006/42/EC Machinery Directive (Valid until 19.01.2027)
   (EU) 2023/1230 Machinery Regulation (Valid from 20.01.2027)
   2011/65/EU RoHS Directive
6. **References to the relevant harmonised standards used or references to the other technical specifications in relation to which conformity is declared:**
   EMC Directive: EN 61131-2: 2007
   Machinery Directive / Machinery Regulation: EN ISO 13849-1:2023 / EN 61508 Parts 1-3:2010
   RoHS Directive: EN IEC 63000: 2018
   prEN 50742:2025 as technical specifications
7. **Name, address, and identification number of Notified Body, Number of EC Type Examination**
   Notified body: TÜV Rheinland Industrie Service GmbH
   Address: Am Grauen Stein, 51105 Köln / Germany
   Notified Body identification No.: 0035
   Certificate for EC Type Examination: 01/205/6092.00/26

Signed and on behalf of: OMRON Corporation
Place and date of issue: Kyoto, Japan 18th Sep, 2026
Signature: 署名者: 78685B1FEB29487...
Name: Kazuo Kondo
Function: Senior General Manager, Controller Division, Industrial Automation Company

1/3
GQ-151845A1

No. EUSP0001B

Name and address of contact in EU

OMRON Europe B.V.
Quality & Environment Department
Attn: J.J.P.W. Vogelaar, European Quality & Environment Manager
Zilverenberg 2, 5234 GM, 's-Hertogenbosch, The Netherlands

2/3
GQ-151845A1

No. EUSP0001B

Additional information

Models List

Model	Type	EMI	EMS	RoHS	Rev
		EN61131-2	EN61131-2	EN IEC 63000	
NXR-SXD1204-CST	Safety I/O Block	2007	2007 zone B	2018	<A>
NXR-SXD1204B-CST	Safety I/O Block	2007	2007 zone B	2018	<A>
NXR-SXD1204-EIT	Safety I/O Block	2007	2007 zone B	2018	<A>

Model name may be followed by additional letter (s) and /or number (s) for sale purposes.

3/3
GQ-151845A1

I

Index

Index

A

Automatic Clock Adjustment....7-91

B

Backup....7-108

C

Calculating the Total Current Consumption in Direct Power Supply....4-7
Calculating the total current consumption in power supply with through-wiring....4-14
Calculating the Voltage Drop in Direct Power Supply....4-11
Calculating the voltage drop in power supply with through-wiring....4-17
Change Initial Safety Password....7-24
Changing the Operating Mode....7-95
Clear All Memory Function....8-4
Communications cable connection procedure (screw connector)....5-8
Communications cable connection procedure (Smartclick connector)....5-7
Communications Cable Diagnosis Function....8-31
Communications cable removal procedure (screw connector)....5-10
Communications cable removal procedure (Smartclick connector)....5-7
communications connectors....3-11
Configuration Lock....7-99
Contact Operation Count Monitor Function....8-29
Cover mounting holes....3-3, 3-4
Cyclic communications....6-6

D

Device Level Ring (DLR) Function....8-10
direct power supply....4-3

E

EtherNet/IP communications connector 1....3-2, 3-4
EtherNet/IP communications connector 2....3-2, 3-4
Event....11-2
Event Log Function....11-6
EX PWR OUT Indicator....3-7
Expected Packet Interval (EPI)....7-33
Export....7-36

F

Firmware Update Function....8-35

H

HTTPS Communications Function....8-8

I

I/O cable connection procedure (screw connector)....5-21
I/O cable connection procedure (Smartclick connector)....5-19
I/O cable removal procedure (screw connector)....5-23
I/O cable removal procedure (Smartclick connector)....5-20
I/O connectors....3-2, 3-4
I/O identification marker....3-3, 3-4
I/O indicators....3-3, 3-4
I/O Monitor Function....8-27
I/O Wiring Checking Function....8-13
Implicit communications....6-6
Importing....7-37
Inspection Items....12-3
Installing the Rotary Switch Cover....5-3
Installing the Unit....5-3
IP Address Indication Function....8-19

L

L/A ETH1 Indicator....3-6
L/A ETH2 Indicator....3-7
Line....1-13
LLDP Function....7-42
Lock Indicator....3-7
Login....7-22
Logout....7-24
Lot number....32

M

M12 attachment....5-8, 5-21
M12 torque handle....5-8, 5-21
MAC address....32
MS Indicator....3-6

N

NS Indicator....3-6

O

Open Types....6-4
Operating Status Monitor Function....11-3
OUT PWR Indicator....3-5
Output power supply....4-2

P

Pin arrangement....3-11, 3-12
Port....3-12
Power OFF Function for Through-wiring Output....8-11
Power supply cable connection procedure....5-16
Power supply cable removal procedure....5-17
Power Supply Capacity....4-21
Power supply connector (input)....3-3, 3-4

Power Supply Connector (Input)..... 3-12
Power supply connector (output).....3-3, 3-4
Power Supply Connector (Output).....3-12
Power Supply Monitor Function.....8-22
Power supply used..... 4-21
Power supply with through-wiring.....4-3
Production Information Screen..... 33

R

Restart..... 7-84
Ring..... 1-14
Rotary switches..... 3-3, 3-4

S

Safety I/O Ports..... 3-13
Safety Input Indicator.....3-8
Safety Input Ports..... 3-12
Safety Output Indicator.....3-8
Safety Output Ports..... 3-13
Safety password..... 7-104
Safety reaction time.....9-2
Safety response performance..... 9-2
Send General CIP Command Function..... 8-15
Setting Procedure for Tag Data Link Communications.... 7-38
Star..... 1-13
Status indicators.....3-3, 3-4

T

Tag data links.....6-6
Tightening Tools..... 5-8, 5-12, 5-21
Tightening Torque.....5-11, 5-12, 5-24
Tools Required for Inspections..... 12-2
Total current consumption from output power supply..... 4-7
Total current consumption from Unit/input power supply... 4-7
Tree..... 1-13

U

U/IN PWR Indicator..... 3-5
Unit Identification Function..... 8-16
Unit identification indicator..... 3-3, 3-4
Unit identification marker.....3-3, 3-4
Unit mounting holes.....3-3, 3-4
Unit Replacement Using the Backup Function..... 12-4
Unit Replacement Without Using the Backup Function... 12-5
Unit/input power supply..... 4-2

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 INDUSTRIAL AUTOMATION (CHINA) CO., LTD.
19th Floor, Tower 2, Shanghai Landmark Center,
No. 88 North Sichuan Road,
Hongkou District, Shanghai, 200085, China
Tel: (86) 21-6023-0333

Authorized Distributor:

©OMRON Corporation 2026 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. W645-E1-04 1026