

Programmable Controller

MELSEC iQ-R
series

MELSEC iQ-R CIP Safety Module User's Manual

-RJ71SEIP91-T4

Powered by
molex

This product was jointly developed and manufactured by
Mitsubishi Electric and Molex.

*Note that the warranty on this product differs from that on other
programmable controller products.
(Refer to "WARRANTY" in this manual.)

COPYRIGHT

This document is protected by the law of copyright, whereby all rights established therein remain with the company Mitsubishi Electric Corporation. Reproduction of this document or parts of this document is only permissible within the limits of the legal determination of Copyright Law. Alteration or abridgement of the document is not permitted without the explicit written approval of the company Mitsubishi Electric Corporation.

PRECAUTIONS REGARDING WARRANTY AND SPECIFICATIONS

This product is jointly developed and manufactured with Molex. Thus, warranty information is different from that of other MELSEC products. Check the restrictions described below and purchase the product.

■ Gratis Warranty Term

Warranty period is one year after delivery. (Maximum of 18 months after produced)

■ Repair

Please note that this product cannot be repaired. Therefore, free replacement is arranged for the failure of our responsibility during the warranty period.



SAFETY PRECAUTIONS

(Read these precautions before using this product.)

Before using this product, please read this manual and the relevant manuals carefully and pay full attention to safety to handle the product correctly.

The precautions given in this manual are concerned with this product only. For the safety precautions of the programmable controller system, refer to the user's manual for the module used.

In this manual, the safety precautions are classified into two levels: "⚠ WARNING" and "⚠ CAUTION".

 WARNING	Indicates that incorrect handling may cause hazardous conditions, resulting in death or severe injury.
 CAUTION	Indicates that incorrect handling may cause hazardous conditions, resulting in minor or moderate injury or property damage.

Under some circumstances, failure to observe the precautions given under "⚠ CAUTION" may lead to serious consequences.

Observe the precautions of both levels because they are important for personal and system safety.

Make sure that the end users read this manual and then keep the manual in a safe place for future reference.

WARNING

- Configure safety circuits external to the programmable controller to ensure that the entire system operates safely even when a fault occurs in the external power supply or the programmable controller. Failure to do so may result in an accident due to an incorrect output or malfunction.
 - (1) Emergency stop circuits, protection circuits, and protective interlock circuits for conflicting operations (such as forward/reverse rotations or upper/lower limit positioning) must be configured external to the programmable controller.
 - (2) When the programmable controller detects an abnormal condition, it stops the operation and all outputs are:
 - Turned off if the overcurrent or overvoltage protection of the power supply module is activated.
 - Held or turned off according to the parameter setting if the self-diagnostic function of the CPU module detects an error such as a watchdog timer error.
 - (3) All outputs may be turned on if an error occurs in a part, such as an I/O control part, where the CPU module cannot detect any error. To ensure safety operation in such a case, provide a safety mechanism or a fail-safe circuit external to the programmable controller. For a fail-safe circuit example, refer to "General Safety Requirements" in the MELSEC iQ-R Module Configuration Manual.
 - (4) Outputs may remain on or off due to a failure of a component such as a relay and transistor in an output circuit. Configure an external circuit for monitoring output signals that could cause a serious accident.
 - In an output circuit, when a load current exceeding the rated current or an overcurrent caused by a load short-circuit flows for a long time, it may cause smoke and fire. To prevent this, configure an external safety circuit, such as a fuse.
 - Configure a circuit so that the programmable controller is turned on first and then the external power supply. If the external power supply is turned on first, an accident may occur due to an incorrect output or malfunction.
 - Configure a circuit so that the external power supply is turned off first and then the programmable controller. If the programmable controller is turned off first, an accident may occur due to an incorrect output or malfunction.
 - For the operating status of each station after a communication failure, refer to manuals for the network used. For the manuals, please consult your local Mitsubishi representative. Incorrect output or malfunction due to a communication failure may result in an accident.
 - When connecting an external device with a CPU module or intelligent function module to modify data of a running programmable controller, configure an interlock circuit in the program to ensure that the entire system will always operate safely. For other forms of control (such as program modification, parameter change, forced output, or operating status change) of a running programmable controller, read the relevant manuals carefully and ensure that the operation is safe before proceeding. Improper operation may damage machines or cause accidents. When a Safety CPU is used, data cannot be modified while the Safety CPU is in SAFETY MODE.
-

[Design Precautions]

WARNING

- Especially, when a remote programmable controller is controlled by an external device, immediate action cannot be taken if a problem occurs in the programmable controller due to a communication failure. To prevent this, configure an interlock circuit in the program, and determine corrective actions to be taken between the external device and CPU module in case of a communication failure.
 - Do not write any data to the "system area" and "write-protect area" of the buffer memory in the module. Also, do not use any "use prohibited" signals as an output signal from the CPU module to each module. Doing so may cause malfunction of the programmable controller system. For the "system area", "write-protect area", and the "use prohibited" signals, refer to the user's manual for the module used. For areas used for safety communications, they are protected from being written by users, and thus safety communications failure caused by data writing does not occur.
 - If a communication cable is disconnected, the network may be unstable, resulting in a communication failure of multiple stations. Configure an interlock circuit in the program to ensure that the entire system will always operate safely even if communications fail. Incorrect output or malfunction due to a communication failure may result in an accident. When safety communications are used, an interlock by the safety station interlock function protects the system from an incorrect output or malfunction.
-

[Design Precautions]

CAUTION

- Do not install the control lines or communication cables together with the main circuit lines or power cables. Doing so may result in malfunction due to electromagnetic interference. Keep a distance of 100mm or more between those cables.
 - During control of an inductive load such as a lamp, heater, or solenoid valve, a large current (approximately ten times greater than normal) may flow when the output is turned from off to on. Therefore, use a module that has a sufficient current rating.
 - After the CPU module is powered on or is reset, the time taken to enter the RUN status varies depending on the system configuration, parameter settings, and/or program size. Design circuits so that the entire system will always operate safely, regardless of the time.
 - Do not power off the programmable controller or reset the CPU module while the settings are being written. Doing so will make the data in the flash ROM and SD memory card undefined. The values need to be set in the buffer memory and written to the flash ROM and SD memory card again. Doing so also may cause malfunction or failure of the module.
 - When changing the operating status of the CPU module from external devices (such as the remote RUN/STOP functions), select "Do Not Open by Program" for "Opening Method" of "Module Parameter". If "Open by Program" is selected, an execution of the remote STOP function causes the communication line to close. Consequently, the CPU module cannot reopen the line, and external devices cannot execute the remote RUN function.
-

[Security Precautions]

WARNING

- To maintain the security (confidentiality, integrity, and availability) of the programmable controller and the system against unauthorized access, denial-of-service (DoS) attacks, computer viruses, and other cyberattacks from external devices via the network, take appropriate measures such as firewalls, virtual private networks (VPNs), and antivirus solutions.
-

[Installation Precautions]

WARNING

- Shut off the external power supply (all phases) used in the system before mounting or removing the module. Failure to do so may result in electric shock or cause the module to fail or malfunction.
-

[Installation Precautions]

CAUTION

- Use the programmable controller in an environment that meets the general specifications in the Safety Guidelines (IB-0800525). Failure to do so may result in electric shock, fire, malfunction, or damage to or deterioration of the product.
 - To mount a module, place the concave part(s) located at the bottom onto the guide(s) of the base unit, and push in the module until the hook(s) located at the top snaps into place. Incorrect interconnection may cause malfunction, failure, or drop of the module.
 - To mount a module with no module fixing hook, place the concave part(s) located at the bottom onto the guide(s) of the base unit, push in the module, and fix it with screw(s). Incorrect interconnection may cause malfunction, failure, or drop of the module.
 - When using the programmable controller in an environment of frequent vibrations, fix the module with a screw.
 - Tighten the screws within the specified torque range. Undertightening can cause drop of the component or wire, short circuit, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, or malfunction. For the specified torque range, refer to the MELSEC iQ-R Module Configuration Manual.
 - When using an extension cable, connect it to the extension cable connector of the base unit securely. Check the connection for looseness. Poor contact may cause malfunction.
 - When using an SD memory card, fully insert it into the SD memory card slot. Check that it is inserted completely. Poor contact may cause malfunction.
 - Securely insert an extended SRAM cassette or a battery-less option cassette into the cassette connector of the CPU module. After insertion, close the cassette cover and check that the cassette is inserted completely. Poor contact may cause malfunction.
 - Beware that the module could be very hot while power is on and immediately after power-off.
 - Do not directly touch any conductive parts and electronic components of the module, SD memory card, extended SRAM cassette, battery-less option cassette, or connector. Doing so can cause malfunction or failure of the module.
-

[Wiring Precautions]

WARNING

- Shut off the external power supply (all phases) used in the system before installation and wiring. Failure to do so may result in electric shock or cause the module to fail or malfunction.
- After installation and wiring, attach a blank cover module (RG60) to each empty slot before powering on the system for operation. Also, attach an extension connector protective cover^{*1} to each unused extension cable connector as necessary. Directly touching any conductive parts of the connectors while power is on may result in electric shock.

^{*1} For details, please consult your local Mitsubishi Electric representative.

[Wiring Precautions]

CAUTION

- Individually ground the FG and LG terminals of the programmable controller with a ground resistance of 100 ohms or less. Failure to do so may result in electric shock or malfunction.
 - Use applicable solderless terminals and tighten them within the specified torque range. If any spade solderless terminal is used, it may be disconnected when the terminal screw comes loose, resulting in failure.
 - Check the rated voltage and signal layout before wiring to the module, and connect the cables correctly. Connecting a power supply with a different voltage rating or incorrect wiring may cause fire or failure.
 - Connectors for external devices must be crimped or pressed with the tool specified by the manufacturer, or must be correctly soldered. Incomplete connections may cause short circuit, fire, or malfunction.
 - Securely connect the connector to the module. Poor contact may cause malfunction.
 - Do not install the control lines or communication cables together with the main circuit lines or power cables. Doing so may result in malfunction due to noise. Keep a distance of 100mm or more between those cables.
 - Place the cables in a duct or clamp them. If not, dangling cables may swing or inadvertently be pulled, resulting in malfunction or damage to modules or cables.
In addition, the weight of the cables may put stress on modules in an environment of strong vibrations and shocks.
Do not clamp the extension cables with the jacket stripped. Doing so may change the characteristics of the cables, resulting in malfunction.
 - Check the interface type and correctly connect the cable. Incorrect wiring (connecting the cable to an incorrect interface) may cause failure of the module and external device.
 - Tighten the terminal screws or connector screws within the specified torque range. Undertightening can cause drop of the screw, short circuit, fire, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, fire, or malfunction.
 - When disconnecting the cable from the module, do not pull the cable by the cable part. For the cable with connector, hold the connector part of the cable. For the cable connected to the terminal block, loosen the terminal screw. Pulling the cable connected to the module may result in malfunction or damage to the module or cable.
 - Prevent foreign matter such as dust or wire chips from entering the module. Such foreign matter can cause a fire, failure, or malfunction.
-

[Wiring Precautions]

CAUTION

- When a protective film is attached to the top of the module, remove it before system operation. If not, inadequate heat dissipation of the module may cause a fire, failure, or malfunction.
 - Programmable controllers must be installed in control panels. Connect the main power supply to the power supply module in the control panel through a relay terminal block. Wiring and replacement of a power supply module must be performed by qualified maintenance personnel with knowledge of protection against electric shock. For wiring, refer to the MELSEC iQ-R Module Configuration Manual.
 - For Ethernet cables to be used in the system, select the ones that meet the specifications in the user's manual for the module used. If not, normal data transmission is not guaranteed.
-

[Startup and Maintenance Precautions]

WARNING

- Do not touch any terminal while power is on. Doing so will cause electric shock or malfunction.
 - Correctly connect the battery connector. Do not charge, disassemble, heat, short-circuit, solder, or throw the battery into the fire. Also, do not expose it to liquid or strong shock. Doing so will cause the battery to produce heat, explode, ignite, or leak, resulting in injury and fire.
 - Shut off the external power supply (all phases) used in the system before cleaning the module or retightening the terminal screws, connector screws, or module fixing screws. Failure to do so may result in electric shock.
-

CAUTION

- When connecting an external device with a CPU module or intelligent function module to modify data of a running programmable controller, configure an interlock circuit in the program to ensure that the entire system will always operate safely. For other forms of control (such as program modification, parameter change, forced output, or operating status change) of a running programmable controller, read the relevant manuals carefully and ensure that the operation is safe before proceeding. Improper operation may damage machines or cause accidents.
 - Especially, when a remote programmable controller is controlled by an external device, immediate action cannot be taken if a problem occurs in the programmable controller due to a communication failure. To prevent this, configure an interlock circuit in the program, and determine corrective actions to be taken between the external device and CPU module in case of a communication failure.
 - Do not disassemble or modify the modules. Doing so may cause failure, malfunction, injury, or a fire.
 - Use any radio communication device such as a cellular phone or PHS (Personal Handy-phone System) 25cm or more away in all directions from the programmable controller. Failure to do so may cause malfunction.
 - Shut off the external power supply (all phases) used in the system before mounting or removing the module. Failure to do so may cause the module to fail or malfunction.
 - Tighten the screws within the specified torque range. Undertightening can cause drop of the component or wire, short circuit, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, or malfunction.
 - After the first use of the product, do not perform each of the following operations more than 50 times (IEC 61131-2/JIS B 3502 compliant).
Exceeding the limit may cause malfunction.
 - Mounting/removing the module to/from the base unit
 - Inserting/removing the extended SRAM cassette or battery-less option cassette to/from the CPU module
 - Mounting/removing the terminal block to/from the module
 - Connecting/disconnecting the extension cable to/from the base unit
-

[Startup and Maintenance Precautions]

CAUTION

- After the first use of the product, do not insert/remove the SD memory card to/from the CPU module more than 500 times. Exceeding the limit may cause malfunction.
 - Do not touch the metal terminals on the back side of the SD memory card. Doing so may cause malfunction or failure of the module.
 - Do not touch the integrated circuits on the circuit board of an extended SRAM cassette or a battery-less option cassette. Doing so may cause malfunction or failure of the module.
 - Do not drop or apply shock to the battery to be installed in the module. Doing so may damage the battery, causing the battery fluid to leak inside the battery. If the battery is dropped or any shock is applied to it, dispose of it without using.
 - Startup and maintenance of a control panel must be performed by qualified maintenance personnel with knowledge of protection against electric shock. Lock the control panel so that only qualified maintenance personnel can operate it.
 - Before handling the module, touch a conducting object such as a grounded metal to discharge the static electricity from the human body. Wearing a grounded antistatic wrist strap is recommended. Failure to discharge the static electricity may cause the module to fail or malfunction.
 - After unpacking, eliminate static electricity from the module to prevent electrostatic discharge from affecting the module. If an electrostatically charged module comes in contact with a grounded metal object, a sudden electrostatic discharge of the module may cause failure.
For details on how to eliminate static electricity from the module, refer to the following.
Antistatic Precautions Before Using MELSEC iQ-R Series Products (FA-A-0368)
 - Use a clean and dry cloth to wipe off dirt on the module.
-

[Operating Precautions]

CAUTION

- When changing data and operating status, and modifying program of the running programmable controller from an external device such as a personal computer connected to an intelligent function module, read relevant manuals carefully and ensure the safety before operation. Incorrect change or modification may cause system malfunction, damage to the machines, or accidents.
 - Do not power off the programmable controller or reset the CPU module while the setting values in the buffer memory are being written to the flash ROM in the module. Doing so will make the data in the flash ROM and SD memory card undefined. The values need to be set in the buffer memory and written to the flash ROM and SD memory card again. Doing so can cause malfunction or failure of the module.
-

[Disposal Precautions]

CAUTION

- When disposing of this product, treat it as industrial waste.
 - When disposing of batteries, separate them from other wastes according to the local regulations. For details on battery regulations in EU member states, refer to the MELSEC iQ-R Module Configuration Manual.
-

[Transportation Precautions]

CAUTION

- When transporting lithium batteries, follow the transportation regulations. For details on the regulated models, refer to the MELSEC iQ-R Module Configuration Manual.
 - The halogens (such as fluorine, chlorine, bromine, and iodine), which are contained in a fumigant used for disinfection and pest control of wood packaging materials, may cause failure of the product. Prevent the entry of fumigant residues into the product or consider other methods (such as heat treatment) instead of fumigation. The disinfection and pest control measures must be applied to unprocessed raw wood.
 - For shipping, always use the original packaging.
-

CONDITIONS OF USE FOR THE PRODUCT

- (1) Although Mitsubishi Electric has obtained the certification for Product's compliance to the international safety standards IEC61508, ISO13849-1 from TUV Rheinland, this fact does not guarantee that Product will be free from any malfunction or failure. The user of this Product shall comply with any and all applicable safety standard, regulation or law and take appropriate safety measures for the system in which the Product is installed or used and shall take the second or third safety measures other than the Product. Mitsubishi Electric is not liable for damages that could have been prevented by compliance with any applicable safety standard, regulation or law.
- (2) Mitsubishi Electric prohibits the use of Products with or in any application involving, and Mitsubishi Electric shall not be liable for a default, a liability for defect warranty, a quality assurance, negligence or other tort and a product liability in these applications.
 - (a) power plants,
 - (b) trains, railway systems, airplanes, airline operations, other transportation systems,
 - (c) hospitals, medical care, dialysis and life support facilities or equipment,
 - (d) amusement equipments,
 - (e) incineration and fuel devices,
 - (f) handling of nuclear or hazardous materials or chemicals,
 - (g) mining and drilling,
 - (h) and other applications where the level of risk to human life, health or property are elevated.
- (3) Mitsubishi Electric shall have no responsibility or liability for any problems involving programmable controller trouble and system trouble caused by DoS attacks, unauthorized access, computer viruses, and other cyberattacks.

INTRODUCTION

Thank you for purchasing the Mitsubishi Electric MELSEC iQ-R series programmable controllers. This manual describes the specifications, procedures before operation, system configuration, wiring, parameter settings, functions, programming, and troubleshooting of the relevant product listed below. Before using this product, please read this manual and the relevant manuals carefully and develop familiarity with the functions and performance of the MELSEC iQ-R series programmable controller to handle the product correctly. When applying the program examples provided in this manual to an actual system, ensure the applicability and confirm that it will not cause system control problems. Please make sure that the end users read this manual.

Relevant product

RJ71SEIP91-T4

Point

Unless otherwise specified, this manual provides program examples in which the I/O signals of the CIP Safety module are assigned as follows.

- Input signal: X0 to X1F
- Output signal: Y0 to Y1F



For the assignment of I/O signals, refer to the following.

 Page 120 PROGRAMMING

COMPLIANCE WITH EMC AND LOW VOLTAGE DIRECTIVES

Method of ensuring compliance

To ensure that Mitsubishi Electric programmable controllers maintain the EMC and Low Voltage Directives or other regulations when incorporated into other machinery or equipment, certain measures may be necessary. Please refer to one of the following manuals.

-  MELSEC iQ-R Module Configuration Manual (SH-081262ENG)
-  Safety Guidelines (IB-0800525)

Certification marks on the side of the programmable controller indicate compliance with the relevant regulations.

Additional measures

To ensure that this product maintains the EMC and Low Voltage Directives or other regulations, please refer to the following.

- Page 34 Conformance with EMC Directive in this manual.

CONTENTS

COPYRIGHT	1
PRECAUTIONS REGARDING WARRANTY AND SPECIFICATIONS	1
SAFETY PRECAUTIONS	2
CONDITIONS OF USE FOR THE PRODUCT	11
INTRODUCTION	12
COMPLIANCE WITH EMC AND LOW VOLTAGE DIRECTIVES	12
RELEVANT MANUALS	16
TERMS	17
GENERIC TERMS AND ABBREVIATIONS	18
CHAPTER 1 PART NAMES	19
CHAPTER 2 SPECIFICATIONS	23
2.1 Performance Specifications	23
2.2 Function List	25
CHAPTER 3 PROCEDURES BEFORE OPERATION	26
CHAPTER 4 SYSTEM CONFIGURATION	28
4.1 EtherNet/IP and CIP Safety on EtherNet/IP Network Configuration	28
4.2 Applicable CPU Modules	30
4.3 Applicable Base Units	31
4.4 Available Software Packages	32
4.5 Safety Standards	33
4.6 Safety Parameters	33
CHAPTER 5 WIRING	34
5.1 Wiring Method	34
5.2 Wiring Products	35
CHAPTER 6 PARAMETER SETTINGS	36
6.1 Procedure for Setting Parameters	36
6.2 Basic Setting	37
6.3 Refresh	38
Refresh Setting	38
Auto Refresh Setting	39
6.4 Writing Parameters	40
6.5 Reading CIP Safety Configuration	41
CHAPTER 7 CIP Safety Configuration Tool	42
7.1 Procedure for Setting Parameters	43
7.2 Window Structure	47
Menu	48
Configuration	49
Device Library	80
Network Detection	83
Logger	84
Window	84

Help	84
CHAPTER 8 COMMUNICATION TYPE	85
8.1 Standard Communications	85
Class1 communications	86
UCMM communications	95
8.2 Safety Communications	97
Overview of safety communications	98
How to check the status during safety communications	101
The number of safety connections used	104
Precautions for using the safety communications	105
CHAPTER 9 FUNCTIONS	106
9.1 Output Hold/Clear When the CPU Module Is Stopped (at Error Occurrence/STOP State)	106
9.2 Block Assurance	107
9.3 Auto Refresh	108
9.4 DLR Function	110
9.5 Safety Diagnostic Function	116
9.6 Firmware Update	117
CHAPTER 10 PROGRAMMING	120
10.1 Class1 Instance Communications	120
System configuration example	120
Parameter settings	121
Program example	137
10.2 Class1 Tag Communications	141
System configuration example	141
Parameter settings	142
Program example	154
10.3 UCMM message communications	159
System configuration example	159
Parameter settings	159
Program example	166
10.4 Safety Program	171
System configuration example	171
Parameter settings	172
Program example	198
CHAPTER 11 TROUBLESHOOTING	201
11.1 Checking with LEDs	201
11.2 Checking the Module Status	205
11.3 Checking the Network Status	207
EtherNet/IP network diagnostics of CIP Safety Configuration Tool	207
Checking with the buffer memory	207
11.4 Troubleshooting by Symptom	208
11.5 List of Error Codes	212
Error codes when a module error occurs	212
Error codes when a communication error occurs	217
11.6 Event List	222

APPENDICES	223
Appendix 1 Module Label	223
Appendix 2 I/O Signals	224
List of I/O signals	224
Details of input signals	225
Appendix 3 List of Special Relay Areas	228
Safety information	228
Appendix 4 List of Special Register Areas	229
Safety information	229
Appendix 5 List of Safety Special Relay Areas	230
Safety information	230
Appendix 6 List of Safety Special Register Areas	231
Safety information	231
Appendix 7 Buffer Memory	234
List of buffer memory addresses	234
Details of buffer memory addresses	238
Appendix 8 Processing Time	252
Refresh processing time	252
Safety response time	253
Communication performance	254
Time required for detecting and recovering from ring configuration error	257
Appendix 9 External Dimensions	258
Appendix 10 Instance Number (Connection Point) for Class1 Instance Communications	259
Appendix 11 Added and Enhanced Functions	260
INDEX	261
REVISIONS	263
WARRANTY	264
INFORMATION AND SERVICES	266
TRADEMARKS	266

RELEVANT MANUALS


The following manuals are relevant to this product.

Manual name [manual number]	Description
MELSEC iQ-R CIP Safety Module User's Manual [SH-082444ENG] (this manual)	Specifications, procedures before operation, system configuration, wiring, parameter settings, CIP Safety Configuration Tool, functions, programming, troubleshooting, I/O signals, and buffer memory of the CIP Safety module
MELSEC iQ-R Module Configuration Manual [SH-081262ENG]	The combination of the MELSEC iQ-R series modules, common information on the installation/wiring in the system, and specifications of the power supply module, base unit, SD memory card, and battery
GX Works3 Operating Manual [SH-081215ENG]	System configuration, parameter settings, and online operations of GX Works3

This manual does not include detailed information on the following:

- General specifications
- Installation

For details, refer to the following.

 MELSEC iQ-R Module Configuration Manual

TERMS

Unless otherwise specified, this manual uses the following terms.

Term	Description
Active ring supervisor	A ring supervisor that controls the ring configuration
Adapter	A device that is used as a target only
Backup ring supervisor	A ring supervisor other than the active ring supervisor in the ring configuration
Beacon	A frame used for the ring configuration diagnostics
Buffer memory	Memory in an intelligent function module to store data such as setting values and monitor values. For CPU modules, it refers to memory to store data such as setting values and monitor values of the Ethernet function, or data used for data communication of the multiple CPU system function.
CIP Safety Configuration Tool	A setting tool used for performing safety communications and EtherNet/IP communications.
Class0	One of the communication types of CIP Safety communications. Cyclic transmission is performed between CIP Safety devices through the established connection.
Class1	One of the communication types of EtherNet/IP. Cyclic transmission is performed between EtherNet/IP devices through the established connection.
Consumer	A device that receives communication data
Cyclic transmission	A communication method by which data are periodically exchanged. On EtherNet/IP, communications are periodically performed by RPI (API) cycle.
Engineering tool	A tool used for setting up programmable controllers, programming, debugging, and maintenance.
EtherNet/IP device	A device, personal computer, and other equipment connected via EtherNet/IP for data communications
Exclusive Owner	One of the connection types of Class1 communications. A connection that allows bidirectional data transmission/reception between a target and an originator.
Global label	A label that is valid for all the program data when multiple program data are created in the project. There are two types of global label: a module specific label (module label), which is generated automatically by GX Works3, and an optional label, which can be created for any specified device.
Input Only	One of the connection types of Class1 communications. A connection that allows unidirectional data transmission from a target to an originator.
Instance communications	Data communications are performed by using an instance ID.
Listen Only	One of the connection types of Class1 communications. As with Input Only, a connection that allows unidirectional data transmission from a target to an originator. However, this connection is allowed only through the established connection.
Module label	A label that represents one of memory areas (I/O signals and buffer memory areas) specific to each module in a given character string. For the module used, GX Works3 automatically generates this label, which can be used as a global label.
Originator	A device that sends the connection establishment request
Producer	A device that sends communication data
Ring fault	Unsustainable status of the ring configuration due to an error in a device or a cable in the ring configuration
Ring node	A device other than the ring supervisor in the ring configuration
Safety Signature	An identifier that indicates the configuration of the CIP Safety device. It consists of CRC of configuration data and the configured date and time.
Scanner	A device that serves as either originator or target
Tag communications	Data communications are performed by using a tag name (character strings).
Target	A device that receives the connection establishment request

GENERIC TERMS AND ABBREVIATIONS

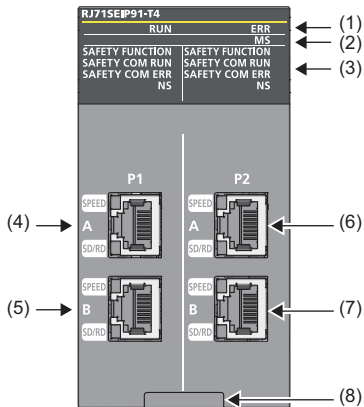
Unless otherwise specified, this manual uses the following generic terms and abbreviations.

Generic term/abbreviation	Description
API	An abbreviation for the Actual Packet Interval. While RPI is the communication cycle requested from an originator, API is the communication cycle decided by a target.
CC-Link IE Field Network-equipped master/local module	A generic term for the following modules: <ul style="list-style-type: none"> • RJ71GF11-T2 CC-Link IE Field Network master/local module • RJ71EN71 (when the CC-Link IE Field Network function is used) • RnENCPU (when the CC-Link IE Field Network function is used)
CC-Link IE TSN master/local module	RJ71GN11-T2
CIP	An abbreviation for the Common Industrial Protocol
CIP Safety module	An abbreviation for the MELSEC iQ-R series CIP Safety module
CIP specifications	A generic term for the following specifications published by ODVA (www.odva.org) <ul style="list-style-type: none"> • THE CIP NETWORKS LIBRARY Volume 1 Common Industrial Protocol (CIP™) • THE CIP NETWORKS LIBRARY Volume 2 EtherNet/IP Adaptation of CIP • THE CIP NETWORKS LIBRARY Volume 5 CIP Safety
CPU module	A generic term for the MELSEC iQ-R series CPU modules
DLR	An abbreviation for the Device Level Ring. A function used when EtherNet/IP or CIP Safety is used in a ring topology.
EDS	An abbreviation for the Electronic Data Sheet. A text-based file describing device information which is provided by the manufacturer.
EPI	An abbreviation for the Expected Packet Interval. A packet transmission interval of CIP Safety communications.
Motion module	RD78G4, RD78G8, RD78G16, RD78G32, RD78G64, RD78GHV, RD78GHW
PPS	An abbreviation for the Packets Per Second. The number of packets that can be processed per second.
RPI	An abbreviation for the Requested Packet Interval. A communication cycle that is decided by the originator during communications between EtherNet/IP devices.
Safety device	A generic term for the device that can be used in safety programs
SNCT	An abbreviation for the Safety Network Configuration Tool. A tool used for setting the CIP Safety communications.
SNN	An abbreviation for the Safety Network Number. A unique number to uniquely identify the safety network on CIP Safety communications.
TUNID	A generic term for the UNID of the target
UCMM	An abbreviation for the Unconnected Message Manager. One of the communication types of EtherNet/IP. Message communications such as read request and write request are performed between EtherNet/IP devices without establishing the connection.
UNID	An abbreviation for the Unique Network Identifier. A unique identifier used for uniquely identifying the device. A 10-byte value which is a combination of SNN and node ID (IP address).

1 PART NAMES

1

This chapter describes the names of each part of the CIP Safety module.



No.	Name	Description
(1)	RUN LED ERR LED	Indicates the operating status. RUN LED on and ERR LED off: Normal operation RUN LED on and ERR LED on: Minor error RUN LED on and ERR LED flashing: Moderate error RUN LED off and ERR LED flashing: Major error RUN LED off and ERR LED off: No power supply
(2)	MS LED	Indicates the module status. Off: No power supply On (green): Operating Flashing (green): Operation stopped (starting-up) Flashing (red): Operation stopped (error) On (red): Operation stopped (error) Flashing (alternating between green and red): Operation stopped (self-test in progress, waiting for the TUNID setting, or configuration setting required)
(3)	SAFETY FUNCTION LED	Indicates whether safety communications are enabled. Off: Safety communications are not set. On: Safety communications are set.
	SAFETY COM RUN LED	Indicates the execution status of safety communications. Off: Safety communication not being executed On: Safety communications being executed on one or more connections
	SAFETY COM ERR LED	Indicates the error status of safety communications. Off: Timeout not occurred in safety communication connection On: Timeout occurred in safety communication connection
	NS LED	Indicates the network status. Off: No power supply (No link-up) On (green): Online (communications being executed on one or more connections) Flashing (green): Online (communications not being executed) ¹ Flashing (red): Online (timeout in the connection) ² On (red): Offline (port stop error) Flashing (alternating between green and red): Offline (self-test in progress, waiting for the TUNID setting, or online (network access error detected))
(4)	Ethernet port (P1-A)	A connector for the EtherNet/IP network. Connect an Ethernet cable. For wiring method and wiring precautions, refer to the following. 🔧 Page 34 WIRING
	SPEED LED (P1-A)	Indicates the link status. On: Link-up (100Mbps) Off: Link-down
	SD/RD LED (P1-A)	Indicates the data sending/receiving status. On: Data being sent or received Off: Data not transmitted or received
(5)	Ethernet port (P1-B)	Refer to the description of Ethernet port (P1-A).
	SPEED LED (P1-B)	
	SD/RD LED (P1-B)	

No.	Name	Description
(6)	Ethernet port (P2-A)	A connector for the EtherNet/IP network. Connect an Ethernet cable.
	SPEED LED (P2-A)	For wiring method and wiring precautions, refer to the following.
	SD/RD LED (P2-A)	☞ Page 34 WIRING
(7)	Ethernet port (P2-B)	Refer to the description of Ethernet port (P2-A).
	SPEED LED (P2-B)	
	SD/RD LED (P2-B)	
(8)	Production information marking	Indicates the production information (16 digits) of the CIP Safety module.

*1 If it flashes when only standard communication is set, TUNID that was set in the past and TUNID in the configuration may be mismatched. Re-set both the Safety Reset and TUNID.

*2 During Class1 communications, it flashes only when the connection type is Exclusive Owner (target). It flashes green when a timeout occurs during other Class1 communications.

Precautions for MS LED

For the CIP Safety module with the firmware version "02" or later, if P1 or P2 does not link up at the module start-up, the status will be self-test in progress and the MS LED will flash alternately between green and red.

In that case, the LED status can be updated by linking up both P1 and P2. For example, when a link-up is started with the set TUNID and no TUNID mismatch has occurred, the MS LED status changes from flashing alternately between green and red to lighting up in green.

CIP Safety module status and LED status

The following table shows the correspondence between the status of the CIP Safety module and the status of the LED.

CIP Safety module status			LED status		
			RUN LED	ERR LED	MS LED
No power supply/power supply being reset			Off	Off	Off
Module initialization in progress			Off	Off	Off
Module initialization completed	Normal operation	Self-test in progress, waiting for the TUNID setting, or configuration being set	On	Off	Flashing (alternating between green and red)
		Starting up	On	Off	Flashing (green)
		Operating	On	Off	On (green)
	Minor error	Self-test in progress, waiting for the TUNID setting, or configuration being set	On	On	Flashing (alternating between green and red)
		Starting up	On	On	Flashing (green)
		Operating	On	On	On (green)
	Moderate error		On	Flashing	Flashing (red), on (red) ^{*2*3}
	Major error		Off	Flashing ^{*1}	

*1 It may not be displayed normally because a major error (hardware failure) has occurred.

*2 It may not be displayed normally because an error has occurred.

*3 Judge whether the error is a moderate error or a major error according to the RUN LED or ERR LED.

Port status and NS LED status

The following table shows the correspondence between the port status and the NS LED status.

Port status	NS LED status
No power supply/power supply being reset	Off
Module initialization in progress	Off

Port status			NS LED status	
Module initialization completed	P1 stop ('Port start status (P1)' (X1): OFF)		Port initialization in progress	Off
	P1 start ('Port start status (P1)' (X1): ON)	P1 stop ('Port stop error status (P1)' (X2): OFF)	Failed to establish connection	Flashing (green)
			Waiting for the TUNID application	Flashing (alternating between green and red)
			One or more connections have been established.	On (green)
			One or more connections have been timed out.	Flashing (red)
		P1 start ('Port stop error status (P1)' (X2): ON)	Stop error (such as due to overlapping IP addresses)	On (red)

CIP Safety module status and SAFETY FUNCTION LED status

The following table shows the correspondence between the status of the CIP Safety module and the status of the SAFETY FUNCTION LED.

CIP Safety module status			SAFETY FUNCTION LED status
No power supply/power supply being reset			Off
Module initialization in progress			Off
Module initialization completed	Normal operation	Safety communications are set.	On
		Safety communications are not set.	Off
	Minor error	Safety communications are set.	On
		Safety communications are not set.	Off
	Moderate error		Off
	Major error		Off

Port status and LED status

The following table shows the correspondence between the port status and the LED status.

Port status				LED status	
				SAFETY COM RUN LED	SAFETY COM ERR LED
No power supply/power supply being reset				Off	Off
Module initialization in progress				Off	Off
Module initialization completed	P1 stop ('Port start status (P1)' (X1): OFF)		Port initialization in progress	Off	Off
	P1 start ('Port start status (P1)' (X1): ON)	P1 stop ('Port stop error status (P1)' (X2): OFF)	Failed to establish safety connection	Off	Off
			One or more safety connections have been established.	On	Off
			One or more safety connections have timed out.	On	On
		P1 start ('Port stop error status (P1)' (X2): ON)	Stop error (such as due to overlapping IP addresses)	Off	On

2 SPECIFICATIONS

2.1 Performance Specifications

The following table lists performance specifications of the CIP Safety module.

Item		Description
Standard communications	Communication method	<ul style="list-style-type: none"> Class1 communications (instance communications, tag communications) UCMM communications (message communications) (Corresponds to each communication of the originator and the target.)
	Maximum number of connections	<ul style="list-style-type: none"> Class1 communications (instance communications, tag communications): 128^{*4} UCMM communications (message communications): 32
	Maximum data size per connection	<ul style="list-style-type: none"> Class1 communications (instance communications, tag communications): 1444 bytes UCMM communications (message communications): 504 bytes
	Maximum data size for all connections	16384 bytes
	RPI (Class1 communications)	1ms to 60000ms
Safety communications	Communication method	Class0 communications
	Number of connections	<ul style="list-style-type: none"> Consumer: 120^{*5} Producer: 120^{*5}
	Data size per connection	<ul style="list-style-type: none"> Consumer: 1 to 14 bytes Producer: 1 to 14 bytes (Variable in increments of 1K bytes)
	RPI	4ms to 1000ms
	Safety CPU transmission interval monitoring time ^{*1}	3 to 1000ms
	CIP Safety module transmission interval monitoring time ^{*1}	3 to 1000ms
	Safety refresh monitoring time ^{*2}	4 to 2000ms
Performance		12000pps ^{*7}
Topology		<ul style="list-style-type: none"> Line topology Star topology Ring topology (The module can operate as a ring node and ring supervisor)^{*6}
Number of network systems		2 systems (P1, P2)
Number of Ethernet ports		4 (P1 × 2, P2 × 2)
Interface		100BASE-TX
Communication method		<ul style="list-style-type: none"> Full-duplex Half-duplex
Data transmission speed		100Mbps (100BASE-TX)
Transmission method		Base band
Maximum segment length (length between a switching hub and a node)		100m ^{*3}
External wiring compatible connector		RJ45 connector
Support function		<ul style="list-style-type: none"> Auto-negotiation (auto-negotiation of communication speed/communication method) Auto MDI/MDIX (auto-negotiation of straight/cross)
Number of occupied I/O points		32 points (I/O assignment: Intelligent 32 points)
Internal current consumption (5VDC)		1.56A
External dimensions	Height	106mm
	Width	56.0mm
	Depth	110mm
Weight		0.38kg

- *1 CIP Safety Configuration Tool automatically calculates the lower limit value of each transmission interval monitoring time that satisfies the following conditions according to the setting details, and displays the result on the setting window.
CIP Safety module: $SC_{GW} \times 3 \leq TM_{GW}$ and $SC_{CPU} \times 2 \leq TM_{GW}$, Safety CPU: $SC_{CPU} \times 3 \leq TM_{CPU}$ and $SC_{GW} \times 2 \leq TM_{CPU}$
- *2 CIP Safety Configuration Tool automatically calculates the lower limit value of the safety refresh monitoring time that satisfies the following conditions according to the setting details, and displays the result on the setting window.
 $TM_{CPU} + (TM_{GW} / 2) \leq RM$ and $(TM_{CPU} / 2) + TM_{GW} \leq RM$
- *3 For maximum segment length (length between switching hubs), consult the manufacturer of the switching hub used.
- *4 The maximum number of connections per port is 64.
- *5 For the CIP Safety module with the firmware version "01", the number of connections is 60.
- *6 For the CIP Safety module with the firmware version "01", the module can operate as a ring node only.
- *7 To maintain communication quality, it is recommended to set a value so that the total communication processing performance (PPS) value does not exceed 80% of the performance value.

Point

- TM_{CPU} : Safety CPU transmission interval monitoring time
- TM_{GW} : CIP Safety module transmission interval monitoring time
- SC_{CPU} : Safety CPU safety cycle time
- SC_{GW} : CIP Safety module safety cycle time
- RM : Safety refresh monitoring time

Precautions

Use the following calculation formula as a guide to set the RPI, number of connections, and data size.

If the calculation formula is not satisfied, the performance limit of the CIP Safety module may be exceeded and the connection may be cut off. (Sufficiently perform the test as the calculation formula may not hold depending on the network environment used.)

- Minimum RPI in all connections > $(0.18 \times \text{number of CIP Safety connections}) + (0.0035 \times \text{total size of CIP Safety data}) + (0.008 \times \text{number of Class1 connections}) + (0.001 \times \text{total size of Class1 data})$

Ex.

Calculation result examples

CIP Safety		Class1		Calculation value
Number of connections	Total data size	Number of connections	Total data size	
4	56 bytes	16	2048 bytes	3.092ms
120	1680 bytes	16	2048 bytes	29.656ms
4	56 bytes	64	8192 bytes	9.620ms

2.2 Function List

The following table lists the function of the CIP Safety module.

Available: ○, Not available: —


Function		Description	Standard communication	Safety communication	Reference
EtherNet/IP communication functions	Class1 communications	Establishes connections between the CIP Safety module and EtherNet/IP devices, and performs data communications at a fixed scan.	○	—	Page 86 Class1 communications
	UCMM communications	Performs communications using data read/write commands between the CIP Safety module and the EtherNet/IP devices at a desired timing without establishing connections.	○	—	Page 95 UCMM communications
	Output hold/clear when the CPU module is stopped (at error occurrence/ STOP state)	Sets whether to clear or hold the output data when the CPU module stops.	○	○	Page 106 Output Hold/ Clear When the CPU Module Is Stopped (at Error Occurrence/ STOP State)
	Block assurance	Assures the I/O data of Class1 communications between the CPU module and the CIP Safety module.	○	—	Page 107 Block Assurance
	DLR (Device Level Ring) function	Continues to communicate with a normally operating station even if a cable disconnection occurs or a faulty station exists in the ring configuration.	○	○	Page 110 DLR Function
Auto refresh		Automatically performs refresh (transfer) operation between the buffer memory and any device of the CPU module.	○	—	Page 108 Auto Refresh
CIP Safety communication functions	Safety communications	Establishes connections between the CIP Safety module and CIP Safety compatible devices, and performs safety communications at a fixed scan.	—	○	Page 97 Safety Communications
	Safety diagnostic function	Performs safety-specific self-diagnostics.	—	○	Page 116 Safety Diagnostic Function
Firmware update		Updates the firmware of the CIP Safety module.	○	○	Page 117 Firmware Update

3 PROCEDURES BEFORE OPERATION

This chapter describes the procedures before operation.



1. Mounting the module to the base unit

For how to mount/remove a module to/from the base unit, refer to the following.

 MELSEC iQ-R Module Configuration Manual

2. Network configuration

Configure the system and set the parameters that are required for start-up.

- Wiring^{*1} ( Page 34 WIRING)
- Parameter settings^{*2} ( Page 36 PARAMETER SETTINGS)

3. Programming

Create a program. For details, refer to the following.

 Page 120 PROGRAMMING

- *1 If the IP addresses may be overlapped because an IP address is not set, the IP address currently used is unknown, or other reasons, wire the cables after setting the parameters (after setting an IP address).
- *2 The parameters must be written to both CPU module and CIP Safety module.

Point

When the version of the engineering tool used is "1.100E" or later, the CIP Safety module can be replaced by the following procedure.

- Read the parameters from the programmable controller with the engineering tool. However, do not read the parameters written by the engineering tool with a version earlier than "1.100E". If such parameters are read and used, the CIP Safety module may not communicate properly.
- Replace the CIP Safety module.
- Follow the procedures before operation to re-set the parameters (such as writing to the programmable controller, downloading parameters, and setting TUNID).

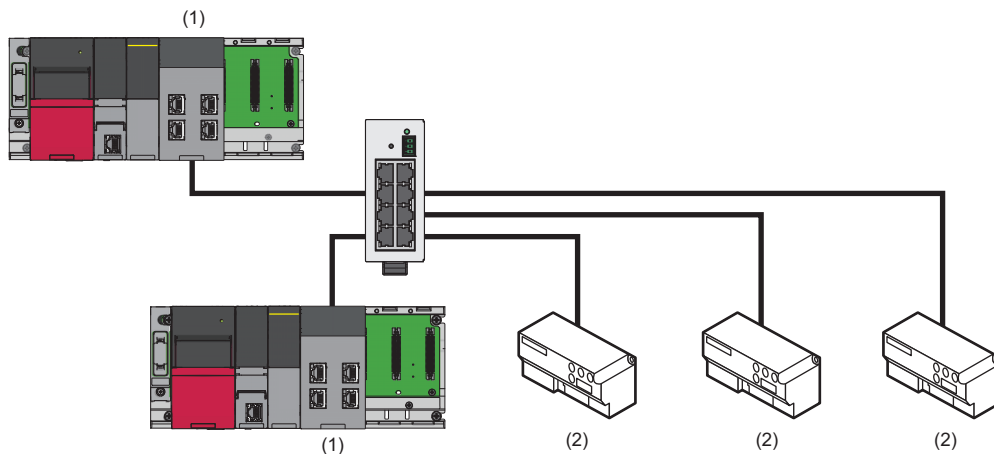
If the version of the engineering tool used is earlier than "1.100E", original parameters of CIP Safety Configuration Tool must be saved in the project file.

Use the saved project to replace the CIP Safety module, and follow the procedures before operation to re-set the parameters (such as writing to the programmable controller, downloading parameters, and setting TUNID).

4 SYSTEM CONFIGURATION

4.1 EtherNet/IP and CIP Safety on EtherNet/IP Network Configuration

The EtherNet/IP network and the CIP Safety on EtherNet/IP network consist of a CIP Safety module (1) and an EtherNet/IP device (2).



Scanner and adapter

In the EtherNet/IP network and the CIP Safety on EtherNet/IP network, station types are separated into scanner and adapter.

Station type	Description
Scanner	A station type of EtherNet/IP. The scanner has the control information and controls the overall network. Devices that have a connection of originator or target can be operated as the scanner.
Adapter	A station type of EtherNet/IP. The adapter indicates stations other than the scanner. Devices that have a connection of target can be operated as the adapter.

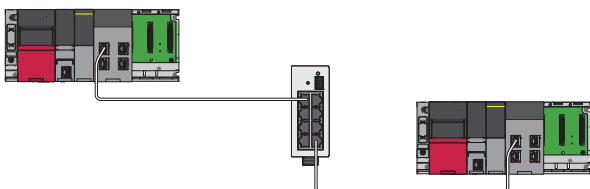
Line topology

Connect the modules in a line topology using Ethernet cables.



Star topology

Connect the modules in a star topology using a switching hub and Ethernet cables.



Ring topology

Connect the modules in a ring topology using Ethernet cables.



4.2 Applicable CPU Modules

The following table shows the availability of the CIP Safety module when each CPU module is used.

The CPU modules are represented by the following symbols.

- Rn: RnCPU
- RnEN: RnENCPU
- RnP(P): Process CPU (process mode)
- RnP(R)(M): Process CPU (redundant mode) (main base unit)
- RnP(R)(E): Process CPU (redundant mode) (redundant system with redundant extension base unit)
- RnMT: Motion CPU
- RnNC: NCCPU
- RnRT: Robot CPU
- RnC: C Controller module
- RnPSF: SIL2 Process CPU
- RnSF: Safety CPU
- Rem: Remote head module
- Rem(R): Remote head module (redundant system)

○: Available, ×: Not available

CPU module	Rn	RnEN	RnP(P)	RnP(R)(M)	RnP(R)(E)	RnMT	RnNC	RnRT	RnC	RnPSF	RnSF	Rem	Rem(R)
CIP Safety module	×	×	×	×	×	×	×	×	×	×	○ ^{*1}	×	×

*1 The firmware version of the module should be 28 or later.

Point

- If the CIP Safety module is installed in a CPU module that cannot be used, an error will occur when writing the engineering tool.
- The backup/restore function of the Safety CPU does not support the setting data of CIP Safety Configuration Tool.

The number of mountable modules

CPU module	Maximum number of mounted modules	
	When configuring a single CPU system	When configuring a multiple CPU system
CIP Safety module	2	2 (maximum one Safety CPU per system)

Point

- The CIP Safety module is a 2-slot module, but like the 1-slot module, it is counted as the 1st/2nd module. Empty slots are not included in the number.
- If attempted to set parameters for the 3rd and subsequent CIP Safety modules, an error will occur in the engineering tool.
- If the CIP Safety module is mounted without setting the parameters, an error (error code: 3110H) will occur in the CIP Safety module when the module is powered on.

4.3 Applicable Base Units

The following table shows whether each base unit can be used when mounted to the CIP Safety module.

○: Applicable, ×: Not applicable

Base unit		Model	Availability
Main base unit	Main base unit	R33B, R35B, R38B, R312B	○
	Extended temperature range main base unit	R310B-HT	×
	Redundant power supply main base unit	R310RB	×
	Extended temperature range redundant power supply main base unit	R38RB-HT	×
Extension base unit	Extension base unit	R65B, R68B, R612B	○
	Extended temperature range extension base unit	R610B-HT	×
	Redundant power supply extension base unit	R610RB	×
	Extended temperature range redundant power supply extension base unit	R68RB-HT	×
	Redundant extension base unit	R68WRB	×
	Extended temperature range redundant extension base unit	R66WRB-HT	×
	RQ extension base unit	RQ65B, RQ68B, RQ612B	×

4

Precautions

- If the power capacity is insufficient, change the power supply module or add more base units.
- The following modules can be installed in the same CPU module, for up to eight modules in total: CIP Safety modules, CC-Link IE TSN master/local modules, CC-Link IE Field Network-equipped master/local modules, and simple motion modules.

4.4 Available Software Packages

To configure the settings of the CIP Safety module, the engineering tool and CIP Safety Configuration Tool are required. The following table shows the combination of the firmware version of the CIP Safety module, CIP Safety Configuration Tool and engineering tool.

Firmware version of the CIP Safety module	CIP Safety Configuration Tool	Engineering tool (GX Works3)
"01"	■Model SW1DNN-SEIPCT-BD ■Software version Version 1.2.0.3	Version 1.090U or later
"02" or later	■Model SW1DNN-SEIPCT-MD ■Software version Version 1.3.0.28 or later	Version 1.100E or later

CIP Safety Configuration Tool

■Operating environment, installation/uninstallation

For the operating environment and installation/uninstallation of CIP Safety Configuration Tool, refer to the following.

 CIP Safety Configuration Tool Installation Instructions

■Operation methods and functions

For the operation methods and functions of CIP Safety Configuration Tool, refer to the following.

 Page 42 CIP Safety Configuration Tool

Profile of the CIP Safety module

Profile is data in which the information (such as models) of the connected devices is stored.

The profile of the CIP Safety module is automatically registered in the engineering tool (GX Works3) when CIP Safety Configuration Tool is installed.

Point

If the software version of CIP Safety Configuration Tool is "1.2.0.3", refer to the following for how to register a profile.

 MELSEC iQ-R CIP Safety Module Profile and Module Label Registration Instruction

Module label for the CIP Safety module

The module label for the CIP Safety module is automatically registered in the engineering tool (GX Works3) when CIP Safety Configuration Tool is installed.

Point

If the software version of CIP Safety Configuration Tool is "1.2.0.3", refer to the following for how to register a module label.

 MELSEC iQ-R CIP Safety Module Profile and Module Label Registration Instruction

4.5 Safety Standards

Observe the following safety standards in using the module.

Region	Standard
International	IEC 61508 Parts 1-7: 2010
Europe	EN ISO 13849-1: 2015 EN IEC 62061: 2021

4.6 Safety Parameters

The following table shows the safety parameters of the CIP Safety module.

Item		Description
Target failure measure	PFDavg	7.11×10^{-6}
	PFH	1.05×10^{-10}
	Proof test interval	10 years

5 WIRING

This chapter describes the wiring for the EtherNet/IP network and the CIP Safety on EtherNet/IP network.

5.1 Wiring Method

This section describes how to connect and disconnect the Ethernet cable.

Connecting the cable

1. Push the Ethernet cable connector into the CIP Safety module until it clicks. Pay attention to the orientation of the connector.
2. Pull each cable lightly and check that it has been connected securely.
3. Check whether the SPEED LED of the port connected with an Ethernet cable is on.^{*1}

^{*1} The time between the cable connection and the turning on of the SPEED LED may vary. The SPEED LED usually turns on in a few seconds. Note, however, that the time may be extended further if the link-up processing is repeated depending on the status of the device on the line. Check whether the cables are connected properly if the SPEED LED does not turn on.

Disconnecting the cable

1. Unplug the Ethernet cable while pressing the latch connector down.

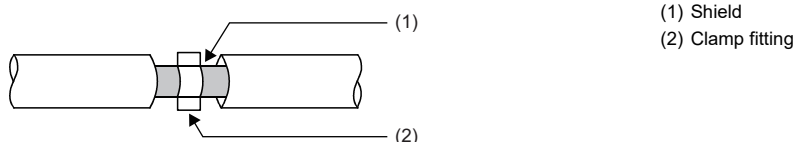
Precautions

- Place the Ethernet cable in a duct or clamp it. Failure to do so may lead to swinging or inadvertent pulling of dangling cable, resulting in damage to the module or the cable or malfunction due to poor contact.
- Do not touch the core of the cable-side or module-side connector, and protect them from dirt or dust. If oil on your hands, dirt, or dust adheres to the core, transmission loss may increase, causing communication problems.
- Check that the Ethernet cable is not disconnected or not shorted and check that the cable is connected properly.
- Do not use Ethernet cables with broken latch connectors. Doing so may cause the Ethernet cables to be disconnected or the module to malfunction.
- Hold the connector part of the Ethernet cable when connecting and disconnecting it. Pulling the cable connected to the module may result in damage to the module or the cable or malfunction due to poor contact.
- The maximum segment length of the Ethernet cable is 100m. However, the acceptable length may be shorter depending on the environment where the cable is used. For details, contact the cable manufacturer.
- The bending radius of the Ethernet cable is limited. For details, check the specifications of the Ethernet cable to be used.

Conformance with EMC Directive

To conform to the EMC Directive, take the following precautionary measure.

- Use a shielded twisted pair cable for a twisted pair cable to be used for the Ethernet cable. Strip off the jacket partly from the shielded twisted pair cable as shown below, and ground the exposed shield with as large a contact surface as possible.



5.2 Wiring Products

This section describes the devices used to comprise the EtherNet/IP network and the CIP Safety on EtherNet/IP network.

Ethernet cable

Use Ethernet cables that meet the following standards.

Communication speed	Ethernet cable	Connector	Standard
100Mbps	Category 5 or higher, (STP) straight cable	RJ45 connector	100BASE-TX
	Category 5 or higher, (STP) crossover cable		



Depending on the connection environment, communication errors may occur due to high-frequency noise from devices other than programmable controllers. The following describes precautionary measures to be taken on the CIP Safety module to avoid the influence of high-frequency noise.

- When wiring cables, do not bundle them together with or keep them in close proximity to the main circuit lines or power cables.
- Place cables in a duct.
- Use STP cables in place of UTP cables.









Switching hub

When using a switching hub for the EtherNet/IP network and the CIP Safety on EtherNet/IP network, use a switching hub that supports the transmission speed of communications.
Using a switching hub with the IGMP snooping function is recommended.

6 PARAMETER SETTINGS

This chapter describes the parameter settings required for communications with the CIP Safety module.

6.1 Procedure for Setting Parameters

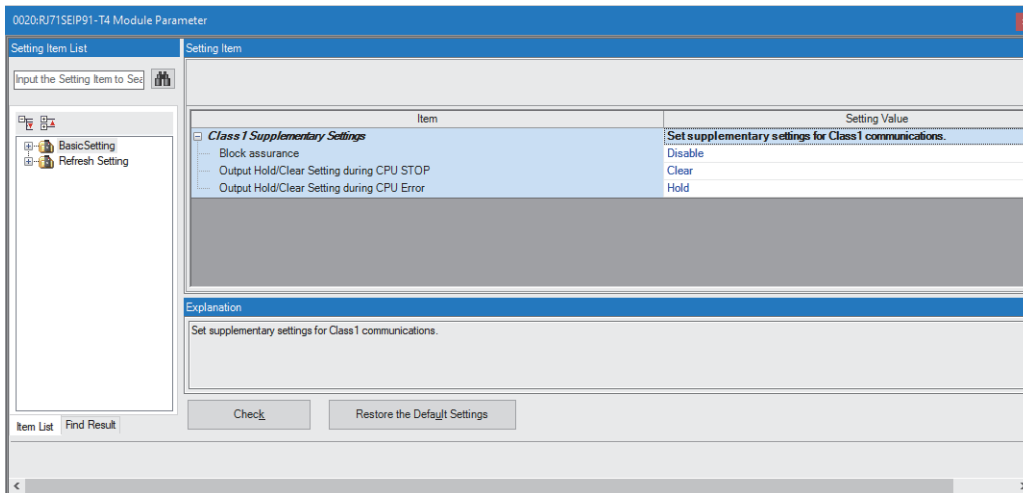
- 1.** Add the CIP Safety module (RJ71SEIP91-T4) in the engineering tool.
 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ Right-click ⇒ [Add New Module]
- 2.** The basic settings and refresh settings are included in the module parameters. Select the settings from the navigation tree in the following window and configure them.
 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4]
- 3.** Use the engineering tool to write the module parameters to the CPU module.
 [Online] ⇒ [Write to PLC]
- 4.** The settings are reflected by resetting the CPU module or powering off and on the system.
- 5.** Start CIP Safety Configuration Tool, and then add an EtherNet/IP device.
 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]
- 6.** Set the CIP Safety module using CIP Safety Configuration Tool.
- 7.** Use CIP Safety Configuration Tool to write the parameters to the CIP Safety module.
 [Configuration] ⇒ [Safety Communication Module] ⇒ [Safety Communication Module Access] ⇒ [Save configuration to module]
- 8.** Close CIP Safety Configuration Tool.
- 9.** Use the engineering tool to write the module parameters to the CPU module.
 [Online] ⇒ [Write to PLC]
- 10.** The settings are reflected by resetting the CPU module or powering off and on the system.
- 11.** Use the engineering tool to set the auto refresh to the CIP Safety module.
 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ Right-click ⇒ [Auto Refresh Setting]
- 12.** Use the engineering tool to write the module parameters to the CPU module.
 [Online] ⇒ [Write to PLC]
- 13.** The settings are reflected by resetting the CPU module or powering off and on the system.

Precautions

- When the parameters are read or written using the engineering tool, use an Ethernet cable or USB cable to connect between a personal computer and the CPU module and close the window of CIP Safety Configuration Tool.
- When the parameters are written using CIP Safety Configuration Tool, use an Ethernet cable to connect between a personal computer and the CPU module.
- When an engineering tool project is closed while the CIP Safety Configuration Tool window is open, the content edited by CIP Safety Configuration Tool is saved. To discard the edited content, close the CIP Safety Configuration Tool window first. (Exit without saving the project of CIP Safety Configuration Tool.)
- The project saved with CIP Safety Configuration Tool with the software version "1.2.0.3" needs to be re-saved when it is opened again with the Tool of the software version "1.3.0.28" or later.

6.2 Basic Setting

Configure the block assurance and output hold clear setting.



6


Class1 Supplementary Settings

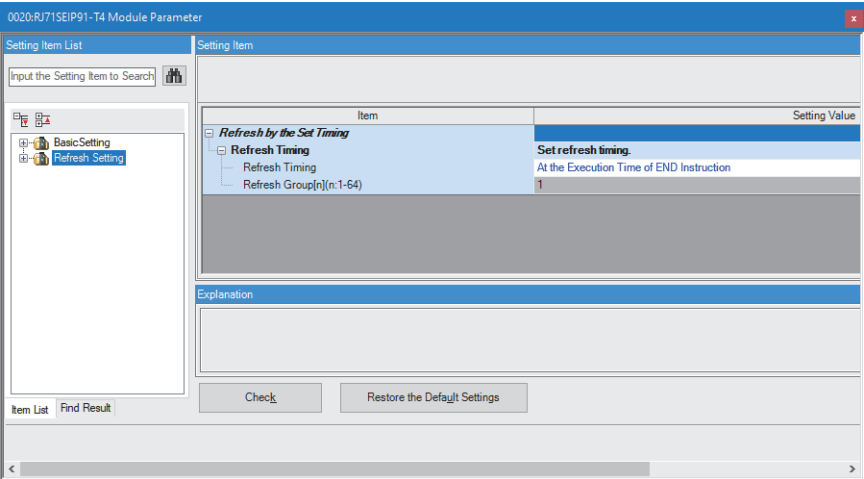
Item	Description	Setting range
Block assurance (Page 107 Block Assurance)	Set whether to perform data assurance when refreshing the input data and output data of Class1 communications between the CPU module and the CIP Safety module. When "Enable" is selected, also set auto refresh. (Page 39 Auto Refresh Setting)	<ul style="list-style-type: none"> • Enable • Disable (Default: Disable)
Output Hold/Clear Setting during CPU STOP (Page 106 Output Hold/Clear When the CPU Module Is Stopped (at Error Occurrence/STOP State))	Select whether to hold or clear the output of CIP Safety module when the CPU module to which the CIP Safety module is mounted is in STOP state. To hold, select "Hold".	<ul style="list-style-type: none"> • Clear • Hold (Default: Clear)
Output Hold/Clear Setting during CPU Error (Page 106 Output Hold/Clear When the CPU Module Is Stopped (at Error Occurrence/STOP State))	Select whether to hold or clear the output of the CIP Safety module when a stop error occurs in the CPU module. To hold, select "Hold".	<ul style="list-style-type: none"> • Clear • Hold (Default: Hold)

6.3 Refresh


Refresh Setting

Set the refresh timing.

 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [Module Parameter] ⇒ [Refresh Setting]



Refresh by the Set Timing		
Item	Description	Setting range
Refresh Timing	Sets the refresh timing.	<ul style="list-style-type: none">At the Execution Time of END InstructionAt the Execution Time of Specified Program (Default: At the Execution Time of END Instruction)
Refresh Group[n](n: 1-64)	Specifies the refresh group of programs. Set a program refresh group in the program settings of the CPU parameter.	<ul style="list-style-type: none">Refresh timing is at the execution time of END instruction: 1Refresh timing is at the execution time of specified program: 1 to 64 (Default: 1)

 **Point**

When the refresh is enabled, the refresh target values will be valid at the timing set in the engineering tool. At that time, buffer memory areas are overwritten with the refresh target values. To change the refresh target values in the buffer memory areas, create a program that changes the values in the refresh target module labels and devices.

Auto Refresh Setting

Set auto refresh.

[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ Right-click ⇒ [Auto Refresh Setting]

Point

- This setting is not required if there is no need to perform auto refresh. (Page 108 Auto Refresh)
- This setting cannot be set for the buffer memory for UCMM. The access to the buffer memory areas need to be programmed using the FROM/TO instruction.

Item	Description		Setting range
User CPU Device	The start address for which the CPU module copies I/O data. D, W, R and ZR devices are supported. When these devices are set in this area, each of them is set at once.		Maximum range of D, W, R, ZR devices (Default: D0)
Assign Devices per Buffer	<ul style="list-style-type: none"> • Not selected: Enter a single device address and all buffer memory device addresses will be calculated from that address. • Selected: "User CPU Device" is disabled and individual devices can be specified for each item listed under "Buffer". 		<ul style="list-style-type: none"> • Not selected • Selected (Default: Not selected)
Output devices (IQ-R CPU -> CIP Safety)	Buffer	Indicates the area to which the address of the CPU device is transferred. The following is set. <ul style="list-style-type: none"> • Class1 Status (P1) • Class1 Status (P2) • Class1 Input (P1)*1 • Class1 Input (P2)*1 • Class1 Output (P1)*1 • Class1 Output (P2)*1 	—
	Start Address	Set to display the start address of the buffer memory and CPU device. When "User CPU Device" is enabled, the value is automatically calculated. (Read-only) Selecting "Assign Devices per Buffer" allows the individual setting.	—
	End Address	Displays the buffer memory and the end address of the CPU device. This address is calculated from the size of static data and network configuration. (Read-only)	—
Input devices (IQ-R CPU <- CIP Safety)	Buffer*1	The same description as "Output devices (IQ-R CPU -> CIP Safety)".	—
	Start Address		
	End Address		

*1 This setting can be set after setting the network settings using CIP Safety Configuration Tool.

Precautions


- When the auto refresh setting window is displayed without setting the parameters in CIP Safety Configuration Tool, Class1 Status (P1) and Class1 Status (P2) can be set, but the I/O data is not set. Therefore, Class1 Input (P1), Class1 Input (P2), Class1 Output (P1), and Class1 Output (P2) cannot be set. Before setting the auto refresh of the I/O area, always set the parameters with CIP Safety Configuration Tool.
- After setting auto refresh, if CIP Safety Configuration Tool was used to make communication settings (setting change) by which the I/O area range changed, the auto refresh setting must also be re-set. (Otherwise, refresh will be performed using the last range that was set.)

6.4 Writing Parameters


The parameters set on the CIP Safety module have different write destinations.

Parameter type	Configuration tool	Write destination
<ul style="list-style-type: none">• Module parameter• Auto refresh setting	GX Works3	CPU module
<ul style="list-style-type: none">• IP address setting• Connection parameter	CIP Safety Configuration Tool	CIP Safety module

For writing parameters to the CPU module, refer to the following.

 GX Works3 Operating Manual

For writing to the CIP Safety module, refer to the following.

 Page 49 [Safety Communication Module Access] tab

6.5 Reading CIP Safety Configuration

The configuration of CIP Safety can be read by reading from the programmable controller.

Point

This function is available in the engineering tool version "1.100E" or later.

Operating procedure

1. Open "Online Data Operation".
-  [Online] ⇄ [Read from PLC]
2. Check "System Parameter/CPU Parameter (Standard/Safety)" and "Module Parameter (Standard/Safety)".

Online Data Operation

Display Setting Related Functions

Write Read Verify Delete

Parameter + Program(F) Select All Open/Close All(T) Deselect All(N)

Legend

CPU Built-in Memory

SD Memory Card

Intelligent Function Module

Refresh(W)

Module Name/Data Name				Detail	Title	Last Change	Size (Byte)
R08SF	<input type="checkbox"/>						
Parameter	<input type="checkbox"/>						
System Parameter/CPU Parameter (...)	<input checked="" type="checkbox"/>					2023/08/24 8:46:54	1228
Module Parameter (Standard/Safety)	<input checked="" type="checkbox"/>					2023/08/24 8:46:54	1780
Remote Password	<input type="checkbox"/>					2023/08/24 8:46:54	200
Global Label	<input type="checkbox"/>						
Global Label Setting	<input type="checkbox"/>					2023/08/24 8:46:54	13200
Device Memory	<input type="checkbox"/>						
Device Memory Data	<input type="checkbox"/>			Detail		2023/08/25 12:47:47	-
File Register	<input type="checkbox"/>			Detail			
MAIN	<input type="checkbox"/>					2023/08/24 8:57:36	65536
Common Device Comment	<input type="checkbox"/>						

Display Memory Capacity

Memory Capacity

Size Calculation

Legend

Used

Increased

Decreased

Free: 5% or Less

Program Memory

Data Memory

Device/Label Memory (File Storage Area)

SD Memory Card

Free

Free

Free

Free

320/320KB

3758/5122KB

850/914KB

0/0KB

Execute Close

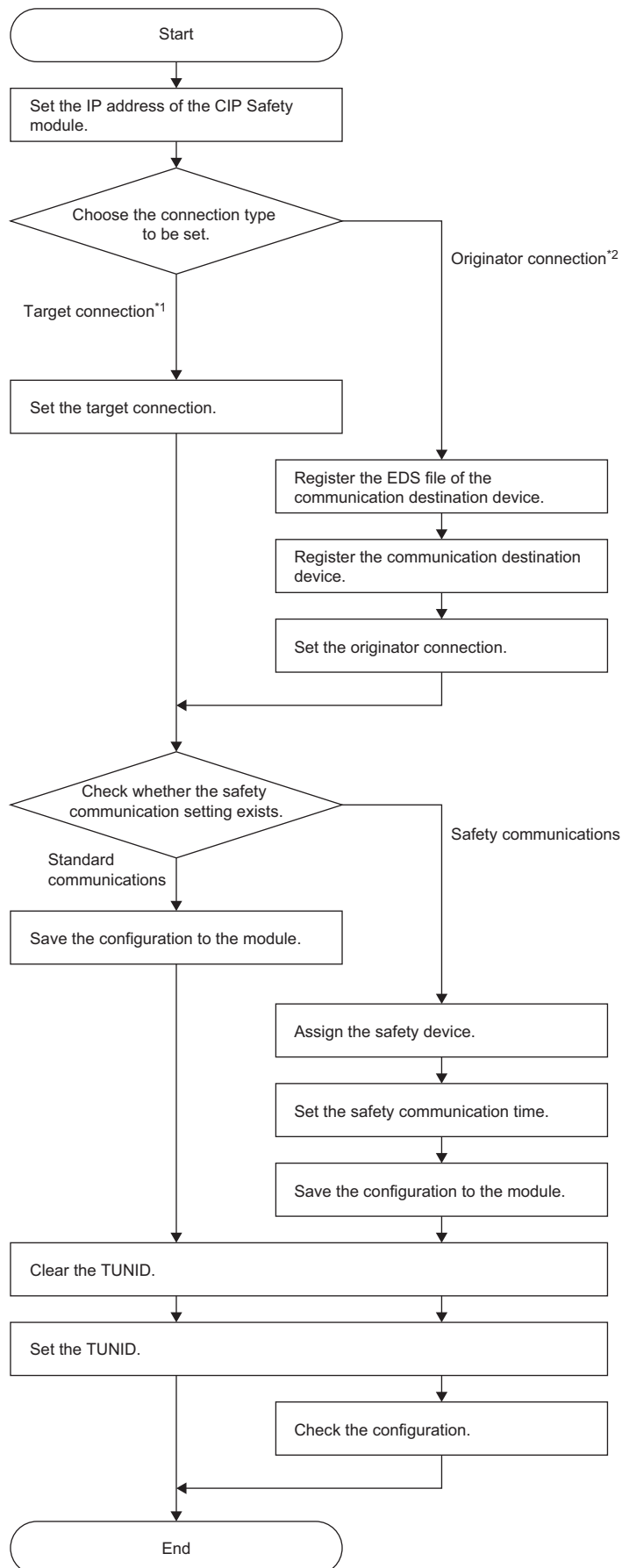
3. Click the [Execute] button.

7 CIP Safety Configuration Tool

This chapter describes operations of CIP Safety Configuration Tool.

7.1 Procedure for Setting Parameters

This section shows the flowchart for setting parameters in CIP Safety Configuration Tool.



- *1 The following are the target connections.
 - Target of Class1 instance communications
 - Producer of Class1 tag communications
 - Target of safety communications
- *2 The following are the originator connections.
 - Originator of Class1 instance communications
 - Consumer of Class1 tag communications
 - Originator of safety communications

Precautions

When a connection is edited (a connection is added/deleted or the instance or tag name is changed), the following information is automatically assigned again. After changing the parameter settings, check the following information again and correct the program as necessary.

- Safety communication connection: Connection No.
- Class1 communication connection: Connection No., 'Class1 Start offset address to the input data' (Un\G98816 to Un\G98943, Un\G1147392 to Un\G1147519), and 'Class1 Start offset address to the output data' (Un\G99072 to Un\G99199, Un\G1147648 to Un\G1147775)

List of parameter settings

Setting is required: ○, Setting is required as necessary: △, Setting is not required: —

Item		Setting details	Reference	Whether setting is required			
				Target		Originator	
				Standard communication	Safety communication	Standard communication	Safety communication
Setting the IP address of the CIP Safety module		Set the IP address.	Page 58 [General] tab	○	○	○	○
Setting the target connection		Enables the target connection.	Page 58 [General] tab	○	○	—	—
		Set the connection.	<ul style="list-style-type: none">• Page 67 [Target (Class1)] tab• Page 68 [Safety Target (Class0)] tab	○	○	—	—
Setting the originator connection	Registering the EDS file of the communication destination device	Add an EDS file of the communication destination device (target device).	Page 81 Adding EDS files	—	—	△ ^{*1}	△ ^{*1}
	Registering the communication destination device	Select the communication destination device (target device) in the device library view and register it to the configuration view. ^{*2}	Page 80 Device Library	—	—	○	○
	Setting the originator connection	Enables the originator connection.	Page 69 [General] tab	—	—	○	○
		Set the connection.	<ul style="list-style-type: none">• Page 74 [Standard Settings] tab• Page 77 [Safety Settings] tab	—	—	○	○
Setting the safety communication connection	Assigning the safety device	Assign the safety device to the connection. ([Labels/ Devices] tab)	Page 51 [CPU Data Exchange] tab	—	○	—	○
	Setting the safety communication time	For the target connection, set the same values as the EPI and Timeout Multiplier to be set on the communication destination device (originator device). ([Timings (Auto Calculation)] tab)		—	○	—	—

Item		Setting details	Reference	Whether setting is required			
				Target		Originator	
				Standard communication	Safety communication	Standard communication	Safety communication
Saving the configuration to the module		Save the configuration to the module.	Page 49 [Safety Communication Module Access] tab	○	○	○	○
TUNID setting	Clearing the TUNID	If a formerly-set TUNID remains in the CIP Safety module, perform Safety Reset to clear it.	Page 60 [Safety] tab	△ ^{*3}	△ ^{*3}	△ ^{*3}	△ ^{*3}
	Setting the TUNID	Set a TUNID if it has not been set to the CIP Safety module.		△ ^{*3}	△ ^{*3}	△ ^{*3}	△ ^{*3}
Checking the configuration		Verify that the configurations of CIP Safety Configuration Tool and CIP Safety module match.	Page 60 [Safety] tab	—	△	—	△

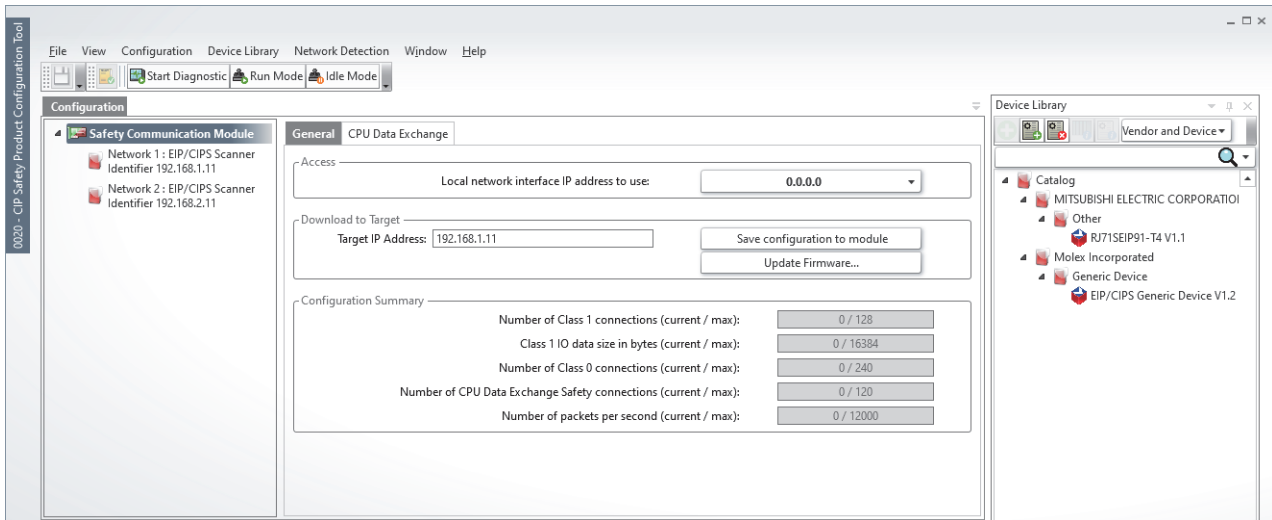
*1 To connect an external device whose EDS file is not registered as the target, register the EDS file of the device to the library. Once the EDS file is registered, re-registration is not required.

*2 During Class1 communications, multiple connections can be set for a single communication destination device.

*3 If changes were made to any of the settings that resulted in changing the TUNID (such as the IP address of the own station and Safety Network Number), the TUNID must be cleared and set again.

7.2 Window Structure

The following figure shows the window structure.



Item	Description	Reference
Menu	The menu of the tool	Page 48 Menu
Configuration	Lists devices to be configured on the tool. This view also displays parameters of the device selected in the tree.	Page 49 Configuration
Device Library	Devices added from EDS files will be registered as components. Displayed devices can be added to the configuration view.	Page 80 Device Library
Network Detection	Detects connected devices and displays them as components. Displayed devices can be added to the configuration view.	Page 83 Network Detection
Logger	Displays errors, warnings, and messages that are raised during edit operation.	Page 84 Logger

Menu

The following table lists the menu items of CIP Safety Configuration Tool.

Menu

File View Configuration Device Library Network Detection Window Help







Item		Description
File	Save	Saves edits made with the tool. This item will be enabled and selectable when a change is made to the settings on the tool after startup.
	Exit	Closes the tool.
View	Logger	Displays or hides an appropriate view.
	Device Library	• Selected: The view is displayed. • Not selected: The view is hidden.
	Network Detection	
Configuration	Listing ^{*1}	Create a list of information from the configuration view.
	Start Diagnostics/Stop Diagnostics ^{*2}	Starts or stops the diagnostics of a device specified in the configuration view.
	Run Mode	Changes the mode of a device specified in the configuration view to the Run mode.
	Idle Mode	Changes the mode of a device specified in the configuration view to the Idle mode.
	CIP options	Starts the option window. (Page 57 CIP options)
Device Library	Insert In Configuration	Inserts a device selected in the device library view into the configuration view.
	Add EDS	Adds a device specified in an EDS file into the device library.
	Remove EDS	Removes a device that is added to the device library.
	Properties	The properties of a device that is added to the device library can be checked.
	Show EDS ^{*3}	The EDS file of a device that is added to the device library can be checked.
Network Detection	Start Network detection	Detects devices on the network to display them.
	Insert In Configuration ^{*3}	Inserts a device detected from the network into the configuration view.
	Copy All ^{*3}	Copies devices detected from the network.
	Properties ^{*3}	Displays the properties of a device detected from the network.
Window	Layout Style Manager	Changes the window color.
Help	View Help	This item is not available.
	About	Displays the version information of the tool.

*1 The item is disabled when "Safety Communication Module" is selected in the configuration view.

*2 During diagnostics, configurations cannot be set and the status is displayed in the configuration view.

*3 The item is enabled when a device is selected.

Tool bar

Icon	Item	Description
	Save	Saves edits made with the tool. This item will be enabled and selectable when a change is made to the settings on the tool after startup.
	Display listing information on the current project	Creates a list of information from the configuration view.
 Start Diagnostic	Start Diagnostics/Stop Diagnostics	Starts or stops the diagnostics of a device specified in the configuration view.
 Stop Diagnostic		
 Run Mode	Run Mode	Changes the mode of a device specified in the configuration view to the Run mode.
 Idle Mode	Idle Mode	Changes the mode of a device specified in the configuration view to the Idle mode.

Configuration

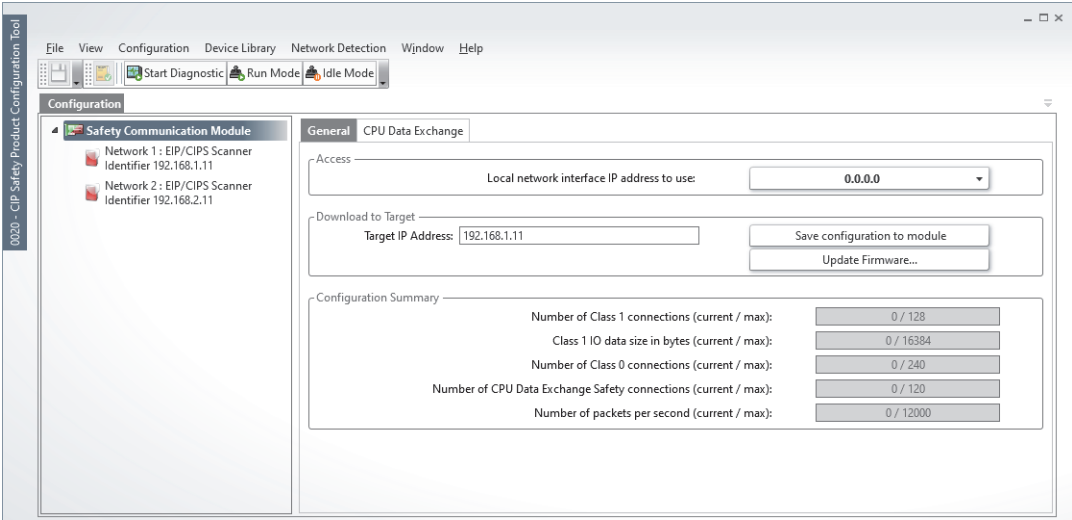
Lists devices to be configured on the tool.
Additionally, the setting pane varies depending on what is selected in the tree.

Point

Since the parameter items of devices are dependent on the EDS files, this section only describes the fixed items in detail.

Safety Communication Module

■[Safety Communication Module Access] tab



Item		Description
Access	Local network interface IP address to use	Set the local network IP address to use.
	Target IP Address	Set the target IP address.
	Save configuration to module	Writes the configuration contents into the module specified with the target IP address.
Download to Target	Update Firmware ^{*1}	Updates the firmware of the CIP Safety module. For details on how to update the firmware of the CIP Safety module, refer to the following. 📖 Page 117 Firmware Update
	Number of Class 1 connections (current/max)	Displays the information of an appropriate item.
	Class 1 IO data size in bytes (current/max)	
Configuration Summary ^{*1}	Number of Class 0 connections (current/maximum)	
	Number of CPU Data Exchange Safety connections(current/max)	
	Number of packets per second (current/maximum)	

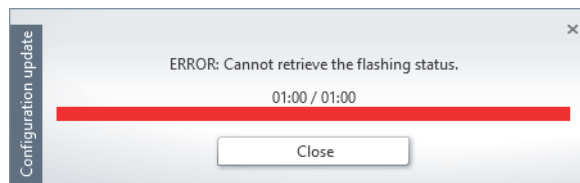
^{*1} This item is displayed when CIP Safety Configuration Tool with the software version "1.3.0.28" or later is used.

- LEDs during configuration writing

Status of writing configuration	RUN LED	ERR LED	MS LED	NS LED
Writing	Off	Off	Flashing (orange) (in 1 to 2s intervals)	Flashing (orange) (in 1 to 2s intervals)
Writing completed			Flashing (green)	Flashing (green)
Writing failed			Flashing (red) (in 500ms intervals)	Flashing (red) (in 500ms intervals)

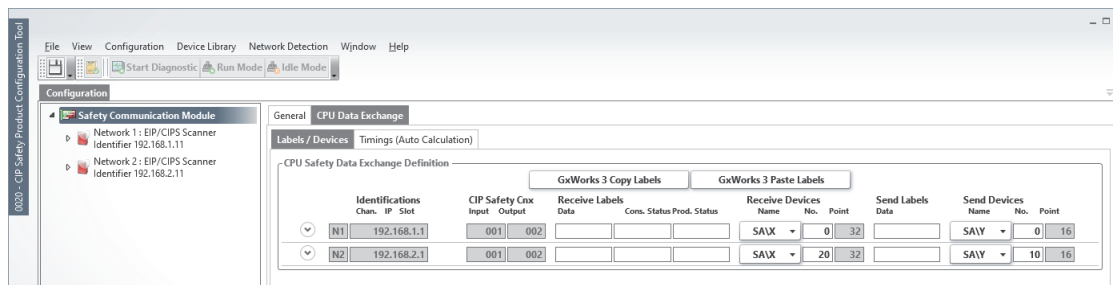
Point

- Do not reset the CPU module or power off and on the system until the MS LED and NS LED start flashing in green. Doing so may cause a failure of the CIP Safety module, and the configuration may not be written again.
- The LED status during configuration writing is not reflected on the "Module Diagnostics" window of the engineering tool.
- Configuration is not written if communications with the CIP Safety module cannot be established due to an incorrect target IP address or another reason. Check the connection with the CIP Safety module.
- Communications end if configuration writing is executed during standard communications or safety communications.
- After the configuration is written, the NS LED indication may change due to a factor such as communication status change. In such a case, judge the writing status by the LED status such as MS LED.
- The flash status may not be acquired. In such a case, judge the writing status by the LED status such as MS LED.



■[CPU Data Exchange] tab

- [Labels/Devices] tab



Item			Description
CPU Safety Data Exchange Definition	Identifications	Chan.	Displays the specified port number.
		IP Slot	<ul style="list-style-type: none"> • Target connection: The specified instance number and tag name are displayed. • Originator connection: The IP address and slot information of the target device are displayed.
	CIP Safety Cnx	Input	Displays the consumer-side connection number (the identifier of the connection managed in the tool).
		Output	Displays the producer-side connection number (the identifier of the connection managed in the tool).
	Receive Labels	Data	Set the label name of the input data inside the receive device.
		Cons. Status	Set the label name of the consumer safety connection status inside the receive device.
		Prod. Status	Set the label name of the producer safety connection status inside the receive device.
	Receive Devices	Name	Set the receive device.
		No.	
		Point	Set the number of assigned points on the receive device.
	Send Labels	Data	Set the label name of the send device.
	Send Devices	Name	Set the send device.
		No.	
		Point	Set the number of assigned points on the send device.
	GxWorks 3 Copy Labels		Copies the contents of "Receive Labels" and "Send Labels" into the clipboard in a format that allows the information to be pasted on a global label in the engineering tool.
	GxWorks 3 Paste Labels ^{*1}		Pastes the content copied into the clipboard with the global labels of the engineering tool to the Labels (Receive) and Labels (Send).

^{*1} This item is displayed when CIP Safety Configuration Tool with the software version "1.3.0.28" or later is used.

Precautions

When setting a receive device or send device, note the following points.

- Be sure that the settings are within the device setting range specified with CPU module parameters.
- Avoid duplicating the assignment of the safety device.
- When the safety device is out of the range or an assignment is duplicated, the relevant items are framed in red and changes to other safety devices are locked. However, if the destination safety device does not have enough room when the user tries to change the safety device type, the assignment is returned to the safety device that was selected before the operation. (An error message will be displayed if the project is attempted to be saved in the red frame state.)*¹
- Assignment of the safety device should not be duplicated with safety devices used for other modules. When duplicated, a red frame is not displayed but an error is displayed when the parameters are saved.
- If one-way communication is set in the assignment of the safety device, one word is assigned for the safety device (send and receive) in the unused direction.*²

*1 This item is displayed in a red frame when CIP Safety Configuration Tool with the software version "1.2.0.3" is used. (If the project is saved while a red frame is displayed, the values set before the red frame is displayed are saved instead of the current values.)

*2 If the software version of CIP Safety Configuration Tool is "1.2.0.3", an unused area whose size is the same as the communication used is assigned for the safety device (send and receive) in the unused direction.

Ex.

Assignment when setting a target connection

Software version	[Safety Target (Class0)] tab settings			[CPU Data Exchange] tab settings				Assignment of the safety device	
	Item	Direction	Size	Receive Device	Point	Send Device	Point	Receive Device	Send Device
"1.2.0.3"	Target (Class0 Instance) definitions* ³	T->O	14	SAID0	7	SAIW0	7	• SAID0: System area • SAID1 to 6: Unused area	SAIW0 to 6: Send data
		O->T	14	SAID0	8	SAIW0	8	• SAID0: System area • SAID1 to 7: Receive data	SAIW0 to 7: Unused area
"1.3.0.28" or later	Target (Class0 Instance) definitions* ³	T->O	14	SAID0	2	SAIW0	7	• SAID0: System area • SAID1: Unused area	SAIW0 to 6: Send data
		O->T	14	SAID0	8	SAIW0	1	• SAID0: System area • SAID1 to 7: Receive data	SAIW0: Unused area

*3 Assigned the same way during tag communications setting.

Ex.

Assignment when setting an originator connection

Software version	[Safety Settings] tab ⇨ [Safety Connections] tab settings				[CPU Data Exchange] tab settings				Assignment of the safety device	
	Input Format	Safety Input	Output Format	Safety Output	Receive Device	Point	Send Device	Point	Receive Device	Send Device
"1.2.0.3"	Safety Input Assembly* ⁴	14	Safety Output Assembly	8	SAID0	8	SAIW0	4	• SAID0: System area • SAID1 to 7: Receive data	SAIW0 to 3: Send data
		14	None	Not settable	SAID0	8	SAIW0	8	• SAID0: System area • SAID1 to 7: Receive data	SAIW0 to 7: Unused area
"1.3.0.28" or later	Safety Input Assembly* ⁴	14	Safety Output Assembly	8	SAID0	8	SAIW0	4	• SAID0: System area • SAID1 to 7: Receive data	SAIW0 to 3: Send data
		14	None	Not settable	SAID0	8	SAIW0	1	• SAID0: System area • SAID1 to 7: Receive data	SAIW0: Unused area

*4 Assigned the same way during tag communications setting.

- GxWorks3 Copy labels and GxWorks3 Paste labels

Ex.

The changed data can be pasted to the global label in the engineering tool (GX Works3) when the settings are changed with CIP Safety Configuration Tool.

1. Click the [GxWorks 3 Copy Labels] button in CIP Safety Configuration Tool.

2. Paste the changed data to the global label in the engineering tool (GX Works3).

	Label Name	Data Type		Class	Assign (Device/Label)
1	cip_label1	Bit(0..15)	...	VAR_GLOBAL	SA\X10
2	cip_label2	Bit	...	VAR_GLOBAL	SA\X0
3	cip_label3	Bit	...	VAR_GLOBAL	SA\X8
4	cip_label4	Bit(0..15)	...	VAR_GLOBAL	SA\Y0

Ex.

The set project configured in CIP Safety Configuration Tool can be pasted into another project in CIP Safety Configuration Tool.

1. Click the [GxWorks 3 Copy Labels] button in CIP Safety Configuration Tool.

2. Click the [GxWorks 3 Paste Labels] button in CIP Safety Configuration Tool of the copy destination.

3. The project of the copy source will be pasted.

Ex.

Using a spreadsheet tool such as Excel, the calculated results of the device offset can be pasted into CIP Safety Configuration Tool.

1. Click the [GxWorks 3 Copy Labels] button in CIP Safety Configuration Tool.

Receive Labels					Receive Devices			Send Labels					Send Devices		
Data	Cons.	Status	Prod.	Status	Name	No.	Point	Data	Cons.	Status	Prod.	Status	Name	No.	Point
cip_Label1					SA\X	0	32	cip_Label4					SA\Y	0	16
cip_Label5					SA\X	20	32	cip_Label8					SA\Y	10	16

2. Paste it into Excel.

cip_Label1	Bit(0..15)	VAR_GLOBAL	SAIX10
cip_Label2	Bit	VAR_GLOBAL	SAIX0
cip_Label3	Bit	VAR_GLOBAL	SAIX8
cip_Label4	Bit(0..15)	VAR_GLOBAL	SAIY0
cip_Label5	Bit(0..15)	VAR_GLOBAL	SAIX30
cip_Label6	Bit	VAR_GLOBAL	SAIX20
cip_Label7	Bit	VAR_GLOBAL	SAIX28
cip_Label8	Bit(0..15)	VAR_GLOBAL	SAIY10

3. Copy the calculated results into the clipboard.

cip_Label1	Bit(0..15)	VAR_GLOBAL	SAIX10
cip_Label2	Bit	VAR_GLOBAL	SAIX0
cip_Label3	Bit	VAR_GLOBAL	SAIX8
cip_Label4	Bit(0..15)	VAR_GLOBAL	SAIY0
cip_Label5	Bit(0..15)	VAR_GLOBAL	SAIX110
cip_Label6	Bit	VAR_GLOBAL	SAIX100
cip_Label7	Bit	VAR_GLOBAL	SAIX108
cip_Label8	Bit(0..15)	VAR_GLOBAL	SAIY10

4. With the results copied to the clipboard, click the [GxWorks 3 Paste Labels] button in CIP Safety Configuration Tool.

Receive Labels					Receive Devices			Send Labels					Send Devices		
Data	Cons.	Status	Prod.	Status	Name	No.	Point	Data	Cons.	Status	Prod.	Status	Name	No.	Point
cip_Label1					SA\X	0	32	cip_Label4					SA\Y	0	16
cip_Label5					SA\X	20	32	cip_Label8					SA\Y	10	16

5. The calculated results will be pasted into CIP Safety Configuration Tool.

Receive Labels					Receive Devices			Send Labels					Send Devices		
Data	Cons.	Status	Prod.	Status	Name	No.	Point	Data	Cons.	Status	Prod.	Status	Name	No.	Point
cip_Label1					SA\X	0	32	cip_Label4					SA\Y	0	16
cip_Label5					SA\X	100	32	cip_Label8					SA\Y	10	16

Precautions

When pasting labels of GX Works3, note the following.

- Use one-byte alphanumeric characters for label names.
- Follow the input character rules of the global label in the engineering tool (GX Works3). (📖 GX Works3 Operating Manual)
- When pasting, the data type (data size) of the global label is not reflected. For the data size, the connection setting in CIP Safety Configuration Tool are used.

	Label Name	Data Type		Class	Assign (Device/Label)
1	cip_label1	Bit(0..15)	...	VAR_GLOBAL	SA\X10
2	cip_label2	Bit	...	VAR_GLOBAL	SA\X0
3	cip_label3	Bit	...	VAR_GLOBAL	SA\X8
4	cip_label4	Bit(0..15)	...	VAR_GLOBAL	SA\Y0

- When pasting, the fragmentation of data in the input connection status area and in the receiving device area are not detected. Set in a range where the data is not fragmented. The definition of "not fragmented" is that the producer status bit is offset by 8 bits, and the receive data is offset by 16 bits, starting from the consumer status bit as an origin, as shown below.

Data	Offset
Cons. status bit	0 bits (0 bytes)
Prod. Status bit	8 bits (1 byte)
Receive data	16 bits (2 bytes)

■Example of fragmentation

	Label Name	Data Type		Class	Assign (Device/Label)
1	cip_label1	Bit(0..15)	...	VAR_GLOBAL	SA\X20
2	cip_label2	Bit	...	VAR_GLOBAL	SA\X0
3	cip_label3	Bit	...	VAR_GLOBAL	SA\X8
4	cip_label4	Bit(0..15)	...	VAR_GLOBAL	SA\Y0

■Example of no fragmentation

	Label Name	Data Type		Class	Assign (Device/Label)
1	cip_label1	Bit(0..15)	...	VAR_GLOBAL	SA\X10
2	cip_label2	Bit	...	VAR_GLOBAL	SA\X0
3	cip_label3	Bit	...	VAR_GLOBAL	SA\X8
4	cip_label4	Bit(0..15)	...	VAR_GLOBAL	SA\Y0

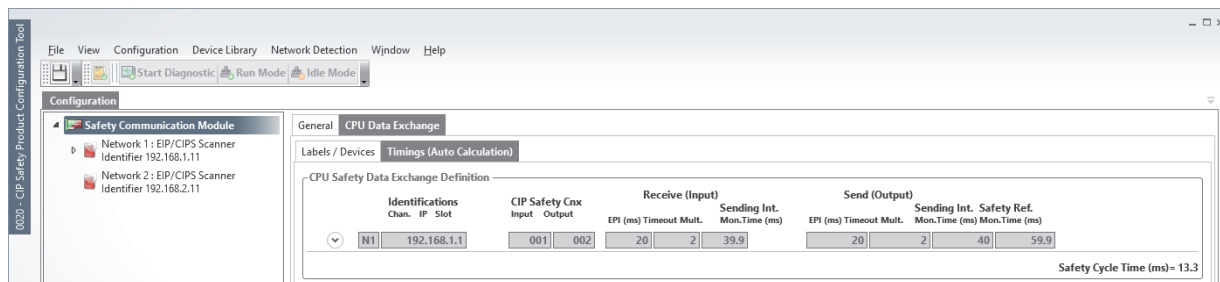
- When pasting, set the class to VAR_GLOBAL. Otherwise, a warning will be displayed.

	Label Name	Data Type		Class	Assign (Device/Label)
1	cip_label1	Bit(0..15)	...	VAR_GLOBAL	SA\X10
2	cip_label2	Bit	...	VAR_GLOBAL	SA\X0
3	cip_label3	Bit	...	VAR_GLOBAL	SA\X8
4	cip_label4	Bit(0..15)	...	VAR_GLOBAL	SA\Y0

■Example of CIP Safety Configuration Tool's warning message

Level	Date / Time	
Warning	Apr 27, 2023 02:16:04.868 PM(+09:00)	On pasted line 1: Expected: VAR_GLOBAL Received: for field number 3


- [Timings (Auto Calculation)] tab



Item			Description
CPU Safety Data Exchange Definition	Identifications	Chan.	Displays the specified port number.
		IP Slot	<ul style="list-style-type: none">• Target connection: The specified instance number and tag name are displayed.• Originator connection: The IP address and slot information of the target device are displayed.
	CIP Safety Cnx	Input	Displays the consumer-side connection number (the identifier of the connection managed in the tool).
		Output	Displays the producer-side connection number (the identifier of the connection managed in the tool).
	Receive (Input)	EPI (ms)	<ul style="list-style-type: none">• Originator connection: The input-side EPI specified for the corresponding connection is displayed.• Target connection: The estimated value of the input-side EPI specified for the corresponding connection is specified.
		Timeout Mult.	<ul style="list-style-type: none">• Originator connection: The input-side timeout multiplier specified for the corresponding connection is displayed.• Target connection: The estimated value of the input-side timeout multiplier for the corresponding connection is specified.
		Sending Int. Mon. Time	Displays the transmission interval (in ms) of safety data to be sent from the CIP Safety module to the CPU module. The value is calculated automatically from the parameter setting values.
	Send (Output)	EPI (ms)	<ul style="list-style-type: none">• Originator connection: The output-side EPI specified for the corresponding connection is displayed.• Target connection: The estimated value of the output-side EPI specified for the corresponding connection is specified.
		Timeout Mult.	<ul style="list-style-type: none">• Originator connection: The output-side timeout multiplier specified for the corresponding connection is displayed.• Target connection: The estimated value of the output-side timeout multiplier for the corresponding connection is specified.
		Sending Int. Mon. Time	Displays the transmission interval (in ms) of safety data to be sent from the CPU module to the CIP Safety module. The value is calculated automatically from the parameter setting values.
		Safety Ref. Mon. Time	Displays the monitoring time (in ms) used to check the safety data receiving interval between the CIP Safety module and the CPU module. The value is calculated automatically from the parameter setting values.
Safety Cycle Time (ms)		Displays the recommended value (in ms) of the safety cycle time for the CPU module. The value is calculated automatically from the parameter setting values.	

CIP options

Displays the option window of CIP Safety Configuration Tool.

 [Configuration] ⇒ [CIP OPTIONS]

CIP OPTIONS

Display in Tree view: Catalog ▾

Display CIP Identifier in Tree view: ☒

Display Version in Tree view: ☒

Upload EDS from device during Network Detection: ☒

Advanced Mode: ☐

Ok

Item	Description	Default
Display in Tree view	Set whether tree items (for example, in the configuration view or device library view) display catalog names or product names from the EDS file.	Catalog
Display CIP Identifier in Tree view	Set whether to display the CIP identifier of each device in the configuration view.	Selected
Display Version in Tree view	Set whether to display the version of each device in the configuration view.	Selected
Upload EDS from device during Network Detection	Set whether to upload EDS files from devices during network detection.	Selected
Advanced Mode ^{*1}	Select this mode only when performing CIP Safety communications with specific products manufactured by other companies. Do not select this mode in any other case. Selecting this mode changes parameters of Ping Interval EPI Multiplier for CIP Safety communications. For details, please consult your local Mitsubishi representative.	Not selected

^{*1} This item is displayed when CIP Safety Configuration Tool with the software version "1.3.0.28" or later is used.

Network 1: EIP/CIPS Scanner, Network 2: EIP/CIPS Scanner

■[General] tab

The screenshot displays the 'General' tab of the CIP Safety Configuration Tool. The left sidebar shows the 'Safety Communication Module' with two networks: 'Network 1: EIP/CIPS Scanner Identifier 192.168.1.11' and 'Network 2: EIP/CIPS Scanner Identifier 192.168.2.11'. The main area contains the following configuration sections:

- Scanner IP Address Settings:** IP Address (Detect, 192.168.1.11), Subnet Mask (255.255.255.0), Network Gateway (0.0.0.0).
- DNS Server:** Primary DNS Server Address (0.0.0.0), Secondary DNS Server Address (0.0.0.0).
- Module Name:** Host Name, Domain Name.
- Ports Settings:** Port 1 baud rate (auto negotiation), Port 2 baud rate (auto negotiation).
- DLR Supervisor Configuration:** Ring Supervisor Enabled (checkbox), Ring Supervisor Precedence (0), Beacon Interval (400 μs), Beacon Timeout (1960 μs), DLR VLAN ID (0).
- Ping:** Send Ping, Loop, Stop on error, Clear message log.
- Operating Mode:** Target (Class 1), Safety Target (Class 0).
- Configuration Summary:** Number of Class 1 connections (current / max): 0 / 64.

Item		Description
Scanner IP Address Settings	IP Address	Set the IP address.
	Subnet Mask	Set the subnet mask.
	Network Gateway	Set the network gateway. (Only Network 1: EIP/CIPS Scanner can be set.)
DNS Server	Primary DNS Server Address	Set the primary DNS server address.
	Secondary DNS Server Address	Set the secondary DNS server address.
Module Name	Host Name	Set the host name.
	Domain Name	Set the domain name.
Ports Settings	Port 1 baud rate	Set the P1-side port baud rate.
	Port 2 baud rate	Set the P2-side port baud rate.
DLR Supervisor Configuration ^{*2}	Ring Supervisor Enabled	Set whether to enable or disable the ring supervisor.
	Ring Supervisor Precedence	Set the priority of the ring supervisor.
	Beacon Interval	Set the beacon interval.
	Beacon Timeout	Set the beacon timeout.
	DLR VLAN ID	Set the DLR VLAN ID.
Ping	Send Ping	Sends a Ping request.
	Loop	Repeatedly sends Ping requests.
	Stop on error	Stops sending Ping requests when an error occurs.
	Clear message	Clears Ping logs.

Item		Description
Operating Mode	Target (Class1)	Configure the settings to be used in Class1 communications. When this item is selected, the [Target (Class1)] tab is added so that the following definitions can be added or deleted. (Page 67 [Target (Class1)] tab) <ul style="list-style-type: none"> Target (Class1 Instance) definitions Target (Class1 Tag) definitions
	Safety Target (Class0)	Configure the settings to be used in Class0 communications. When this item is selected, the [Safety Target (Class0)] tab is added so that the following definitions can be added or deleted. (Page 68 [Safety Target (Class0)] tab) <ul style="list-style-type: none"> Target (Class0 Instance) definitions Target (Class0 Tag) definitions
Configuration Summary* ¹	Maximum Number of Standard Connections	Displays the information of an appropriate item.
	Number of Standard Connections	
	Maximum Number of Safety Connections	
	Number of Safety Connections	
	Maximum Number of Packets Per Second	
	Number of Packets Per Second	
Configuration Summary* ²	Number of Class 1 connections (current/maximum)	Displays the information of appropriate items.

*1 This item is displayed when the CIP Safety Configuration Tool with the software version "1.2.0.3" is used.

*2 This item is displayed when CIP Safety Configuration Tool with the software version "1.3.0.28" or later is used.

■[Safety] tab

Configuration

Safety Communication Module

Network 1 : EIP/CIPS Scanner Identifier 192.168.1.11

Network 2 : EIP/CIPS Scanner Identifier 192.168.2.11

General Safety I/O Mapping Information IP/Port DLR Comment

Identification

Scanner CIP Identifier: 192.168.1.11

Safety Network Number: 4856_000E_F67D

Edit

Copy

Paste

Set TUNID

Safety Reset

Safety Reset

Signature in SNCT

ID: ###

Date: ###

Time: ### ms

Signature in Scanner

ID: ###

Date: ###

Time: ### ms

Refresh

Safety Lock/Unlock

Locking prevents configuration download and safety reset

Lock Scanner

Unlock Scanner

Change Mode

Allow to set Idle state or Executing state. Executing state will start the I/O exchange data between the scanner and the devices.

Set Idle State


Set Executing State

Item		Description
Identification	Scanner CIP Identifier	Displays the scanner identifier.
	Safety Network Number	Displays the Safety Network Number. Click the [Edit] button to change to any value manually or on a time basis. Also, Copy and Paste can be used.
	Set TUNID	Set the TUNID ^{*1} on the corresponding device.
Safety Reset	Safety Reset	Executes the reset.
Signature in SNCT	ID	Displays the ID in SNCT.
	Date	Displays the date in SNCT.
	Time	Displays the time in SNCT.
Signature in Scanner	ID	Gets and displays the ID from the device.
	Date	Gets and displays the date from the device.
	Time	Gets and displays the time from the device.
	[Refresh] button	ID, Date, and Time are displayed and whether they match the signature in the SNCT can be checked.
Safety Lock/Unlock	Lock Scanner	Prevents configuration downloads and Safety Reset.
	Unlock Scanner	Cancels the prevention of configuration downloads and Safety Reset.
Change Mode	Set Idle State	Enables the Idle state.
	Set Executing State	Enables the Executing state.

*1 This value is the combination of Scanner CIP Identifier and Safety Network Number and is a specific identifier for identifying devices on the network.

Point

The target device checks if the following TUNIDs match when it receives a connection open request from the originator. For this reason, the TUNID of the target and originator must match.

- (1): TUNID set on the own station (target) (above items)
- (2): TUNID included in the connection request from the originator ( Page 77 [Safety Settings] tab)

In the CIP Safety module, (1) is reflected by the [Set TUNID] button and (2) is reflected by the [Save configuration to module] button. When the target is the CIP Safety module, setting the TUNID using the [Set TUNID] button in this item is recommended.

60

7 CIP Safety Configuration Tool
7.2 Window Structure

- Safety Reset behavior during communications

Communication type			Behavior
Standard communication	Class1 communications	Instance communications	Finishes communications and executes Safety Reset.
		Tag communications	
	UCMM communications	Message communications	
Safety communications	Class0 communications	Instance communications	Continues communications. Safety Reset fails, causing an error.
		Tag communications	

Point

- When the firmware version of the CIP Safety module is "01", do not reset the CPU module or power off and on the system until the MS LED lights up in green and other LEDs are turned off.
- When the firmware version of the CIP Safety module is "02", do not reset the CPU module or power off and on the system until the MS LED lights up in red and other LEDs are turned off.
- When Reset Type 1 is selected or when "Preserve Soft-set MacId" is not selected for Reset Type 2, the IP address of the CIP Safety module is also cleared. Therefore, the configuration must be reset.
- Executing Safety Reset will cause an error (2450H: module major error) on the CPU module. Confirm that stopping the system will not cause any problems before execution.
- The LED status during Safety Reset is not reflected to the Module Diagnostics window of the engineering tool.
- Reset is not executed when communication with the CIP Safety module cannot be established due to an incorrect target IP address or for other reasons. Check the connection with the CIP Safety module.

■[I/O Mapping] tab

- [General] tab

The description of the item is displayed when a communication destination device (target device) is selected.

Configuration

Safety Communication Module

- Network 1: EIP/CIPS Scanner Identifier 192.168.1.11
- Network 2: EIP/CIPS Scanner Identifier 192.168.2.11

General Safety I/O Mapping Information IP/Port DLR Comment

Standard Safety

Set Manual to All Set Automatic to All Recalculate the Offsets

Input

ID	CIP Identifier	Slot	Size	Connection	Offset	Offset Calculation
----	----------------	------	------	------------	--------	--------------------

Output

ID	CIP Identifier	Slot	Size	Connection	Offset	Offset Calculation
----	----------------	------	------	------------	--------	--------------------

Item	Description
Input	Lists the information of specified devices.
Output	When using the auto refresh setting, set "Offset Calculation" to "Automatic".

- [Safety] tab

Configuration

Safety Communication Module

- Network 1: EIP/CIPS Scanner Identifier 192.168.1.11
- Network 2: EIP/CIPS Scanner Identifier 192.168.2.11

General Safety I/O Mapping Information IP/Port DLR Comment

Standard Safety

Set Manual to All Set Automatic to All Recalculate the Offsets

Input

ID	CIP Identifier	Slot	Size	Connection
----	----------------	------	------	------------

Output

ID	CIP Identifier	Slot	Size	Connection
----	----------------	------	------	------------

Item	Description
Input	Lists the information of specified devices.
Output	

■[Information] tab

Configuration

Safety Communication Module

Network 1 : EIP/CIPS Scanner
Identifier 192.168.1.11

Network 2 : EIP/CIPS Scanner
Identifier 192.168.2.11

General

Safety

I/O Mapping

Information

IP/Port

DLR

Comment

Identification

Vendor ID: ###

Product Type: ###

Product Code: ###

Product Name: ###

Software Revision: ###

Manufacturer Serial Number: ###

State

Major Fault: ###

Minor Fault: ###

State: ###

CIP Identifier, SNN: ###

Lock State: ###

Configuration Owning UNID: ###

Exception Status

Alarm Device Common

Alarm Device Specific

Alarm Manufacturer Specific

Warning Device Common

Warning Device Specific

Warning Manufacturer Specific

Refresh

Item		Description
Identification	Vendor ID	Displays the information of an appropriate item.
	Product Type	
	Product Code	
	Product Name	
	Software Revision	
	Manufacturer Serial Number	
State	Major Fault	Displays the information of an appropriate item.
	Minor Fault	
	State	
	CIP Identifier, SNN	
	Lock State	
	Configuration Owning UNID	
Exception Status	Alarm Device Common	Displays the status of an appropriate item as an LED status.
	Alarm Device Specific	
	Alarm Manufacturer Specific	
	Warning Device Common	
	Warning Device Specific	
	Warning Manufacturer Specific	

■[IP/Port] tab

The screenshot shows the 'IP/Port' configuration tab in the CIP Safety Configuration Tool. The left sidebar lists the 'Safety Communication Module' and two network identifiers: 'Network 1 : EIP/CIPS Scanner Identifier 192.168.1.11' and 'Network 2 : EIP/CIPS Scanner Identifier 192.168.2.11'. The main configuration area is divided into two main sections: 'TCP/IP Parameters' and 'Port Configuration And Diagnostic'. The 'TCP/IP Parameters' section includes 'Configuration Control' (Startup Configuration), 'Interface Configuration' (IP Address, Network Mask, Gateway Address, DNS Primary Server, DNS Secondary Server, Domain Name), 'Host Name' (Name), 'Last Address Conflict State' (Interface Config State, Conflicting MAC), 'Multicast TTL' (TTL Value), and 'TCP Timeout' (Encapsulation Inactivity Timeout (Sec)). Each of these sections has 'Apply' and 'Refresh' buttons. The 'Port Configuration And Diagnostic' section is a table with columns: Name, Negotiation Status, Link, Speed, Duplex, Change, and Diagnostics. It has a 'Refresh' button at the bottom right.

Item			Description
TCP/IP Parameters	Configuration Control	Startup Configuration	The information of each item can be displayed, applied, or refreshed.
	Interface Configuration	IP Address	
		Network Mask	
		Gateway Address	
		DNS Primary Server	
		DNS Secondary Server	
		Domain Name	
	Host Name	Name	
	Last Address Conflict State	Interface Config State	
		Conflicting MAC	
	Multicast TTL	TTL Value	
	TCP Timeout	Encapsulation Inactivity Timeout (Sec)	
Port Configuration And Diagnostic	Name		Displays the information of an appropriate item. Click the [Refresh] button to get and display the information of each item from the actual machine.
	Negotiation Status		
	Link		
	Speed		
	Duplex		
	Change		Set the Ethernet port.
	Diagnostics		The following Ethernet counters can be displayed and cleared: <ul style="list-style-type: none"> • Interface Counters • Media Counters

■[DLR] tab

The screenshot shows the CIP Safety Configuration Tool interface. The left sidebar lists the 'Safety Communication Module' with two networks: 'Network 1 : EIP/CIPS Scanner Identifier 192.168.3.51' and 'Network 2 : EIP/CIPS Scanner Identifier 192.168.0.5'. The main window has tabs for 'General', 'Safety', 'I/O Mapping', 'Information', 'IP/Port', 'DLR', and 'Comment'. The 'DLR' tab is active, displaying various configuration fields:

- DLR Section:**
 - Network Topology: Linear
 - Network Status: Normal
- Capabilities Section:**
 - Announce-based Ring Node: ☐
 - Beacon-based Ring Node: ☒
 - Supervisor Capable: ☒
- Active Supervisor Address Section:**
 - Supervisor IP: 0.0.0.0
 - Supervisor MAC: 00:00:00:00:00:00
- DLR Supervisor Section:**
 - Buttons: Verify Fault Location, Clear Rapid Fault, Restart Sign On
 - Ring Supervisor Status: Cannot Support Parameters
- Supervisor Configuration Section:**
 - Ring Supervisor Enable: ☐
 - Ring Supervisor Precedence: 0
 - Beacon Interval: 400 μs
 - Beacon Timeout: 1960 μs
 - DLR VLAN ID: 0
 - Buttons: Apply, Refresh
- Ring Fault Count Section:**
 - Ring Fault Count: ###
 - Buttons: Clear, Refresh
- Last Active Node Section:**
 - Port 1: [Field]
 - Port 2: [Field]
- Ring Participants List Section:**
 - Table with columns: IP Address, MAC Address
 - Active Supervisor Precedence: ###
 - Button: Refresh

7

Item		Description
DLR	Network Topology	Displays the information of an appropriate item.
	Network Status	
Capabilities	Announce-based Ring Node	
	Beacon-based Ring Node	
	Supervisor Capable	
Active Supervisor Address	Supervisor IP	
	Supervisor MAC	
DLR Supervisor ^{*1}	Ring Supervisor Status	Displays menu items including [Verify Fault Location], [Clear Rapid Fault], and [Restart Sign On].
Supervisor Configuration ^{*1}	Ring Supervisor Enabled	The information of each item can be displayed, applied, or refreshed. Click the [Refresh] button to get and display the information of each item from the actual machine.
	Ring Supervisor Precedence	
	Beacon Interval	
	Beacon Timeout	
	DLR VLAN ID	
Ring Fault Count ^{*1}	Ring Fault Count	The information of each item can be displayed, cleared, or refreshed. Click the [Refresh] button to get and display the information of items from the actual machine.
Last Active Node ^{*1}	Port 1 ^{*2}	Displays the information of an appropriate item. Click the [Refresh] button to get and display the information of each item from the actual machine.
	Port 2 ^{*3}	
Ring Participants List ^{*1}	IP Address	
	MAC Address	
Active Supervisor Preference ^{*1}		

^{*1} This item is displayed when CIP Safety Configuration Tool with the software version "1.3.0.28" or later is used.

^{*2} Read the term as P1-A and P2-A in the CIP Safety module.

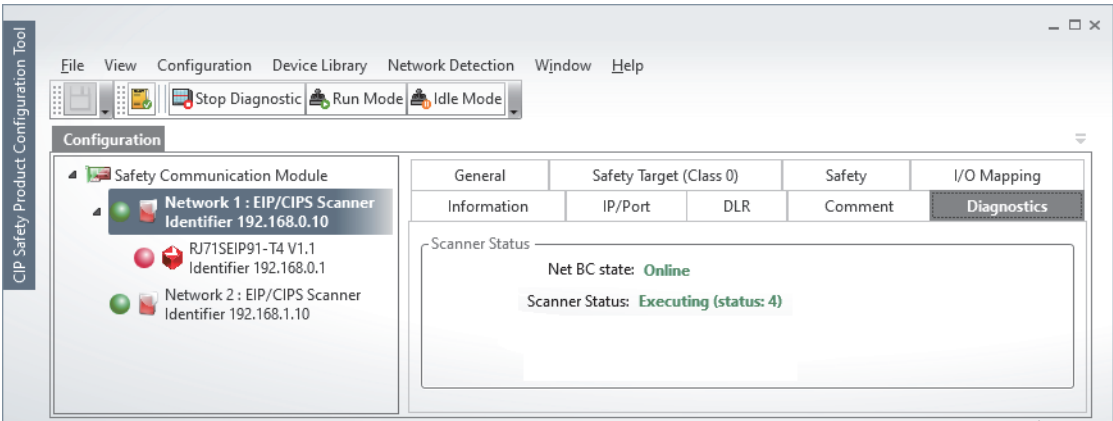
^{*3} Read the term as P1-B and P2-B in the CIP Safety module.

■[Comment] tab

Comments can be entered.

■[Diagnostics] tab

This tab is displayed only during diagnostics.



Item		Description
Scanner Status	Net BC state	Displays the information of an appropriate item only during diagnostics.
	Scanner Status	

■[Target (Class1)] tab

Configuration

Safety Communication Module

Network 1 : EIP/CIPS Scanner
Identifier 192.168.1.11

Network 2 : EIP/CIPS Scanner
Identifier 192.168.2.11

General

Target (Class 1)

Safety

I/O Mapping

Information

IP/Port

DLR

Comment

Target (Class 1 Instance) definitions

Add

Remove

Connection:

T->O Size

O->T Size

Active on startup

1

256

256

☒

Target (Class 1 Tag) definitions

Add

Remove

Name

T->O Size

Active on startup

MyClass1Tag1

2

☒

(O means Originator so it is an external scanner that will connect to the local slave - T means Target so this is the local slave)

Item		Description
Target (Class1 Instance) definitions	Add	Adds a target definition.
	Remove	Removes a target definition.
	Connection	Displays the connection.
	T->O Size	Set the T->O size.
	O->T Size	Set the O->T size.
	Active on startup ^{*1}	Set whether to be active on startup.
Target (Class1 Tag) definitions	Add	Adds a target definition.
	Remove	Removes a target definition.
	Name	Set the tag name.
	T->O Size	Set the T->O size.
	Active on startup ^{*1}	Set whether to be active on startup.

^{*1} This setting value is reflected to 'Reserved station (Class1)' (Un\G99440 to Un\G99447, Un\G1148016 to Un\G1148023). Selecting the checkbox sets no reserved station and clearing the checkbox sets a reserved station.

■[Safety Target (Class0)] tab

Configuration

Safety Communication Module

Network 1 : EIP/CIPS Scanner
Identifier 192.168.1.11

Network 2 : EIP/CIPS Scanner
Identifier 192.168.2.11

General

Target (Class 1)

Safety Target (Class 0)

Safety

I/O Mapping

Information

IP/Port

DLR

Comment

Target (Class 0 Instance) definitions

Add

Remove

Direction	Instance	Size	Max Subscribers
T->O	528	14	1

Target (Class 0 Tag) definitions

Add

Remove

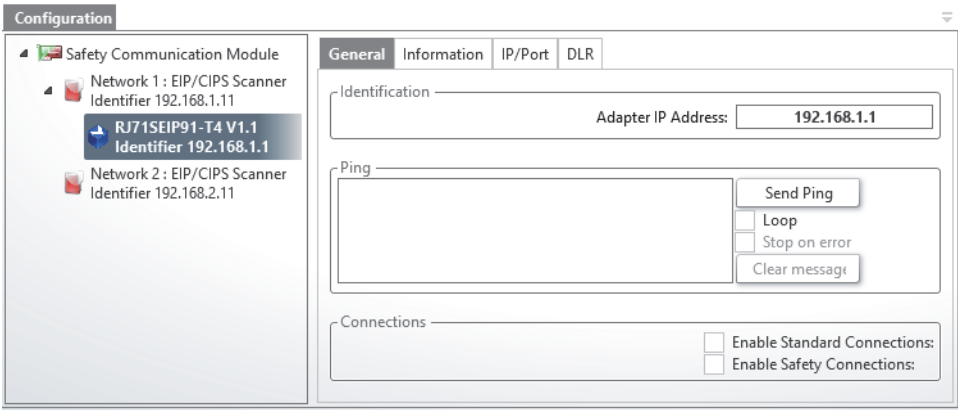
Direction	Name	Tag Size	Max Subscribers
T->O	MyClass0Tag1	14	1

(O means Originator so it is an external scanner that will connect to the local slave - T means Target so this is the local slave)

Item		Description
Target (Class0 Instance) definitions	Add	Adds a target definition.
	Remove	Removes a target definition.
	Direction	Set the communication direction (T->O or O->T).
	Instance	Set the instance number. (Value range: 528 to 767)
	Size	Set the size.
	Max Subscribers	Set the maximum number of concurrent connections for multicast communications. This item is available only when the direction is T->O.
Target (Class0 Tag) definitions	Add	Adds a target definition.
	Remove	Removes a target definition.
	Direction	Set the communication direction (T->O or O->T).
	Name	Set the tag name.
	Tag Size	Set the size.
	Max Subscribers	Set the maximum number of concurrent connections for multicast communications. This item is available only when the direction is T->O.

When a communication destination device (target device) is selected

■[General] tab



Item		Description
Identification	Adapter IP Address	Set the IP address of the target device.
Ping	Send Ping	Sends a Ping request.
	Loop	Repeatedly sends Ping requests.
	Stop on error	Stops sending Ping requests when an error occurs.
	Clear message	Clears Ping logs.
Connections	Enable Standard Connections	Configure the settings to be used in standard communications (Class1 communications). Select this item to add the [Standard Settings] tab to enable the Class1 communications setting. (☞ Page 74 [Standard Settings] tab)
	Enable Safety Connections	Configure the settings to be used in safety communications (Class0 communications). Select this item to add the [Safety Settings] tab to enable the Class0 communications setting. (☞ Page 77 [Safety Settings] tab)

■[Information] tab

Configuration

Safety Communication Module

Network 1 : EIP/CIPS Scanner
Identifier 192.168.1.11

RJ71SEIP91-T4 V1.1
Identifier 192.168.1.1

Network 2 : EIP/CIPS Scanner
Identifier 192.168.2.11

GeneralInformationIP/PortDLR

Identification

Vendor ID: ###

Product Type: ###

Product Code: ###

Product Name: ###

Software Revision: ###

Manufacturer Serial Number: ###

State

Major Fault: ###

Minor Fault: ###

State: ###

CIP Identifier, SNN: ###

Lock State: ###

Configuration Owning UNID: ###

Exception Status

☐ Alarm Device Common

☐ Alarm Device Specific

☐ Alarm Manufacturer Specific

☐ Warning Device Common

☐ Warning Device Specific

☐ Warning Manufacturer Specific

Output Connections Owner

Resource

UID

Refresh

Item		Description
Identification	Vendor ID	Displays the information of an appropriate item.
	Product Type	
	Product Code	
	Product Name	
	Software Revision	
	Manufacturer Serial Number	
State	Major Fault	
	Minor Fault	
	State	
	CIP Identifier, SNN	
	Lock State	
	Configuration Owning UNID	
Exception Status	Alarm Device Common	Displays the status of an appropriate item as an LED status.
	Alarm Device Specific	
	Alarm Manufacturer Specific	
	Warning Device Common	
	Warning Device Specific	
	Warning Manufacturer Specific	
Output Connections Owner	Resource	Displays the information of an appropriate item.
	UID	
[Refresh] button		Gets and displays the information of each item from the actual machine.

70

7 CIP Safety Configuration Tool

7.2 Window Structure

■[IP/Port] tab

The screenshot displays the 'Configuration' window of the CIP Safety Configuration Tool, specifically the 'IP/Port' tab. The left sidebar shows a tree structure with 'Safety Communication Module' expanded, containing 'Network 1: EIP/CIPS Scanner Identifier 192.168.1.11' and 'Network 2: EIP/CIPS Scanner Identifier 192.168.2.11'. The 'RJ71SEIP91-T4 V1.1 Identifier 192.168.1.1' is selected. The main area has tabs for 'General', 'Information', 'IP/Port', and 'DLR'. The 'IP/Port' tab is active, showing 'TCP/IP Parameters'. It includes sections for 'Configuration Control' (Startup Configuration dropdown, Apply, Refresh), 'Interface Configuration' (IP Address, Network Mask, Gateway Address, DNS Primary Server, DNS Secondary Server, Domain Name, Apply, Refresh), 'Host Name' (Name, Apply, Refresh), and 'Last Address Conflict State' (Interface Config State, Conflicting MAC, Clear, Refresh). At the bottom, there's a 'Port Configuration And Diagnostic' section with a table header: Name, Negotiation Status, Link, Speed, Duplex, Change, Diagnostics, and a Refresh button.

7

Item			Description
TCP/IP Parameters	Configuration Control	Startup Configuration	Displays the information of an appropriate item.
	Interface Configuration	IP Address	
		Network Mask	
		Gateway Address	
		DNS Primary Server	
		DNS Secondary Server	
		Domain Name	
	Host Name	Name	
	Last Address Conflict State	Interface Config State	
Conflicting MAC			
Port Configuration And Diagnostic	Name		Displays the information of an appropriate item.
	Negotiation Status		
	Link		
	Speed		
	Duplex		
	Change		The Ethernet port can be set.
	Diagnostics		The following Ethernet counters can be displayed and cleared: <ul style="list-style-type: none">• Interface Counters• Media Counters
[Refresh] button		Gets the information of each item from the actual machine.	
[Apply] button		Sets the information of each item into the actual machine.	
[Clear] button		Clears the settings of each item from the actual machine.	

■[DLR] tab

The screenshot shows the 'CIP Safety Configuration Tool' window. The left sidebar lists the 'Safety Communication Module' with two networks: 'Network 1: EIP/CIPS Scanner Identifier 192.168.3.51' and 'Network 2: EIP/CIPS Scanner Identifier 192.168.0.5'. The main area is the 'DLR' tab, which includes sections for 'DLR' (Network Topology: Linear, Network Status: Normal), 'Capabilities' (Announce-based Ring Node: unchecked, Beacon-based Ring Node: checked, Supervisor Capable: checked), 'Active Supervisor Address' (Supervisor IP: 0.0.0.0, Supervisor MAC: 00:00:00:00:00:00), 'DLR Supervisor' (Verify Fault Location, Clear Rapid Fault, Restart Sign On buttons; Ring Supervisor Status: Cannot Support Parameters), 'Supervisor Configuration' (Ring Supervisor Enable: unchecked, Ring Supervisor Precedence: 0, Beacon Interval: 400 μs, Beacon Timeout: 1960 μs, DLR VLAN ID: 0), 'Ring Fault Count' (Ring Fault Count: 0), 'Last Active Node' (Port 1: 0.0.0.0, Port 2: 0.0.0.0), 'Ring Participants List' (IP Address: ###.###.###.###, MAC Address: ##:##:##:##:##:##), and 'Active Supervisor Precedence: 0'. A 'Refresh' button is at the bottom right.

Item		Description
DLR	Network Topology	Click the [Refresh] button to get and display the information of each item.
	Network Status	
Capabilities	Announce-based Ring Node	
	Beacon-based Ring Node	
	Supervisor Capable	
Active Supervisor Address	Supervisor IP	
	Supervisor MAC	
DLR Supervisor ^{*1}	Ring Supervisor Status	Displays menu items including [Verify Fault Location], [Clear Rapid Fault], and [Restart Sign On].
Supervisor Configuration ^{*1}	Ring Supervisor Enabled	The information of each item can be displayed, applied, or refreshed. Click the [Refresh] button to get and display the information of each item from the actual machine.
	Ring Supervisor Precedence	
	Beacon Interval	
	Beacon Timeout	
	DLR VLAN ID	
Ring Fault Count ^{*1}	Ring Fault Count	The information of each item can be displayed, cleared, or refreshed. Click the [Refresh] button to get and display the information of items from the actual machine.
Last Active Node ^{*1}	Port 1 ^{*2}	Displays the information of an appropriate item. Click the [Refresh] button to get and display the information of each item from the actual machine.
	Port 2 ^{*3}	
Ring Participants List ^{*1}	IP Address	
	MAC Address	
Active Supervisor Preference ^{*1}		

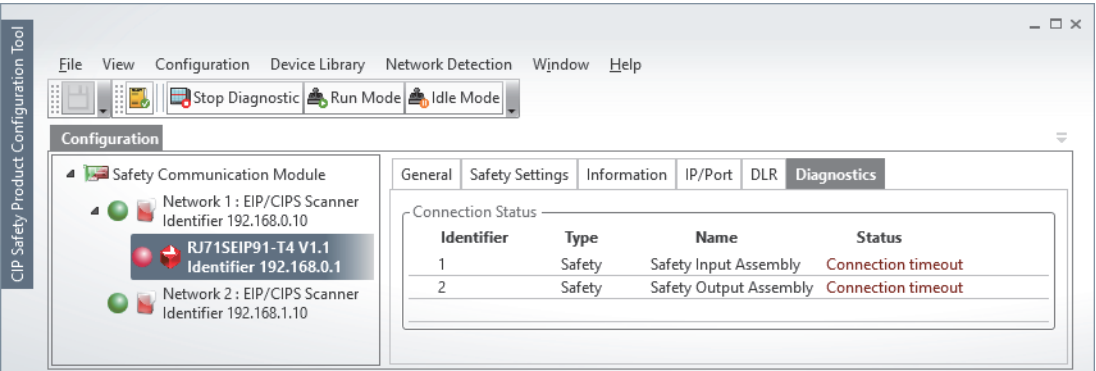
^{*1} This item is displayed when CIP Safety Configuration Tool with the software version "1.3.0.28" or later is used.

^{*2} Read the term as P1-A and P2-A in the CIP Safety module.

^{*3} Read the term as P1-B and P2-B in the CIP Safety module.

■[Diagnostics] tab

This tab is displayed only during diagnostics.



Item		Description
Connection Status	Identifier	Displays the information of an appropriate item.
	Type	
	Name	
	State	

■[Standard Settings] tab

Item	Description
Selected Connections	Lists the added connections. Click the [Remove] button to remove a selected connection.
Available Connections	Lists the available connections defined in the EDS file. Click the [Add] button to add the connection to "Selected Connections".

• [Connection Parameters] tab

Item	Description
General	This Connection is active at startup*1
	Connection Name
	Connection Type
	Identifier
	Timeout Multiplier

Item		Description
Path Parameters ^{*2}	Assembly Instance(O->T) ^{*3}	Set the connection number of the connection destination (target-side connection, which is specified by the CIP Safety module on the external device side). This item is displayed when the connection of "Exclusive Owner (Class1 Instance)" is selected.
	Assembly Instance(T->O) ^{*3}	Set the connection number of the connection destination (target-side connection, which is specified by the CIP Safety module on the external device side). This item is displayed when the connection of "Exclusive Owner (Class1 Instance)" or "Input Only (Class1 Instance)" is selected.
	Symbol Ansi	Set the tag name of the connection destination (target-side connection, which is specified by the CIP Safety module on the external device side). This item is displayed when the connection of "Input Only (Class1 Tag)" is selected.
Input Connection Parameters (Target To Originator) ^{*2}	Size	Set the data size in units of bytes.
	Input Mode	Select the input mode setting from the following options: <ul style="list-style-type: none"> • Multicast connection • Point To Point connection
	Input Type	The only available option is "Fixed".
	Priority ^{*4}	Select the priority setting from the following options: <ul style="list-style-type: none"> • Low • High • Scheduled
	Trigger Type	The only available option is "Cyclic".
	RPI	Set the RPI. This item can be set to a value in the range from 1 to 60000 in increments of 1ms.
Output Connection Parameters (Originator To Target) ^{*2}	Size	Set the data size in units of bytes.
	Output Type	The only available option is "Fixed".
	Priority ^{*4}	Select the priority setting from the following options: <ul style="list-style-type: none"> • Low • High • Scheduled
	RPI	Set the RPI. This item can be set to a value in the range from 1 to 60000 in increments of 1ms.

*1 This setting value is reflected to 'Reserved station (Class1)' (Un\G99440 to Un\G99447, Un\G1148016 to Un\G1148023). Selecting the checkbox sets no reserved station and clearing the checkbox sets a reserved station.

*2 These items are displayed when the registered EDS file is for the CIP Safety module.

*3 Set the same value.

*4 The priority is in the order of "Scheduled" → "High" → "Low".

- [Keying] tab

Connection Parameters
Keying
Application Parameters

Identification

Check Type:Exact Match

Vendor Code:161

Product Type:140

Product Code:11

Major Version:1

Minor Version:1

Item	Description	
Identification	Check Type	Configure settings for verification (keying) to check the actual machine against the setting values of each item when setting up a connection. The displayed items and their settings are dependent on the EDS file of the device. (When a generic device is registered, all the items can be set.)
	Vendor Code	
	Product Type	
	Product Code	
	Major Version	
	Minor Version	

- [Application Parameters] tab

Connection Parameters
Keying
Application Parameters

Restore Default Values

Collapse All

Expand All

Get Online Values

Copy Online values to Configuration

Item ^{*1}	Description
Restore Default Values	Executes an appropriate operation listed on the left.
Collapse All	
Expand All	
Get Online Values	Gets the values from the actual machine.
Copy Online values to Configuration	

^{*1} The displayed items and their settings are dependent on the EDS file of the device. No items are available for the CIP Safety module.

■[Safety Settings] tab

- [Safety Parameters] tab

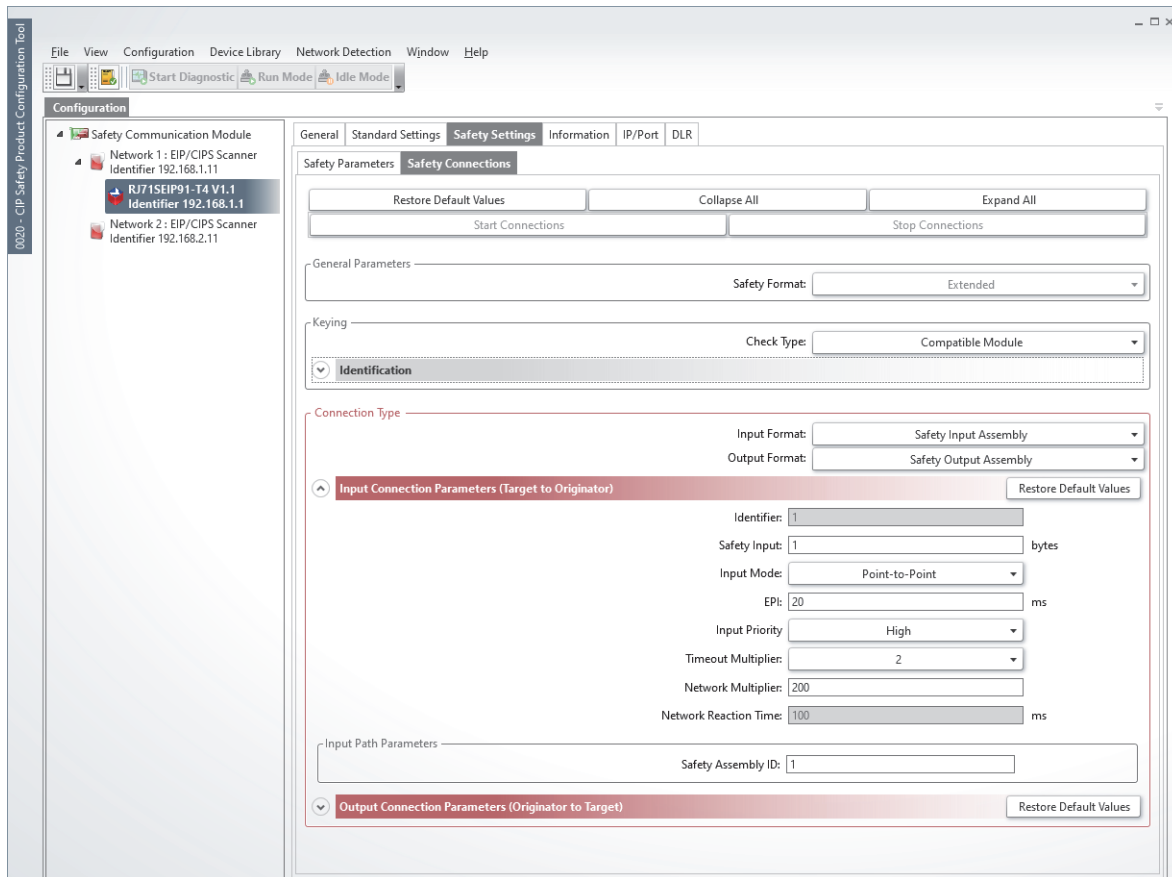
7

Item		Description
General	Configuration Type	Set the configuration type from the following options: <ul style="list-style-type: none"> Externally Initialized This Tool
Identification	Adapter CIP identifier	Displays the IP address.
	Safety Network Number	Displays the Safety Network Number.
	Edit	Edit the Safety Network Number.
	Copy	Copies the Safety Network Number into the clipboard.
	Paste	Pastes the Safety Network Number from the clipboard.
	Set TUNID	Set the TUNID ^{*1} on the corresponding device. ^{*2}
Safety Reset	Safety Reset	Executes Safety Reset on the corresponding device.
Signature in SNCT	Enable Signature	Enables or disables signature verification to establish a connection.
	ID	Gets and displays the ID from the device.
	Date	Gets and displays the date from the device.
	Time	Gets and displays the time from the device.
	Copy	Copies the values of these items into the clipboard.
	Paste	Pastes the values from the clipboard to these items.
Signature in Device	ID	Gets and displays the ID from the device.
	Date	Gets and displays the date from the device.
	Time	Gets and displays the time from the device.
	Copy	Copies the values of these items into the clipboard.
	Refresh	Gets the signature from the corresponding device.

*1 This value is the combination of Adapter CIP identifier and Safety Network Number and is a specific identifier for identifying devices on the network.

*2 When the target is the CIP Safety module, setting using the [Set TUNID] button is not recommended. Reflect the TUNID of the target using the [Save configuration to module] button. (Page 49 [Safety Communication Module Access] tab)

- [Safety Connections] tab



Item		Description
Restore Default Values		Executes an appropriate operation listed on the left.
Collapse All		
Expand All		
Start Connections		
Stop Connections		
General Parameters	Safety Format	The only available option is "Extended".* ³
Keying	Check Type	Configure settings for verification (keying) to check the actual machine against the setting values of each item when setting up a connection.

Item		Description
Connection Type ^{*4}	Input Format	Select the format of the input-side (T->O) communications from the following options: <ul style="list-style-type: none"> • Safety Input Assembly • Safety Input Class0 Tag
	Output Format	Select the format of the output-side (O->T) communications from the following options: <ul style="list-style-type: none"> • Safety Output Assembly • Safety Output Class0 Tag • None
	Input Connection Parameters (Target To Originator)	Identifier
		Safety Input
		Input Mode
		EPI ^{*8}
		Input Priority
		Timeout Multiplier ^{*8}
		Network Multiplier
		Network Reaction Time
		Safety Assembly ID ^{*5}
		Symbol Ansi ^{*6}
	Output Connection Parameters (Originator To Target) ^{*7}	Identifier
		Safety Output
		EPI ^{*8}
		Output Priority
		Timeout Multiplier ^{*8}
		Network Multiplier
		Network Reaction Time
		Safety Assembly ID ^{*5}
		Symbol Ansi ^{*6}

*3 The CIP Safety modules support only the Extended format and do not support the Base format.

*4 These items are displayed when the registered EDS file is for the CIP Safety module.

*5 Set the instance setting value of the target-side connection, which is specified by the CIP Safety module on the external device side. Also, match the value with that of the target-side connection direction (T->O or O->T).

*6 Set the tag name of the target-side connection, which is specified by the CIP Safety module on the external device side. Also, match the value with that of the target-side connection direction (T->O or O->T).

*7 These items are displayed when "Output Format" is set to other than None.

*8 Do not set 1000 for "EPI" or 1 for "Timeout Multiplier" as it may make communications unstable.

Precautions

If one-way communication is set in the assignment of the safety device, an unused area whose size is the same as the communication used is assigned for the safety device (send and receive) in the unused direction. For details, refer to the following precautions.

☞ Page 68 [Safety Target (Class0)] tab








Device Library

Devices added from EDS files will be registered as components.

Displayed devices can be added to the configuration view by drag-and-drop action.

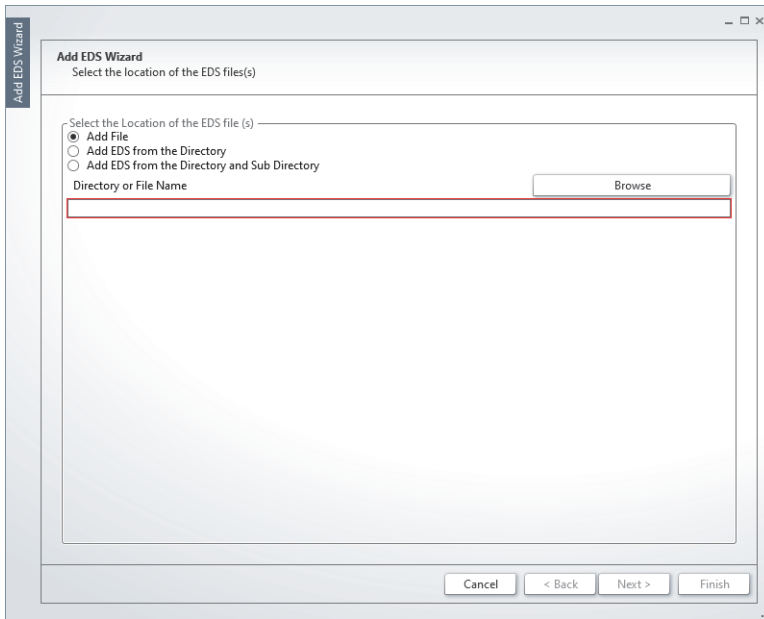
Tool bar



Icon	Item	Description
	Insert In Configuration	Adds a selected EDS file to the configuration view.
	Add EDS	Adds an EDS file to the library.
	Remove EDS	Removes an EDS file from the library.
	Properties	Displays the properties of the EDS file.
	Show EDS	Displays the contents of the EDS file.
	Open File Location	Opens the system folder where the EDS file is added. This icon is not shown in the toolbar.
	Filter	Sorts and filters files displayed in the tree in accordance with the selected condition. <ul style="list-style-type: none"> • Raw: Simply lists EDS files without grouping. • Vendor: Lists EDS files for each vendor folder. • All EDS: Lists all EDS files for each type, such as general and non-modular. • Type: Lists EDS files for each type, such as general and non-modular. • Name: Simply lists EDS files in order of name without grouping. • Vendor and Type: Lists EDS files by grouping them by vendor and type. • Device Profile: Lists EDS files by grouping them by device profile type, such as Generic Device. • Vendor and Device: Lists EDS files by grouping them by vendor and device profile.

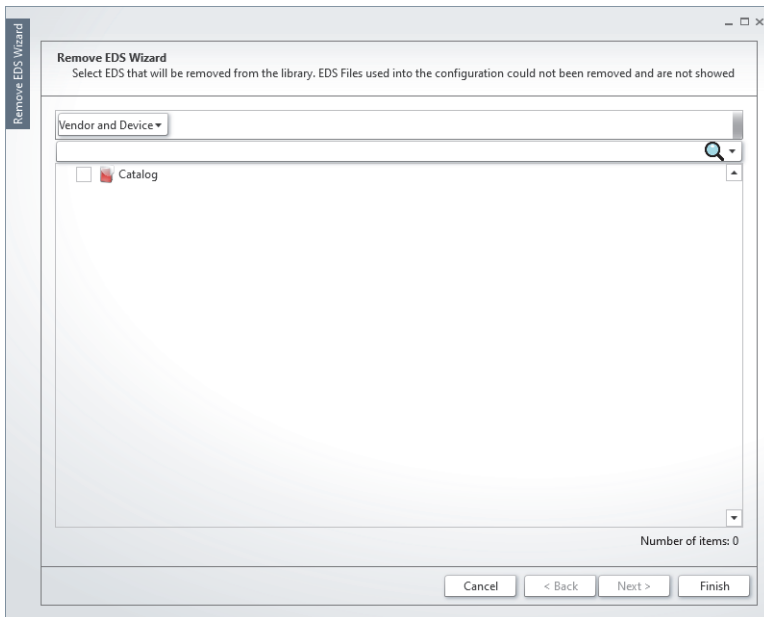
Adding EDS files

Select a radio button to specify a file or folder. Click the [Finish] button to add EDS files.



Removing EDS files

Specify an EDS file or folder to remove. Click the [Finish] button to remove the specified files.



Properties of an EDS file







This window displays the following information defined for an EDS file:

- File Name
- Vendor
- Product Type
- Product Code
- Revision
- Product Name



Network Detection

The EtherNet/IP devices on the network are detected and listed.
Displayed devices can be added to the configuration view by drag-and-drop action.

Tool bar		
Icon	Item	Description
	Start Network detection	Executes the network detection.
	Insert In Configuration	Copies a selected device to the configuration view.
	Copy All	Copies all detected devices to the configuration view.
	Properties	Displays the properties of the EDS file.
	Show EDS	Displays the contents of the EDS file.
	Open File Location	Opens the system folder where the EDS file is added. This icon is not shown in the toolbar.


Logger

This view displays the following types of records that are logged during edit operation.

- Fatal
- Error(s)
- Warning(s)
- Message(s)
- Reserved

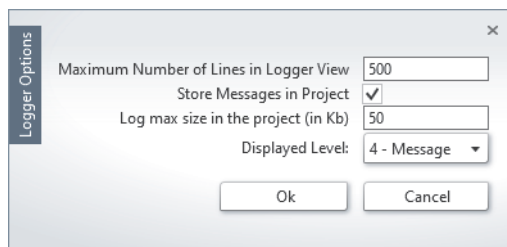
The maximum number of log records is limited by the maximum log size that is specified as a logger option.

The right-click menu provides commands to work with displayed records.

Item	Description
Clear All	Deletes all records displayed in the logger view.
Copy Selection	Copies records selected in the logger view.
Copy All	Copies all records displayed in the logger view.
Options	Displays the logger options. ( Page 84 Options)
Save	Export records from the logger view to a text file.

Options

Right-click in the logger view and select "Options" to display this window.

The image shows a 'Logger Options' dialog box. It has a title bar with a close button. Inside, there are four settings: 'Maximum Number of Lines in Logger View' with a text box containing '500'; 'Store Messages in Project' with a checked checkbox; 'Log max size in the project (in Kb)' with a text box containing '50'; and 'Displayed Level' with a dropdown menu showing '4 - Message'. At the bottom are 'Ok' and 'Cancel' buttons.

Item	Description	Default	Allowable setting range
Maximum Number of Lines in Logger View	Set the number of lines to display.	500	10 to 10000
Store Messages in Project	Set whether to store messages.	Selected	—
Log max size in the project (in Kb)	Set the upper limit of capacity for collected log records.	50	1 to 1048576
Displayed Level	Set the lowest level of records to be displayed.	4 - Message	<ul style="list-style-type: none">• 1 - Fatal• 2 - Error• 3 - Warning• 4 - Message• 5 - Reserved

Window

Layout Style Manager

The color of CIP Safety Configuration Tool can be changed in accordance with the selected color.

Help

About

The installed files of CIP Safety Configuration Tool are displayed in a hierarchy.

8 COMMUNICATION TYPE

8.1 Standard Communications

Communication is performed between the CIP Safety module and EtherNet/IP device on the network.

The CIP Safety module performs data communication between the originator and the target using the following communication method.

- Class1 communications
- UCMM communications

Communication method		Communication cycle	Connection establishment	Request source	Request destination	Description	Reference
Class1 communications	Instance communications	Fixed scan	Established	Originator	Target	This is the most commonly used communication method for EtherNet/IP. Specify the instance number to communicate.	Page 88 Instance communications
	Tag communications	Fixed scan	Established	Consumer	Producer	This is a communication method specialized for communication between programmable controllers. Specify the defined producer tag to receive the data held by the external device. Communication is performed from the producer to the consumer. In order for programmable controllers to send data to each other, it is necessary to set up a connection from both sides to the other producer tag.	Page 93 Tag communications
UCMM communications	Message communications	Acyclic	Not established	Client	Server	This is a request/response type communication method that executes various services by specifying the CIP object defined in the EtherNet/IP device.	Page 95 Message communications

Main applications

■Class1 communications

- Instance communications: Device control, data communications with other programmable controllers
- Tag communications: Data communications with other programmable controllers

■UCMM communications

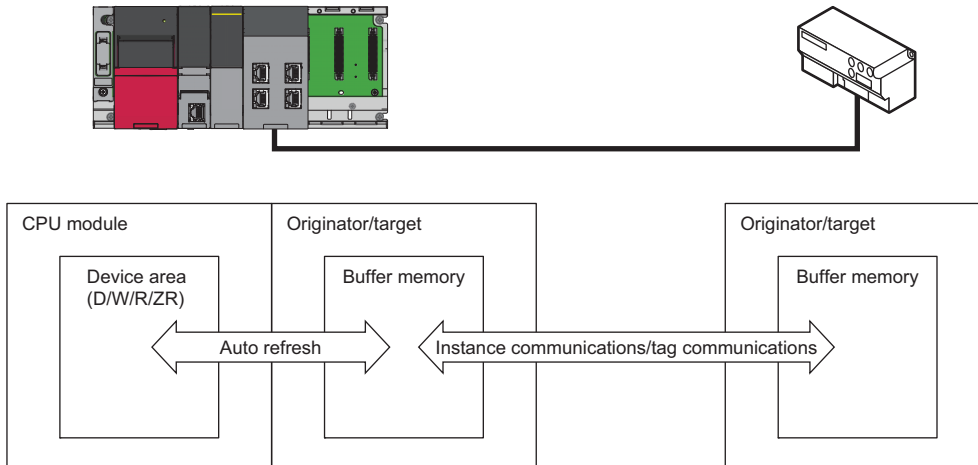
- Message communications: Parameter setting, diagnostics and information reading

Class1 communications

With Class1 communications, data communications are performed at a fixed scan by establishing connections between the CIP Safety module and EtherNet/IP devices.

There are two methods in which to establish communications: instance communications that use instance IDs and tag communications that use tag names.

The originator or target assigns the send/receive range to the buffer memory for each connection and automatically communicates data. Since this data is accessed from the program, it is normally expanded to the device memory of the CPU module by auto refresh.



Communication method and connection setting compatibility

■When the CIP Safety module is the originator

○: Request to the external device possible, ×: Request to the external device not possible

Communication method	Connection setting							
	Connection type	Trigger type			Input format (target to originator)		Output format (originator to target)	
		Cyclic	Application Trigger	Change of State	Fixed	Variable	Fixed	Variable
Instance communications	Exclusive Owner	○	×	×	○	○	○	○ ^{*1}
	Input Only	○	×	×	○	○	○	×
	Listen Only	○	×	×	○	○	○	×
	Redundant Owner	×	×	×	×	×	×	×
Tag communications	Input Only	○	×	×	○	○	○	×

^{*1} Connection requests can be set, but are always sent from the CIP Safety module with a fixed size (size setting value).

■When the CIP Safety module is the target

○: Request to the external device possible, ×: Request to the external device not possible

Communication method	Connection setting							
	Connection type	Trigger type			Input format (target to originator)		Output format (originator to target)	
		Cyclic	Application Trigger	Change of State	Fixed	Variable	Fixed	Variable
Instance communications	Exclusive Owner ^{*1}	○	×	×	○	×	○	×
	Input Only	○	×	×	○	×	○	×
	Listen Only	×	×	×	×	×	×	×
	Redundant Owner	×	×	×	×	×	×	×
Tag communications	Input Only	○	×	×	○	×	○	×

^{*1} With the setting that allows for one connection, communication is not possible for Exclusive Owner connections with 2 or more connections.

Instance communications

Instance communications are mainly used when communication is to be performed with EtherNet/IP devices at a fixed scan. Data communications are performed between the CIP Safety module and the EtherNet/IP device at a fixed scan by establishing connections using an instance ID.

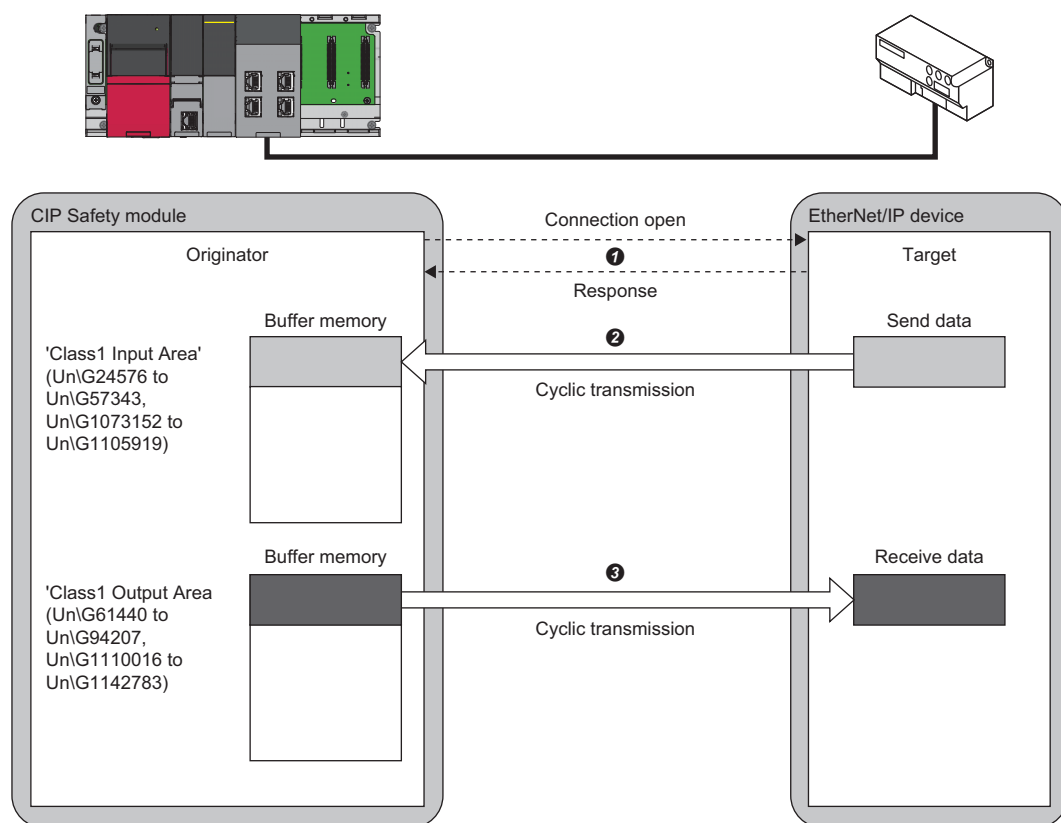
The CIP Safety module acts as an originator or target.

The following connection types are available.

- Exclusive Owner
- Input Only
- Listen Only

■When the connection type is Exclusive Owner

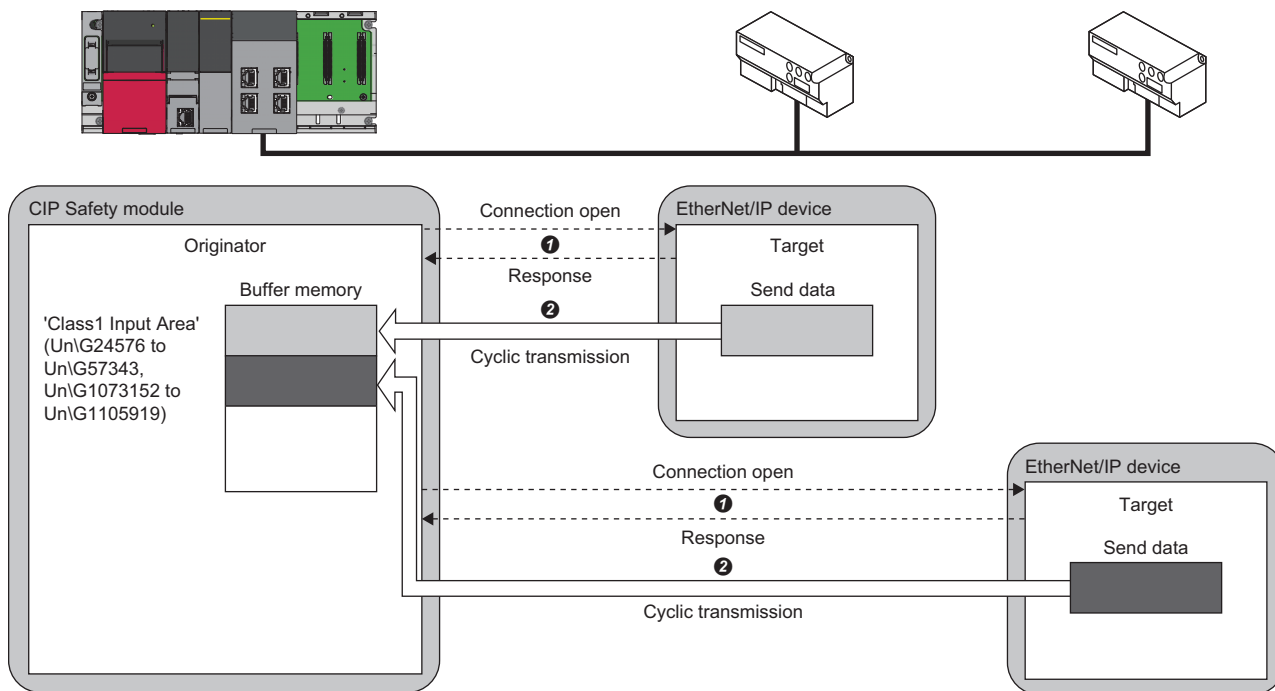
Exclusive Owner is used when sending and receiving data using a single connection.



- ① The CIP Safety module (originator) sends a connection open request, then the EtherNet/IP device (target) responds it and establishes the connection.
- ② Send data of the EtherNet/IP device (target) is sent by cyclic transmission and the data is stored in 'Class1 Input Area' (UnG24576 to UnG57343, UnG1073152 to UnG1105919) of the CIP Safety module (originator).
- ③ Data in 'Class1 Output Area' (UnG61440 to UnG94207, UnG1110016 to UnG1142783) of the CIP Safety module (originator) is sent by cyclic transmission and the data is stored in the receive data buffer of the EtherNet/IP device (target).

■When the connection type is Input Only

Input Only is used when only receiving data using a single connection.



- ❶ The CIP Safety module (originator) sends a connection open request, then the EtherNet/IP device (target) responds it and establishes the connection.
- ❷ Send data of the EtherNet/IP device (target) is sent by cyclic transmission and the data is stored in 'Class1 Input Area' (Un\G24576 to Un\G57343, Un\G1073152 to Un\G1105919) of the CIP Safety module (originator).

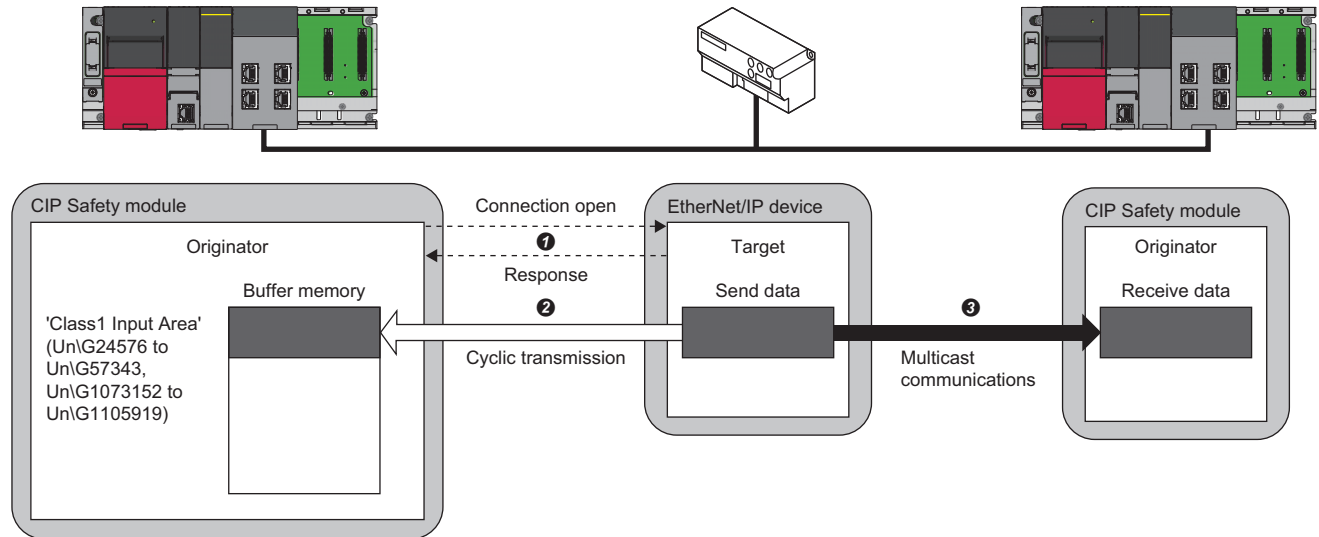
■When the connection type is Listen Only

Listen Only is used when receiving data from multiple devices for a single connection.

The same multicast communication settings need to be set for both the scanner with the connection of Exclusive Owner or Input Only and the scanner with the connection of Listen Only.

The connection of Listen Only cannot be opened when the connection such as Exclusive Owner and Input Only that is set for multicast communications is not opened.

Even when communications are performed normally with the target that is opened using Listen Only, the data receiving will be stopped if all the communications with other originators that are opened using the connection such as Exclusive Owner and Input Only that is set for multicast communications.



- 1 The CIP Safety module (originator) sends a connection open request, then the EtherNet/IP device (target) responds it and establishes the connection.
- 2 Send data of the EtherNet/IP device (target) is sent by cyclic transmission and the data is stored in 'Class1 Input Area' (UnG24576 to UnG57343, UnG1073152 to UnG1105919) of the CIP Safety module (originator).
- 3 In Exclusive Owner or Input Only connection, sending data by the multicast communications sends to the receive data buffer of the CIP Safety module (originator (Exclusive Owner or Input Only)) by cyclic transmission.

■Setting method

This communication method can be used by setting Class1 communications (instance communications) for EtherNet/IP devices.

📖 Page 121 Parameter settings

■Buffer memory to be used

Name	Address		Description
	P1	P2	
Class1 Input Area	Un\G24576 to Un\G57343	Un\G1073152 to Un\G1105919	The data receive area
Class1 Output Area	Un\G61440 to Un\G94207	Un\G1110016 to Un\G1142783	The data send area
Class1 Input data size	Un\G98304 to Un\G98431	Un\G1146880 to Un\G1147007	The data input size for each connection
Class1 Output data size	Un\G98560 to Un\G98687	Un\G1147136 to Un\G1147263	The data output size of each connection
Class1 Start offset address to the input data	Un\G98816 to Un\G98943	Un\G1147392 to Un\G1147519	The start address of the input data area for each connection
Class1 Start offset address to the output data	Un\G99072 to Un\G99199	Un\G1147648 to Un\G1147775	The start address of the output data area for each connection
Class1 communication status data link status	Un\G99408 to Un\G99415	Un\G1147984 to Un\G1147991	The communication status of each connection
Class1 communication status error status	Un\G99424 to Un\G99431	Un\G1148000 to Un\G1148007	The error status of each connection

■I/O signals to be used

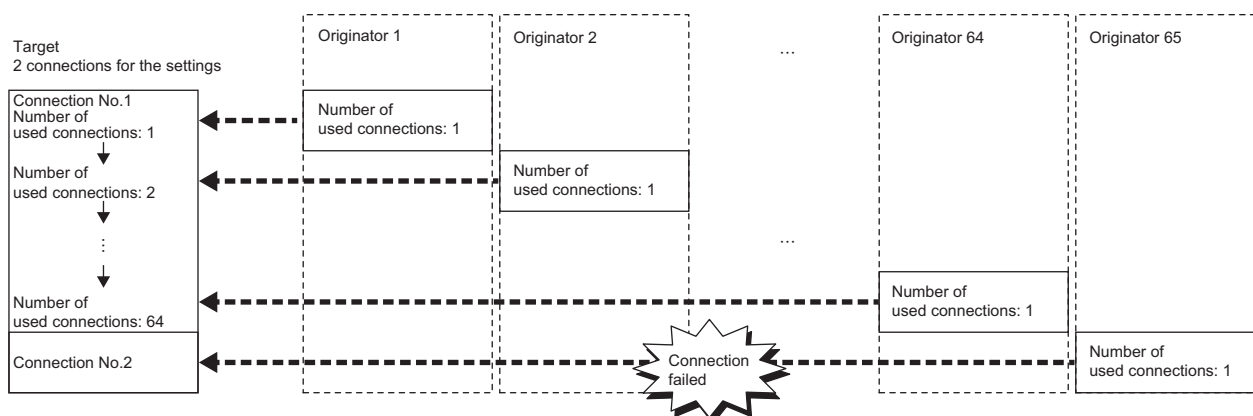
- 'Module READY' (X0)
- 'Port start status (P1)' (X1), 'Port start status (P2)' (X11)

■Error codes and event codes that occur

Type	Code
Error code	3110H
Event code	00100H
	00400H
	00401H
	00800H

■Precautions

- When the CIP Safety module is the target, if multiple connections are connected for one connection setting in multicast communications and unicast communications, the number of connections will be one in the setting. However, the number of used connections will be equivalent to the number of connected connections. The total number of used connections is up to 64.



Due to the parameter settings, the number of connections is 2. However, if there are 64 originators connected to the connection number 1 and the 65th originator tries to connect to connection number 2, the connection will not be made and an error will occur.

- The current number of consumed connections can be checked from 'Number of connection consumed' (Un\G1777843, Un\G1777844).
- If the current number of consumed connections is 64, 36FBFB0AH will be stored in 'Class1 Connection Behavior Error status' (Un\G99584 to Un\G100351, Un\G1148160 to Un\G1148927).
- If the CIP Safety module is the target, when connecting multiple connections for one connection setting, multicast communications and unicast communications can be mixed.

Existing connection	Connection to be connected additionally			
	Multicast communications		Unicast communications	
	Exclusive Owner Input Only	Listen Only	Exclusive Owner Input Only	Listen Only
Not performed	Can be connected (new connection)	Cannot be connected ^{*1}	Can be connected (new connection)	Cannot be connected ^{*1}
During multicast communications	Can be connected ^{*2}		Can be connected ^{*3}	
During unicast communications	Can be connected ^{*3}			

^{*1} A CIP response code (General Status: 1H, Extended Status: 119H) is sent to the external device.

^{*2} Communication from the target to originator reuses multicast communications, and thus the load on the CIP Safety module and the line is low.

^{*3} Communication in which both directions are handled (from the target to originator, and from the originator to target) is newly started, and thus the load on the CIP Safety module and on the line is high.

- In multicast communications, connection cannot be made if the existing connection and the connection settings are different. Each originator to be connected must match the settings of the following parameter items. Otherwise, a CIP response code is sent to the additionally connected device.

Parameter item	General Status	Extended Status
RPI from the target to originator	1H	112H
Size from the target to originator	1H	134H
Fixed/Variable from the target to originator	1H	135H
Priority from the target to originator	1H	136H
Transport Class	1H	137H
Production Trigger from the target to originator	1H	138H
Production Inhibit Time from the target to originator	1H	139H

- In unicast communications, connection can be made even if the existing connection and the connection settings are different.
- If the Ethernet cable is disconnected and connected within 3 seconds or if it is connected to a different port during communication, connection will not be established again, causing a data link error in some cases. In this case, disconnect and connect the Ethernet cable again.

Tag communications

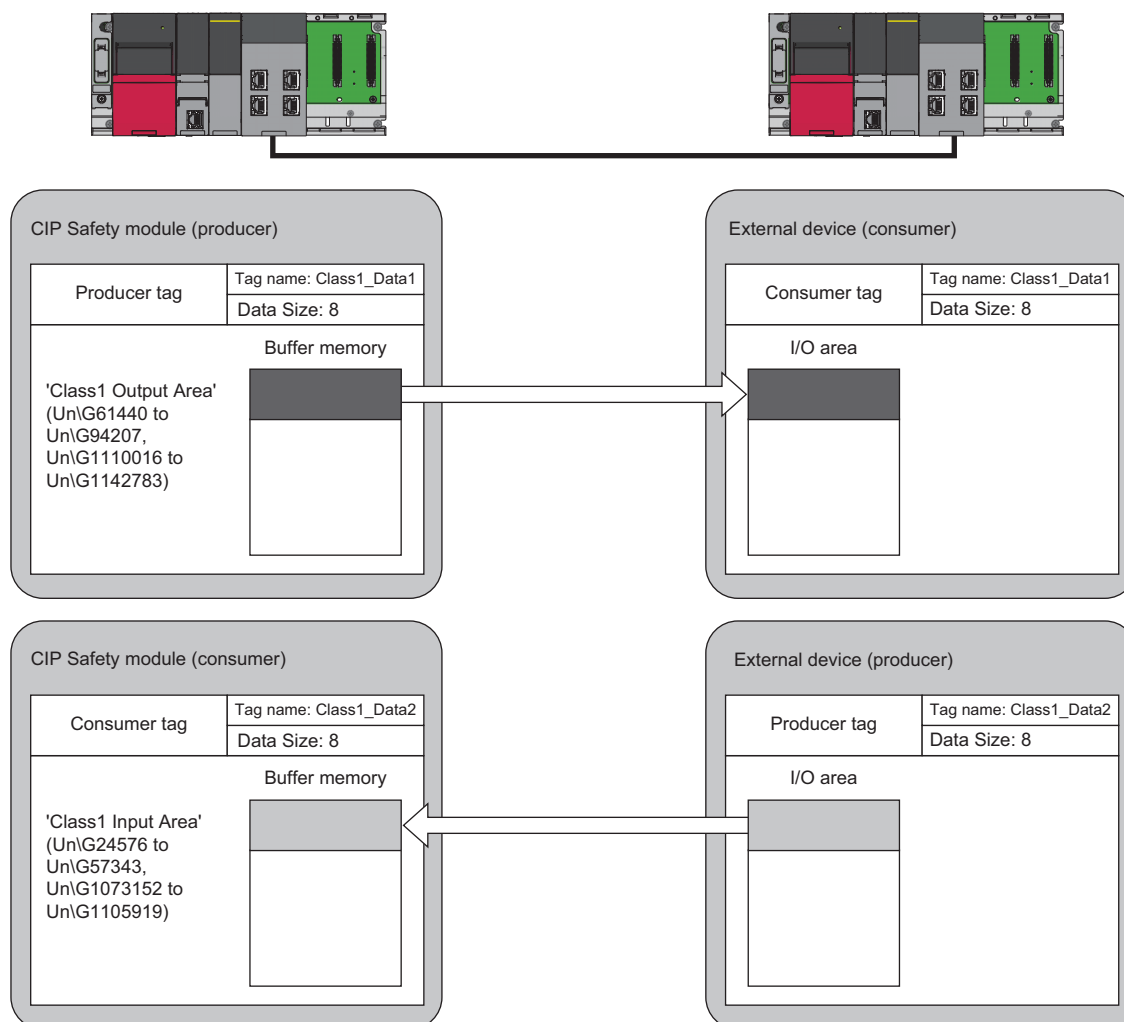
Tag communications are used when communication is to be performed between programmable controllers.

Data communications are performed at a fixed scan by establishing connections between tags whose tag name and data size are the same.

Producer tag data can be received by specifying the destination (IP address), tag name, and data size of the producer tag on the consumer tag side.

Producer tags and consumer tags are defined between programmable controllers and connections are established from both sides for communicating data each other.

- Producer tag: This tag is for sending data. It receives a connection establishment request from the consumer and sends the data to the consumer.
- Consumer tag: This tag is for receiving data. It makes a connection establishment request to the producer and receives the data from the producer.



Point

- It is necessary to set the producer tag and consumer tag for each external device that wants to communicate with the CIP Safety module.
- Tags whose tag name and data size are the same form a set of communication settings for communication.

■For producer

If the producer tag is set, data is sent to the external device when a connection establishment request is made from the external device for which the corresponding consumer tag is set.

If the tags are set correctly for the CIP Safety module and the external device, communication will start automatically when both communication preparations are complete.

The CIP Safety module sends the data stored in 'Class1 Output Area' (Un\G61440 to Un\G94207, Un\G1110016 to Un\G1142783) to the receive area of the external device.

■For consumer

If the consumer tag is set, data is received from the external device when a connection establishment response is made from the external device for which the corresponding producer tag is set.

If the tags are set correctly for the CIP Safety module and the external device, communication will start automatically when both communication preparations are complete.

The CIP Safety module receives the information of the output area of the external device in the 'Class1 Input Area' (Un\G24576 to Un\G57343, Un\G1073152 to Un\G1105919).

■Setting method

This communication method can be used by setting Class1 communications (tag communications) for EtherNet/IP devices.

☞ Page 142 Parameter settings

■Buffer memory to be used

☞ Page 91 Buffer memory to be used

■I/O signals to be used

☞ Page 91 I/O signals to be used

■Error codes and event codes that occur

☞ Page 91 Error codes and event codes that occur

■Precautions

☞ Page 92 Precautions

UCMM communications

In UCMM communications, data read/write commands are used to communicate between the CIP Safety module and the EtherNet/IP device at a desired timing without establishing connections.

The functions include a client function (commands are sent from the CIP Safety module to the EtherNet/IP device) and a server function (commands are sent from the EtherNet/IP device to the CIP Safety module).

Communication method	Client function	Server function
Message communications	Used	Used

Message communications

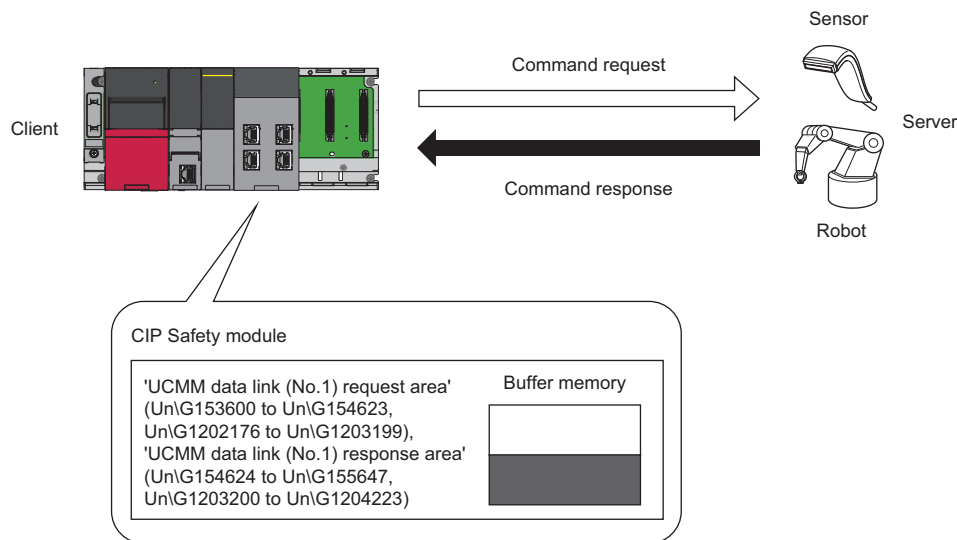
Message communications allow for the CIP object of the external device to execute various services. Communications start without establishing connections.

Also, the parameter settings of the external device can be written, and the device information can be read.

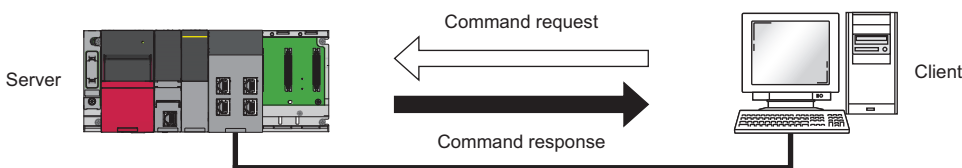
With the client function, the buffer memory is used to communicate with arbitrary timing.

The server function communicates at the timing when the request on the client side is processed.

• Client function



• Server function



■Setting method

- Server function: This function can be used to set the IP address for the CIP Safety module. (📖 Page 58 Network 1: EIP/CIPS Scanner, Network 2: EIP/CIPS Scanner)
- Client function: This function can be used to set a request to the buffer memory. (📖 Page 96 Buffer memory to be used)

■Buffer memory to be used

Name	Address		Description
	P1	P2	
Data link execution request (No.1 to No.32)	Un\G151552 to Un\G151553	Un\G1200128 to Un\G1200129	Used for requesting/checking the communication status.
Data link execution request acceptance (No.1 to No.32)	Un\G151568 to Un\G151569	Un\G1200144 to Un\G1200145	
Data link execution completion (No.1 to No.32)	Un\G151584 to Un\G151585	Un\G1200160 to Un\G1200161	
UCMM communications (No.1 to No.32)	Un\G153600 to Un\G219135	Un\G1202176 to Un\G1267711	The communication request area for the client

■I/O signals to be used

- 'Module READY' (X0)
- 'Port start status (P1)' (X1), 'Port start status (P2)' (X11)

■Error codes that occur

Type	Code
Error code	3110H

■Command

Items such as data and parameters can be read and written with commands.

For details on supported commands (objects), refer to the CIP specifications.

8.2 Safety Communications

The CIP Safety module operates as an originator or target, establishes a connection with a CIP Safety compatible device, and performs safety communications at a fixed scan.

There are two methods in which to establish safety communications: instance communications that use instance IDs and tag communications that use tag names.

Both communication methods allow unicast and multicast communications.

The side that sends data is the producer, and the side that receives data is the consumer.

The following table shows the combinations that can be set for each communication method.


○: Settable, ×: Not settable

CIP Safety module	Instance communications				Tag communications	
	Unicast		Multicast		Unicast and multicast	
	Consumer	Producer	Consumer	Producer	Consumer	Producer
Originator	○	○	○	×	○	×
Target	○	○	×	○	×	○

Precautions

If a momentary power failure occurs, the error is detected and the safety communications may be suspended. To restart the safety communications, release an interlock.

For measures against the momentary power failure, refer to the following.

 MELSEC iQ-R Module Configuration Manual

Communication method and connection setting compatibility

8

■When the CIP Safety module is the originator

○: Request to the external device possible, ×: Request to the external device not possible

Communication method		Connection setting				
		Trigger to send data			Input data length (target to originator)	Output data length (originator to target)
		Cyclic	Application Trigger	Change of State	Fixed	Fixed
Instance communications	Producer	○	×	×	○	○
	Consumer	○	×	×	○	○
Tag communications	Producer	○	×	×	○	○
	Consumer	○	×	×	○	○

■When the CIP Safety module is the target

○: Request to the external device possible, ×: Request to the external device not possible

Communication method		Connection setting				
		Trigger to send data			Input data length (target to originator)	Output data length (originator to target)
		Cyclic	Application Trigger	Change of State	Fixed	Fixed
Instance communications	Producer	○	×	×	○	○
	Consumer	○	×	×	○	○
Tag communications	Producer	○	×	×	○	○
	Consumer	○	×	×	○	○

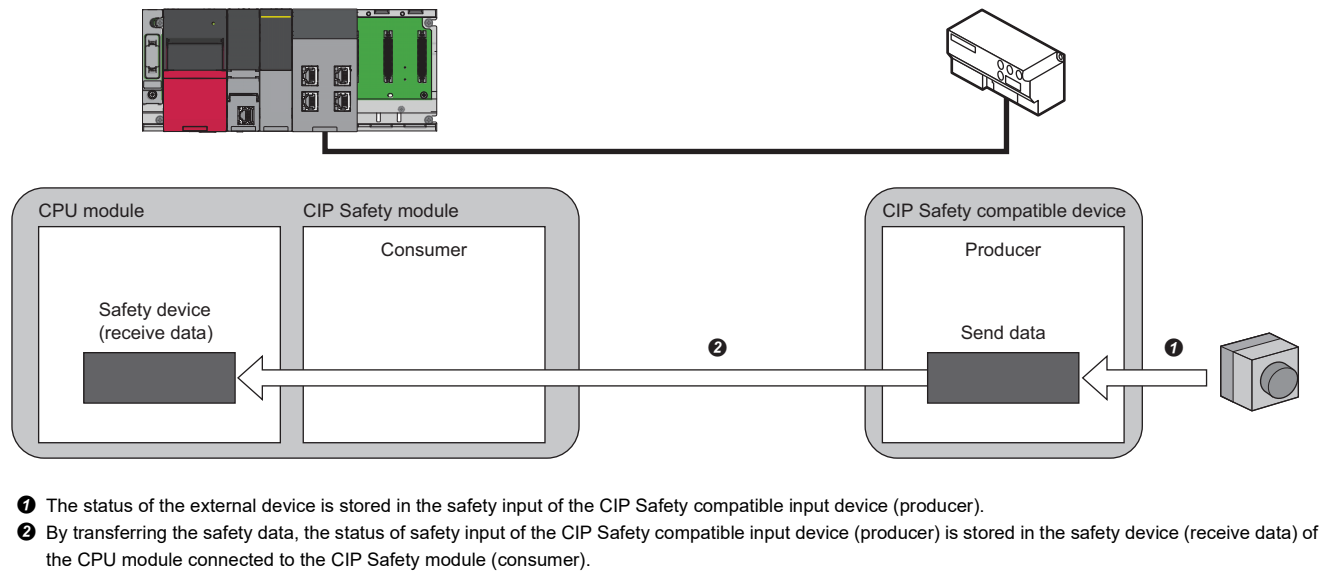
Overview of safety communications

The following describes the communication between the CIP Safety module and a CIP Safety compatible device.

Safety communications when unicast is selected

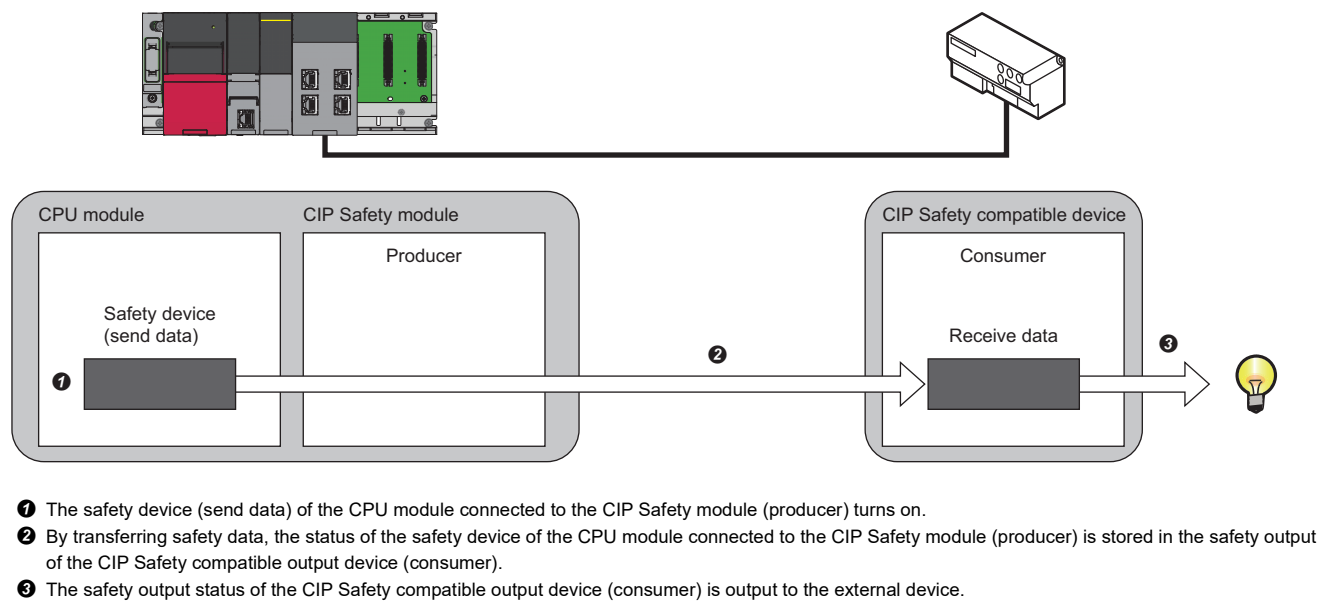
■Between the CIP Safety module (consumer) and an input device (producer)

When receiving data from a CIP Safety compatible device, set the CIP Safety module as the originator and consumer.



■Between the CIP Safety module (producer) and an output device (consumer)

When sending data to a CIP Safety compatible device, set the CIP Safety module as the target and producer.

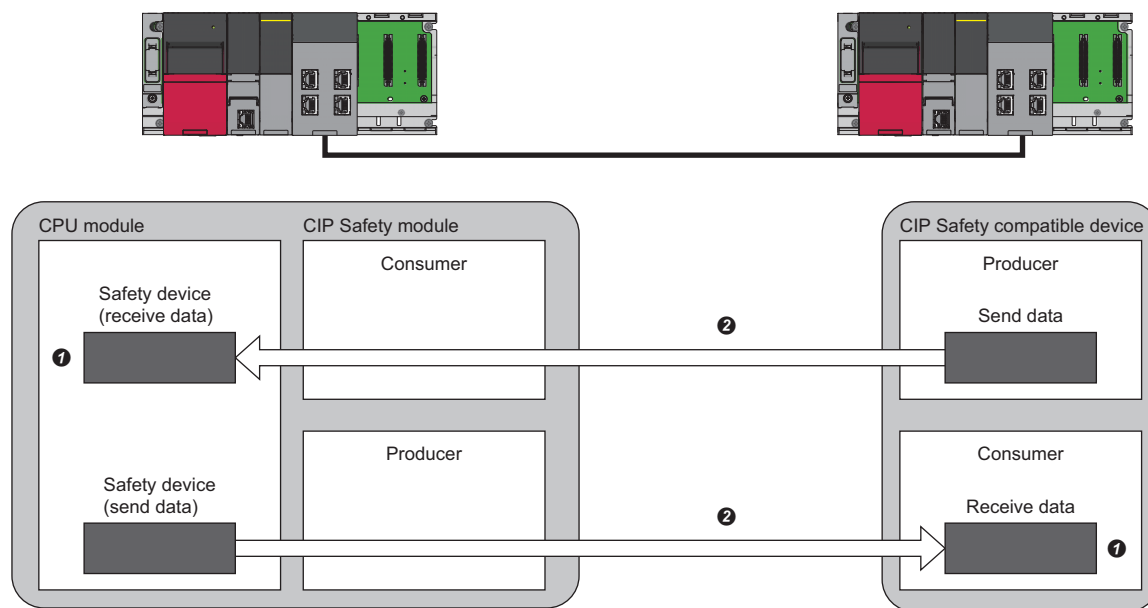


Point

Data and signals can be communicated between the CIP Safety module (producer) and the CIP Safety compatible output device (consumer) only when either of the following conditions is met: the CIP Safety module is the target; the CIP Safety module is the originator and a consumer connection to the CIP Safety compatible output device exists.

■Between the CIP Safety modules (producer/consumer)

When communicating data with a CIP Safety compatible device, set one producer connection and one consumer connection in the CIP Safety module and set the CIP Safety module as the producer and consumer.

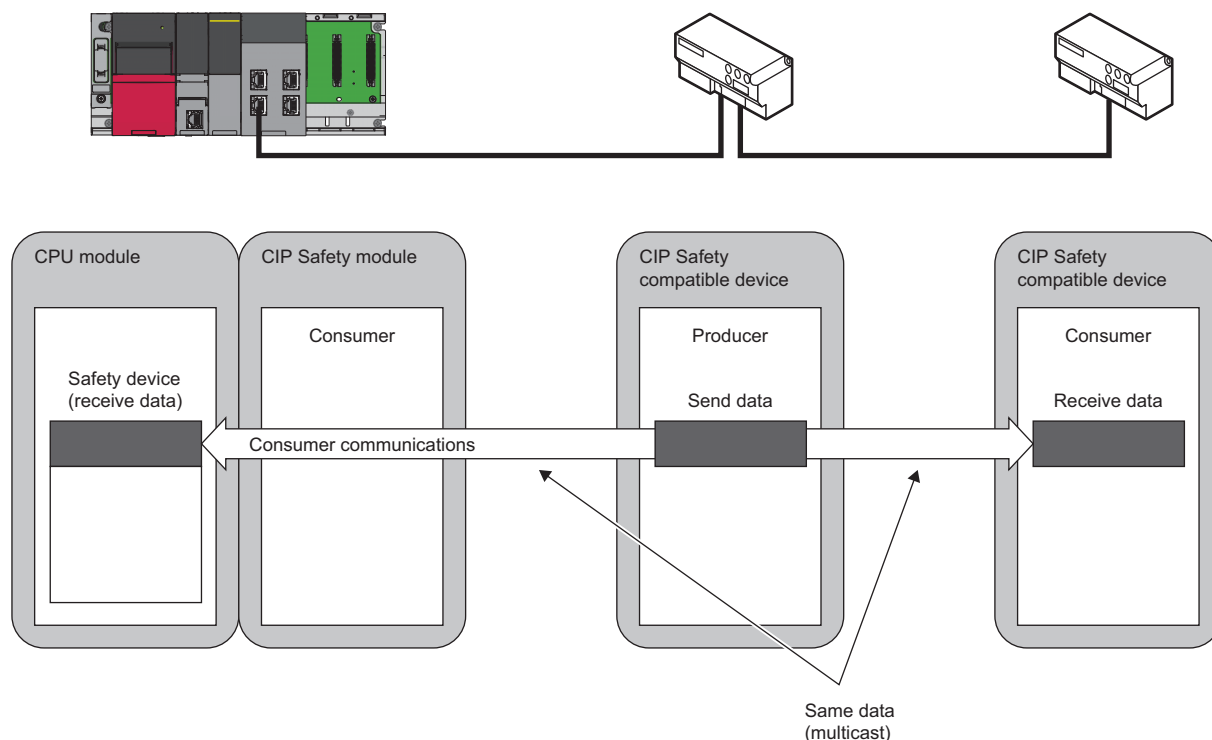


- ❶ The safety device (send data) of the CPU module connected to the CIP Safety module (producer) turns on.
- ❷ By transferring safety data, the status of the safety device (send data) of the CPU module connected to the CIP Safety module (producer) is stored in the safety device (receive data) of the CPU module connected to the CIP Safety module (consumer).

Safety communications when multicast is selected

■When receiving data from a CIP Safety compatible device

When receiving data from a CIP Safety compatible device, set the CIP Safety module as the originator and consumer.

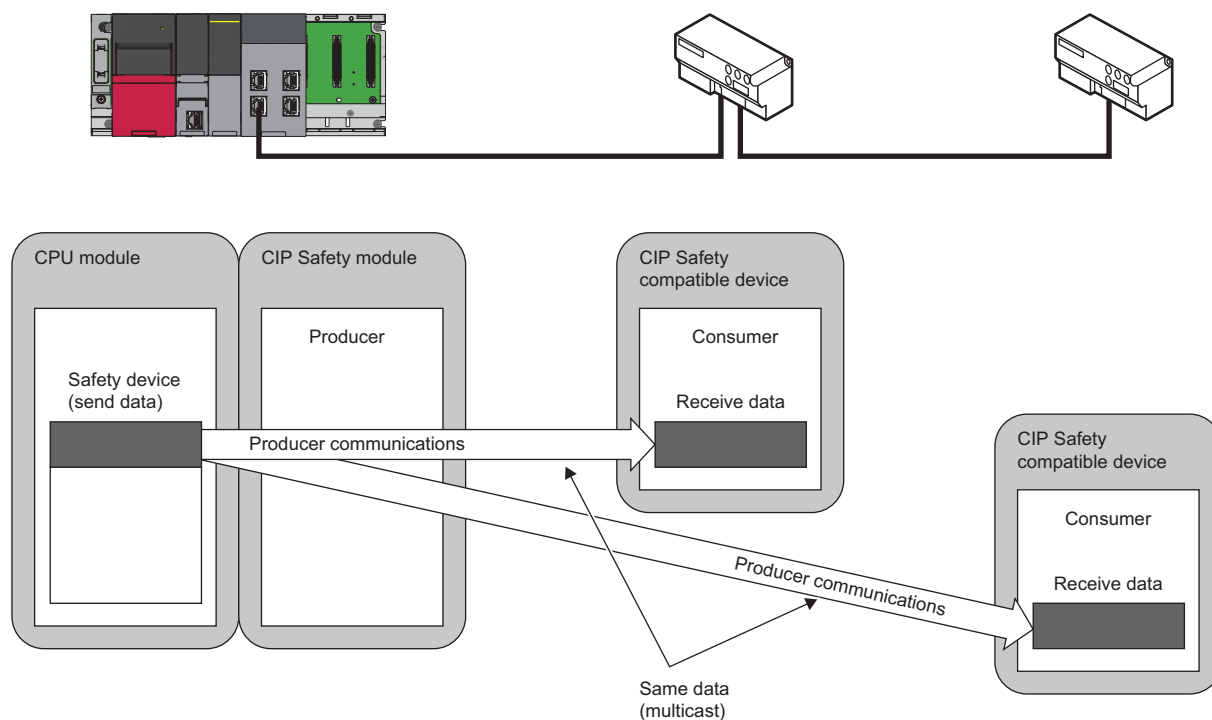


Point

Set the same RPI for all devices that receive data by multicast communications.

■When sending data to a CIP Safety compatible device

When sending data to a CIP Safety compatible device, set the CIP Safety module as the target and producer.



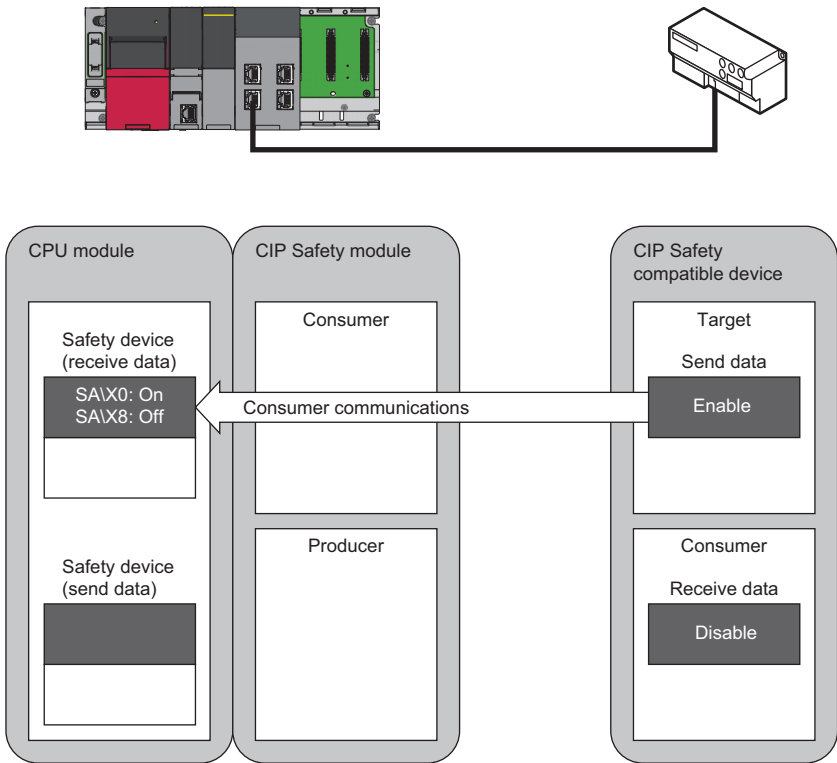
How to check the status during safety communications

Information indicating whether safety communications are normal for each connection is stored in the 0th and 8th bits of the receive data storage device (SA□□) of the CPU module set for each connection.

Item	Description
Consumer safety connection status (0th bit of the safe input device)	Indicates whether safety communications of the consumer connection are normal. The bit is on when normal and is off when abnormal. Also, if the consumer connection is not set, this bit will always remain turned off. If the bit is on, create a safety program such that the safety input data is enabled.
Producer safety connection status (8th bit of the safety input device)	Indicates whether safety communications of the producer connection are normal. The bit is on when normal and is off when abnormal. Also, if the producer connection is not set, this bit will always remain turned off. If the bit is on, create a safety program such that the safety output data is enabled.

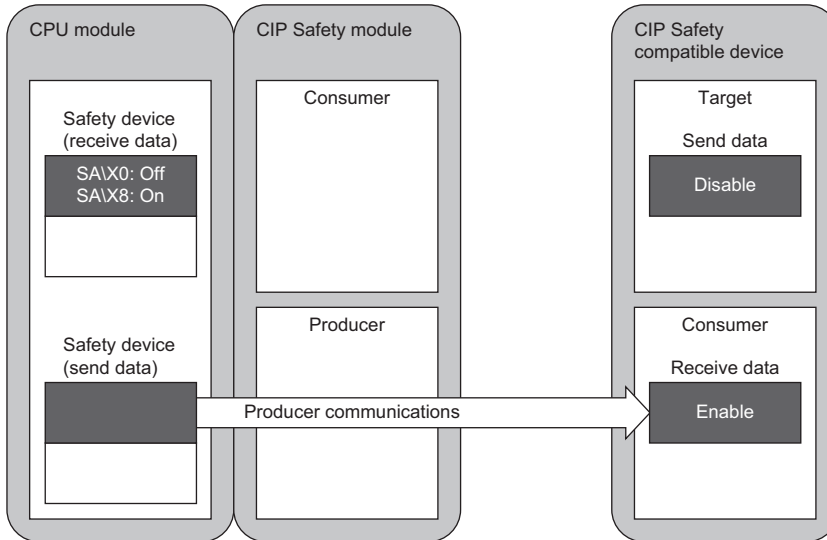
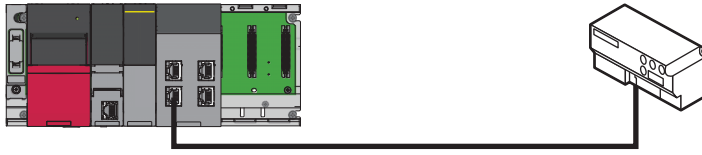
Ex.

When the safe input device is set from SA\X0 and the consumer safety connection status changes to on



Ex.

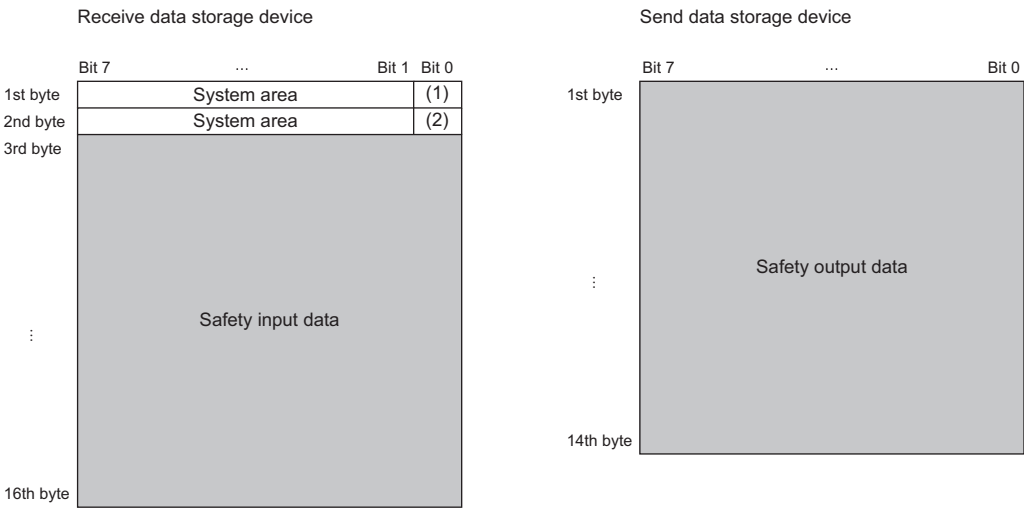
When the safe input device is set from SA\X0 and the producer safety connection status changes to on



- Unicast: Since the number of connections that can be established for one connection setting is one, if an error occurs in safety communications, the consumer safety connection status and the producer safety connection status are turned off.
- Multicast: The number of connections that can be established for one connection setting may be multiple. In that case, if there is even one connection that can perform safety communications normally, the producer safety connection status turns on, and if safety communications on all connections become abnormal, it turns off.

Precautions

- When safety input data is received in safety communications, two bytes of system data is added and stored as well. Therefore, the receive data storage device (SA\□□) of the CPU module secures two bytes more areas in addition to the areas of safety input data to be received by safety communications. For the receive data storage device (SA\□□) of the CPU module, set it even when setting only the producer connection.



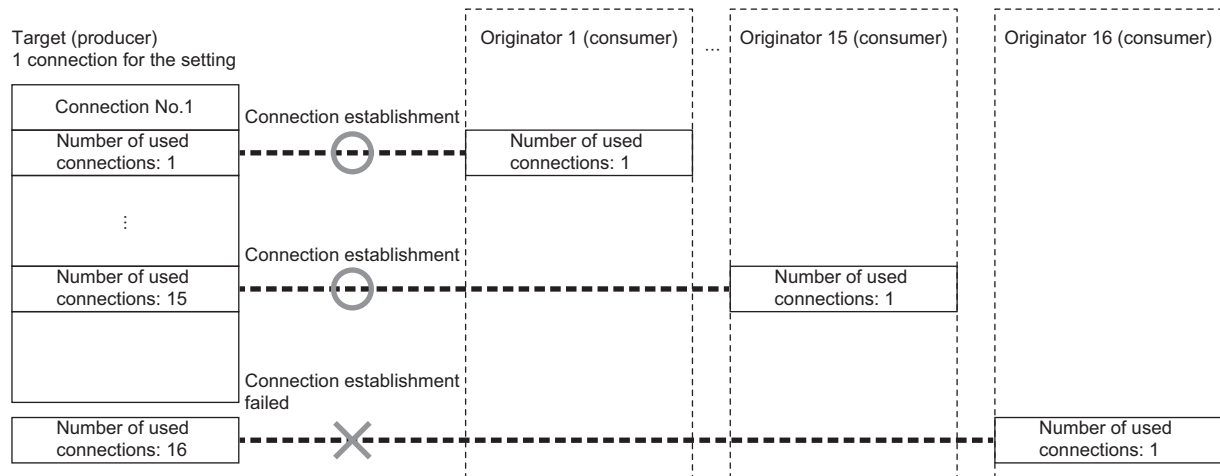
- (1) Consumer safety connection status
(2) Producer safety connection status
- When the status of safety communications changes from abnormal to normal, the consumer safety connection status and producer safety connection status automatically change from off to on.

The number of safety connections used

The following describes the examples of when the CIP Safety module sends data by multicast.

Ex.

When establishing 15 connections with the originator for the multicast connection setting

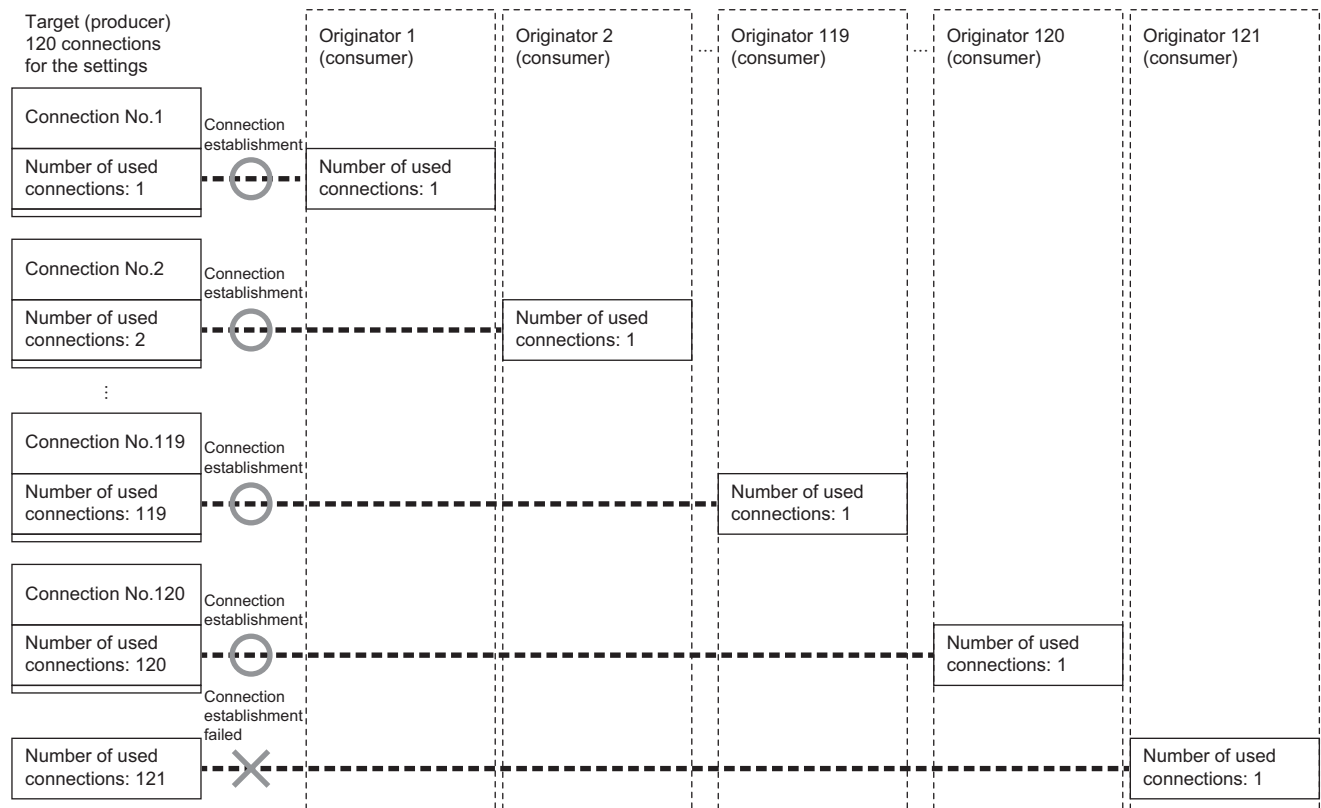


Only one connection is set, but the number of consumed connections is the number of connections connected to the originator (up to 15).

When establishing 15 connections of originators 1 to 15 (consumer) to connection number 1 of the target (producer), if originator 16 tries to connect to connection number 1, the connection cannot be established.

Ex.

When only one connection can be established with the originator for the multicast connection setting




If the number of unicast connections is set to 119 (connection number 1 to 119) and the number of multicast connections is set to 1 (connection number 120), 120 connections are used at that point.

Therefore, if originator 121 tries to connect to connection number 120, the connection cannot be established.

Precautions for using the safety communications


Check the following when testing the entire system operation.


1. Use CIP Safety Configuration Tool to set the safety connection and write the parameters to the CIP Safety module.

 [Configuration] ⇒ [Safety Communication Module] ⇒ [Safety Communication Module Access] ⇒ [Save configuration to module]

2. Reset the CPU module or power off and on the system, then check whether the same value between the acquired value from the CIP Safety module and the setting value in CIP Safety Configuration Tool with the output list. (Check both ports as necessary.)

For details, refer to Step 17 as below.

 Page 172 Parameter settings for the CIP Safety module (target)

3. For the safety connection, check that the safety connection status is normal and safety input and output data are normal.
( Page 103 Precautions)
4. Check that all safety devices operate according to a program.
5. Check that the system is tested according to the system configuration and it has no problem.

9 FUNCTIONS

9.1 Output Hold/Clear When the CPU Module Is Stopped (at Error Occurrence/STOP State)

Whether to clear or hold the output data when the CPU module stops in standard communications can be set.

Data to be held or cleared is output from the CIP Safety module to another EtherNet/IP device on EtherNet/IP packet. ('Class1 Output Area' (Un\G61440 to Un\G94207, Un\G1110016 to Un\G1142783) is not cleared.)

The state in which the CPU module is stopped refers to the following two situations.

- CPU error: When a stop error occurs in the CPU module that manages the CIP Safety module
- CPU STOP: When the CPU module that manages the CIP Safety module is set to the STOP state

The settings differ depending on the type of communication method.

Communication method	Setting
Class1 communications	Enable
UCMM communications ^{*1}	Disable

^{*1} Regardless of this setting, message communications (client function) stop when the CPU module stops. This is because message communications are executed by the program that uses buffer memory.

If an execution instruction is made directly to the CIP Safety module using the device monitor of an engineering tool instead of a program, message communications will operate even when the CPU module is stopped.

Behavior

The following shows how the hold and clear operations behave depending on the CPU module status corresponding to each setting status when the setting is enabled.

"Output Hold/Clear Setting during CPU Error"	"Output Hold/Clear Setting during CPU STOP"	CPU module status	Hold/clear
Hold	Hold	RUN → STOP	Hold
		Error stop	Hold
Hold	Clear	RUN → STOP	Clear
		Error stop	Hold
Clear	Hold	RUN → STOP	Hold
		Error stop	Clear
Clear	Clear	RUN → STOP	Clear
		Error stop	Clear

Precautions

For safety communications, the operation differs depending on the safe operation mode of the CPU module.

- Test mode: Output data is held at RUN to STOP and is cleared at a CPU module stop.
- Safety mode: Output data is cleared at RUN to STOP or a CPU module stop.

Setting method

For the setting method, refer to the following.

☞ Page 37 Basic Setting

9.2 Block Assurance

This function guarantees the I/O data of Class1 communications between the CPU module and the CIP Safety module.

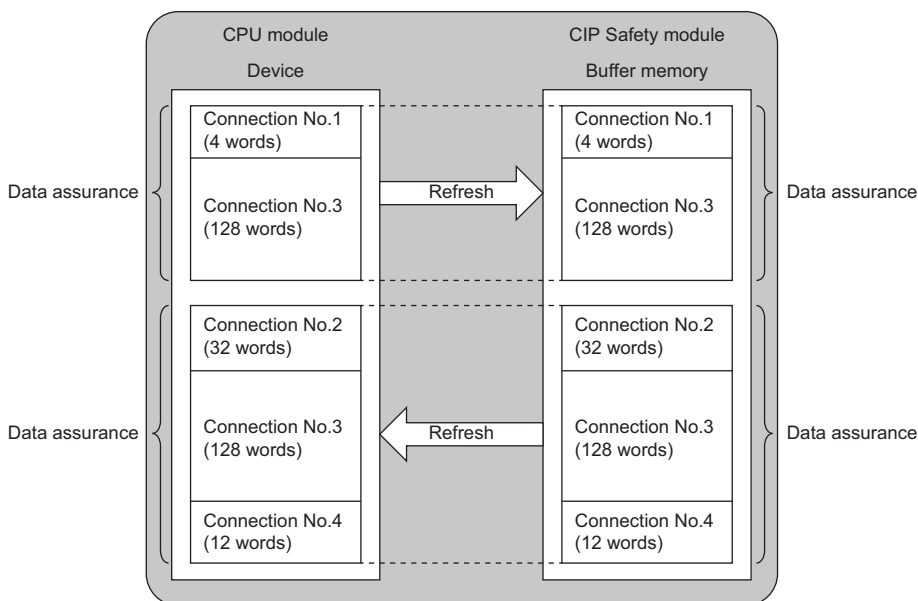
By enabling this function, the I/O data inconsistency can be prevented.

In standard communications, whether or not to guarantee I/O data is determined according to the parameter settings of the engineering tool.

In safety communications, I/O data is guaranteed regardless of the parameter settings of the engineering tool.

Behavior

When block assurance is enabled, block assurance is applied to I/O data for both write processing to the buffer memory and read processing from the buffer memory.



The range in which block assurance is applied is the range set for the auto refresh target of the following buffer memory. Block assurance is applied per input area and output area. (Not applied per connection)

- 'Class1 Input Area' (Un\G24576 to Un\G57343, Un\G1073152 to Un\G1105919)
- 'Class1 Output Area' (Un\G61440 to Un\G94207, Un\G1110016 to Un\G1142783)

Setting method

For the setting method, refer to the following.

📖 Page 37 Basic Setting

Precautions

- If this function is not enabled for standard communications, I/O data may be separated into new data and old data during auto refresh.
- If this function is enabled for standard communications, the transmission delay time will be longer.

9.3 Auto Refresh

Auto refresh is a function that automatically performs refresh (transfer) operation between the buffer memory used in standard communications (Class1 communications) and any device of the CPU module.

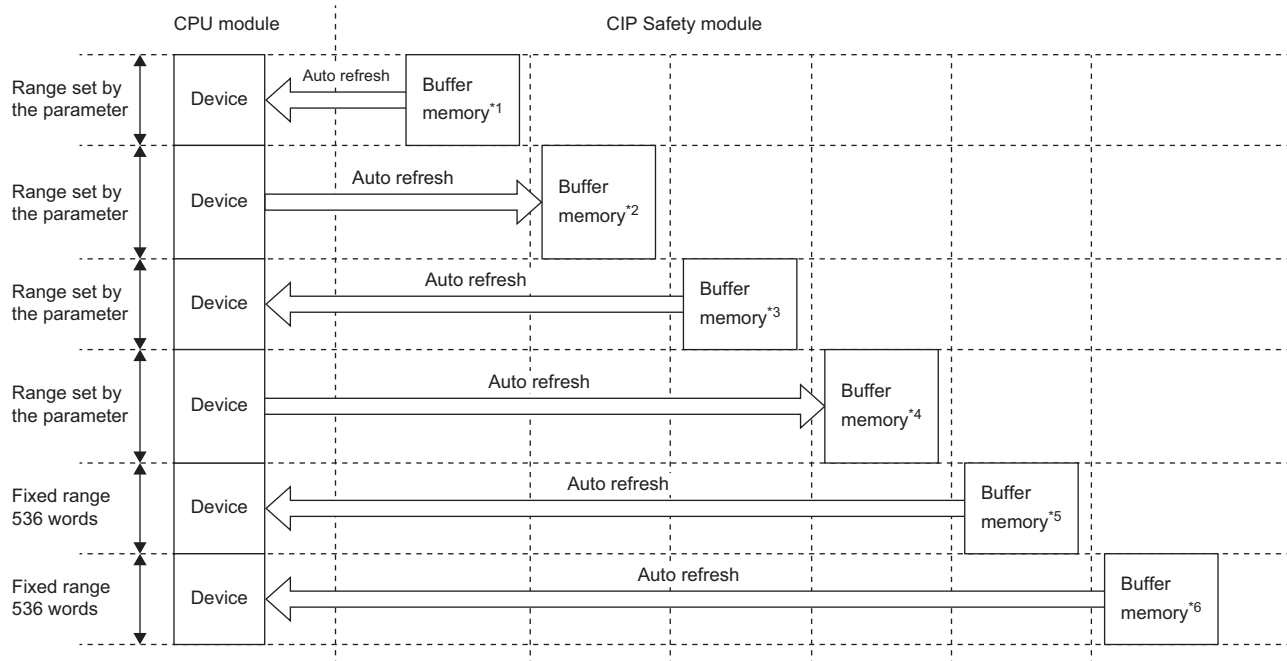
This function can be used to access the assigned device without having to directly access the buffer memory in the specified area, thereby simplifying the program.

In addition, by also enabling block assurance, data inconsistency can be prevented.

Behavior

Auto refresh is executed during the END processing of the control CPU.

Also, only the devices set in the auto refresh setting is refreshed.



*1 'Class1 Input Area (P1)' (UnG24576 to UnG57343)

*2 'Class1 Output Area (P1)' (UnG61440 to UnG94207)

*3 'Class1 Input Area (P2)' (UnG1073152 to UnG1105919)


*4 'Class1 Output Area (P2)' (UnG1110016 to UnG1142783)

*5 'Class1 communication status (P1)' (UnG99408 to UnG99447), 'Class1 Connection Behavior Error status (P1)' (UnG99584 to UnG100351)

*6 'Class1 communication status (P2)' (UnG1147984 to UnG1148023), 'Class1 Connection Behavior Error status (P2)' (UnG1148160 to UnG1148927)

Setting method

For the setting method, refer to the following.



 Page 39 Auto Refresh Setting

Buffer memory to be used

The buffer memory to be automatically refreshed is the I/O data area and status area of Class1 communications (standard communications).

Name	Address		Description
	P1	P2	
Class1 Input Area	Un\G24576 to Un\G57343	Un\G1073152 to Un\G1105919	The data receive area
Class1 Output Area	Un\G61440 to Un\G94207	Un\G1110016 to Un\G1142783	The data send area
Class1 communication status data link status (Class1)	Un\G99408 to Un\G99415	Un\G1147984 to Un\G1147991	The communication status of each connection
Class1 communication status error status (Class1)	Un\G99424 to Un\G99431	Un\G1148000 to Un\G1148007	The error status of each connection
Class1 Connection Behavior Error status input	Un\G99584 to Un\G99839	Un\G1148160 to Un\G1148415	The error code on the input side (at the time of reception) that occurred at each connection during Class1 communications is stored.
Class1 Connection Behavior Error status output	Un\G100096 to Un\G100351	Un\G1148672 to Un\G1148927	The error code on the output side (at the time of transmission) that occurred at each connection during Class1 communications is stored.

Precautions

- If block assurance is disabled, data inconsistency may occur. ( Page 107 Block Assurance)
- Since auto refresh can be set only for each area, if the connection size is changed, the program needs to be modified after the connection in which the device area is changed. Check the list of assignment destinations for each connection with the engineering tool, and modify the program as needed. ( Page 39 Auto Refresh Setting)

9.4 DLR Function

The DLR (Device Level Ring) function continues to communicate with a normally operating station even if a cable disconnection occurs or a faulty station exists in the ring configuration. In the line topology, all stations after the point of cable disconnection or faulty station are disconnected, but the data link with the normal station is maintained by using this function in a ring topology.

In the CIP Safety module, a ring configuration can be set in combination with other devices that support the DLR function. In addition, each can be a ring configuration with two networks.

Point

- When using this function, check the firmware version of the CIP Safety module and software version of CIP Safety Configuration Tool. (📖 Page 260 Added and Enhanced Functions)
- When using this function, use line configuration to configure the setting. If the ring configuration is used before configuring the setting, a broadcast storm may occur, resulting in network failure.

Ring Configuration

A ring configuration is built with one or more ring supervisors and multiple ring nodes.

The CIP Safety module is compatible with both a ring supervisor and a ring node.

For details on the installation of ring configurations, refer to the following.

📖 CIP specifications

The maximum number of ring nodes supported by the CIP Safety module is less than 50 nodes.

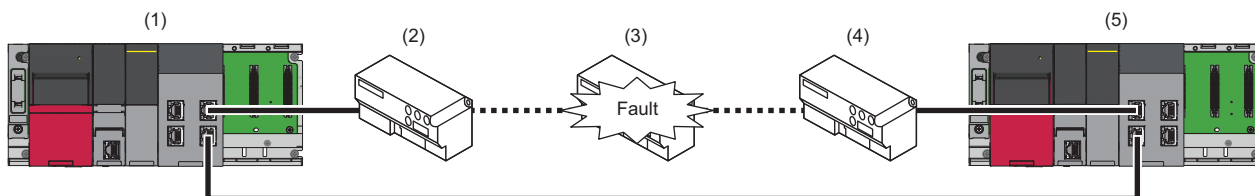
Behavior

■ For one ring supervisor

- When an error occurs in the ring node

When an error occurs in the ring node 2, the active ring supervisor detects the error, notifies each station of the error, and reconstructs the connection route.

When the error occurred in the ring node 2 is resolved, the active ring supervisor detects the recovery, notifies each station of the normal detection, and reconstructs the connection route.

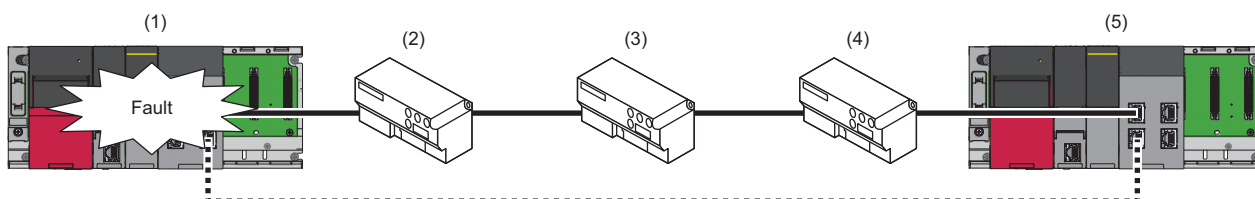


- (1) Active ring supervisor
- (2) Ring node 1
- (3) Ring node 2
- (4) Ring node 3
- (5) Ring node 4

- When an error occurs in the active ring supervisor

When an error occurs in the active ring supervisor, the stations detecting and notifying the error are disconnected, so each station cannot detect the error. The system configuration becomes a line topology state.

When the error occurred in the active ring supervisor is resolved, communications with the active ring supervisor is resumed. The system configuration is back in the ring topology state.



- (1) Active ring supervisor
- (2) Ring node 1
- (3) Ring node 2
- (4) Ring node 3
- (5) Ring node 4

■ For multiple ring supervisors

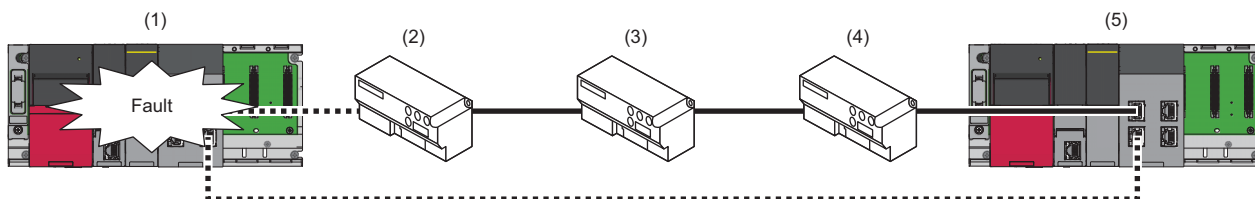
- When an error occurs in the ring node

The situation is the same as when an error occurs in a ring node with one ring supervisor. (☞ Page 111 For one ring supervisor)

- When an error occurs in the active ring supervisor

When an error occurs in the active ring supervisor, the backup ring supervisor becomes the active ring supervisor, notifying each station of the error, and reconstructing the connection route.

When the error occurred in the active ring supervisor is resolved, the station operating as the active ring supervisor returns to the backup ring supervisor.

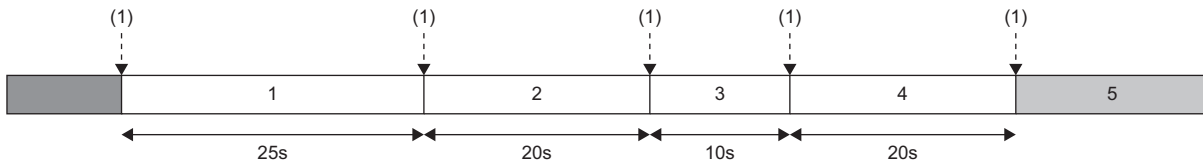


- (1) Active ring supervisor
- (2) Ring node 1
- (3) Ring node 2
- (4) Ring node 3
- (5) Backup ring supervisor → Active ring supervisor

■ When the ring fault is detected continuously

When using the CIP Safety module as the active ring supervisor, the module operates as follows.

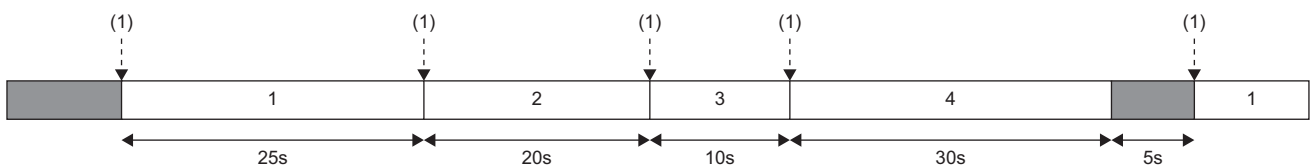
- When the ring fault within 30 seconds is detected for five consecutive times, rapid fault (high-speed fault) occurs.



(1) Ring fault detection

- 1: First time
- 2: Second time
- 3: Third time
- 4: Fourth time
- 5: Fifth time (rapid-fault status)

- The ring fault which is detected after passing 30 seconds from the last ring fault detection is counted as the first time because the condition of consecutive detection is reset.



(1) Ring fault detection

- 1: First time
- 2: Second time
- 3: Third time
- 4: Fourth time

Once the rapid fault (high-speed fault) occurs, the status is not cleared automatically. For how to check and clear the rapid fault (high-speed fault) status, refer to the following.

☞ Page 210 Communications cannot be properly performed using the DLR function

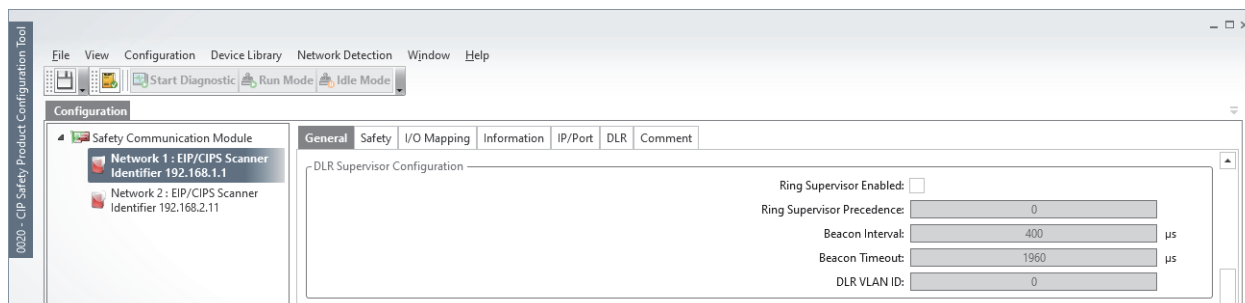
Setting method

Operating procedure

1. Start CIP Safety Configuration Tool.

[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Display the DLR Supervisor settings on the [General] tab and set the DLR parameters.



Item	Description	Setting range
Ring Supervisor Enabled	Sets whether to have the CIP Safety module operate with a ring supervisor or a ring node. <ul style="list-style-type: none"> Selected: Ring supervisor Not selected: Ring node^{*4} 	<ul style="list-style-type: none"> Selected Not selected (Default: Not checked)
Ring Supervisor Precedence	Sets the active ring supervisor if multiple ring supervisors exist. When using the CIP Safety module as the active ring supervisor, set its priority higher than that of other supervisors. The higher the value is, the higher the priority is.	0 to 255 (Default: 0)
Beacon Interval	Sets the beacon interval. ^{*1*2*3}	100μs to 100000μs (Default: 400μs)
Beacon Timeout	Sets the beacon timeout. ^{*1*2*3}	800μs to 500000μs (Default: 1960μs)
DLR VLAN ID	Sets the VLAN ID used in DLR protocol frames.	0 to 4094 (Default: 0)

^{*1} For the error detection time, refer to the following.

Page 257 Time required for detecting and recovering from ring configuration error

^{*2} If the CIP Safety module is a backup ring supervisor, it is automatically overwritten with the value of the active ring supervisor.

^{*3} Set the beacon timeout to at least twice the beacon interval.

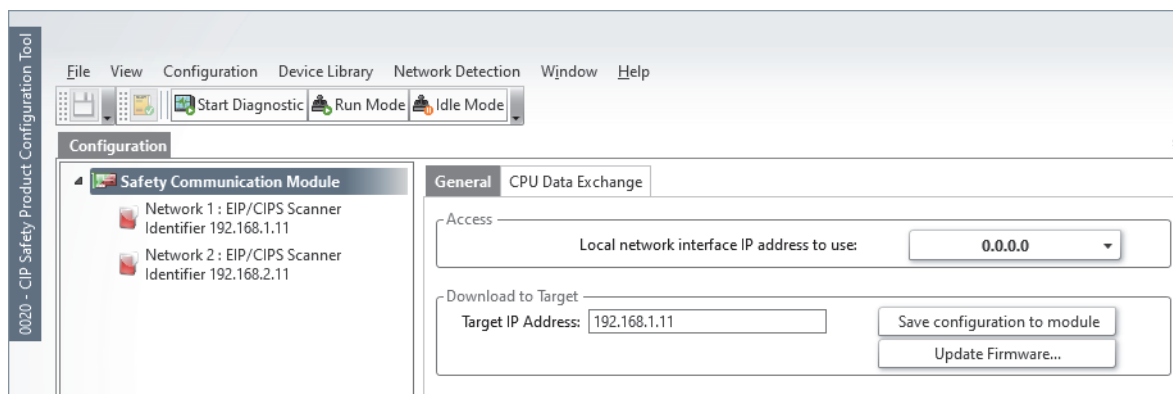
^{*4} When a ring node is selected, default (initial) values are written to the other four setting values.

Point

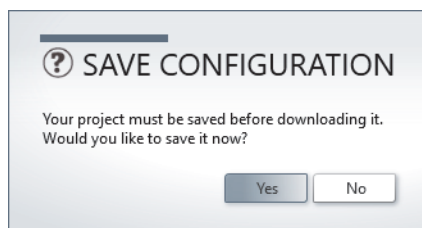
The above settings can also be set from the Device Level Ring (DLR) object. For details on the object, refer to the following.

- CIP specifications

3. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



4. Click the [Yes] button in the following window to save the configuration.



5. Reset the CPU module or power off and on the system.

Precautions


- For the ring configuration, use DLR-compliant devices. For details, refer to the manual of the device used.
- A ring configuration requires one or more ring supervisors. The ring supervisor setting is disabled by default for the CIP Safety module parameters. If a ring configuration is used without a ring supervisor, an unmanaged network group is configured. An unmanaged network group can lead multicast, unicast, or broadcast storms, possibly disrupting network communications.
- When the CIP Safety module operates as a ring node, it operates as a beacon method node.
- If the cable disconnection frequently occurs, the communications may not be performed.
- The CIP Safety module has four ports, but some port combinations do not accept the ring configuration. The following table shows the port combinations which can accept the ring configuration.

Port to be connected		Ring configuration acceptability
P1-A	P1-B	Yes
P1-A	P2-A	No
P1-A	P2-B	No
P1-B	P2-A	No
P1-B	P2-B	No
P2-A	P2-B	Yes

9.5 Safety Diagnostic Function

The following table shows the safety diagnostic functions of the CIP Safety module.

This information can be checked in the [Error Information] tab of the "Module Diagnostics" window of the CIP Safety module.

( Page 205 Error information)

Item		Description	Diagnostic timing	Error code	Action
Memory diagnostics	RAM diagnostics	Detects an error in the memory installed in the CIP Safety module.	<ul style="list-style-type: none"> • At powering off and on • At reset • During operation 	3E00H, 3E01H	The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative.
	Firmware diagnostics	Diagnoses whether the firmware is corrupt.	<ul style="list-style-type: none"> • At powering off and on • At reset 	3E02H, 3E03H	
System diagnostics	MPU/MCU diagnostics	Diagnoses whether an error has occurred in the MPU/MCU.	<ul style="list-style-type: none"> • At powering off and on • At reset • During operation 	3E10H to 3E2FH	
	Firmware operation diagnostics	Diagnoses whether firmware is functioning normally.	During operation	3E04H to 3E07H	
Power supply voltage monitoring	Power supply voltage monitoring	Diagnoses whether power is being supplied correctly.	During operation	3E08H, 3E09H	

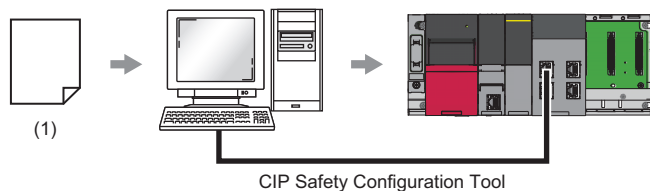
9.6 Firmware Update

This function updates the firmware of the CIP Safety module.

Execute the function with CIP Safety Configuration Tool.

Point

- All communications are stopped during the firmware update. Stop equipment targeted for the firmware update and confirm the safety before executing the update.
- This function is available when the software version of CIP Safety Configuration Tool is "1.3.0.28" or later.



(1) Firmware file

A firmware file is read to CIP Safety Configuration Tool and is directly written to the CIP Safety module.

The firmware update is prioritized over standard communications and safety communications when it is executed during these communications.

Communication type			Behavior
Standard communications	Class1 communications	Instance communications	Instance communications are stopped and the firmware update is executed.
		Tag communications	Tag communications are stopped and the firmware update is executed.
	UCMM communications	Message communications	Message communications are stopped and the firmware update is executed.
Safety communications	Class0 communications	Instance communications	Instance communications are stopped and the firmware update is executed.
		Tag communications	Tag communications are stopped and the firmware update is executed.

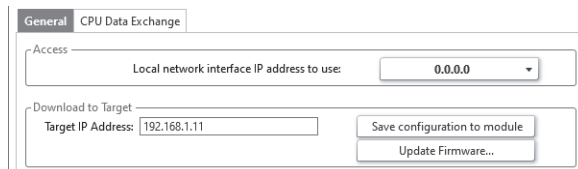
Firmware update procedure

Operating procedure

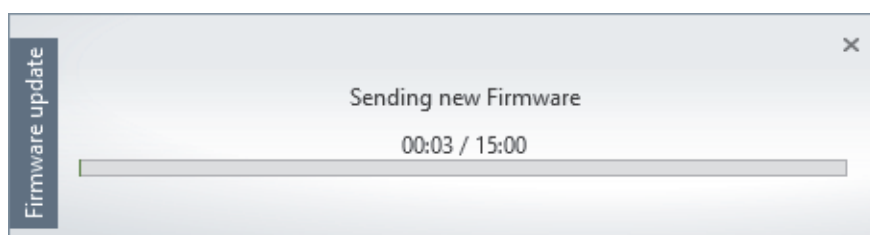
1. Start CIP Safety Configuration Tool.

☞ [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

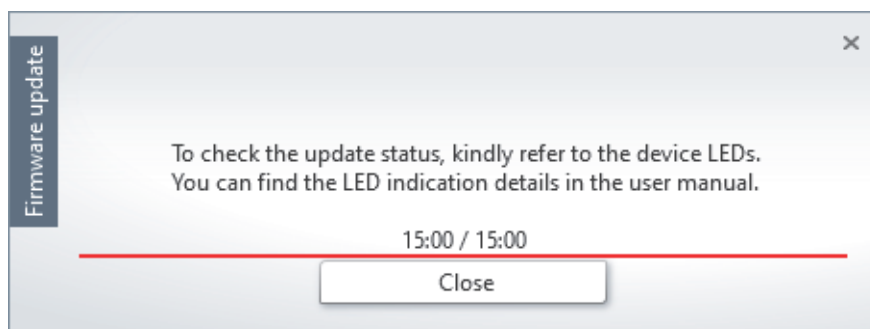
2. Click the [Update Firmware] button, and select the firmware file of the CIP Safety module.



3. The following window appears and the firmware update starts. The MS LED and NS LED flash in orange. It takes a few minutes for the firmware update to be completed.

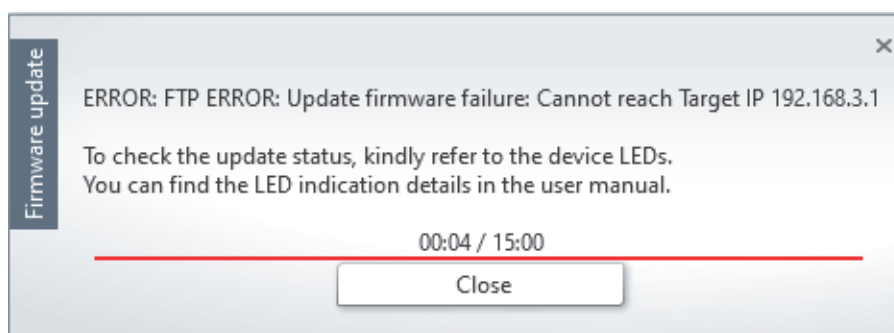


The following window is displayed when the firmware update is performed. Judge whether the writing has completed or has failed by the LED status such as MS LED.



4. After the color of MS LED and NS LED flashing changes to green, power off and on the system. After checking the writing completion with the LED status, close the firmware update window with the [×] button in the upper right corner.
 - When the writing is completed, the MS LED and NS LED flash in green.
 - When the writing fails, the MS LED and NS LED flash in red.
5. Check that a new firmware version is displayed in the product information list of the system monitor of the engineering tool.

- Do not reset the CPU module or power off and on the system until the MS LED and NS LED start flashing in green. Doing so may cause a failure of the CIP Safety module, and the module may become unusable.
- An error (2450H: module major error) occurs on the CPU module some time after the firmware update execution. Therefore, confirm that stopping the system does not cause any problems before executing the firmware update.
- The LEDs status during firmware update is not reflected on the "Module Diagnostics" window of the engineering tool.
- After the firmware update starts, the NS LED indication may change due to a factor such as communication status change. In such a case, judge the firmware update status by the LED status such as MS LED.
- When communication with the CIP Safety module cannot be established due to an incorrect target IP address or for other reasons, the following window appears and the firmware update does not start. Check the CIP Safety module state.



■LEDs during firmware update

Firmware update state	RUN LED	ERR LED	MS LED	NS LED
Writing	Off	Off	Flashing (orange)	Flashing (orange)
Writing completed			Flashing (green)	Flashing (green)
Writing failed			Flashing (red)	Flashing (red)

Precautions

Performing any of the following operations during firmware update may cause an error completion of the update, disabling the CIP Safety module start or a second firmware update. Therefore, pay full attention when executing the firmware update.

- Power-off or reset
- Operating status change using the remote operation from the engineering tool or the switch of the CPU module
- Operation from an external device
- Connection/disconnection of the module targeted for the firmware update
- Firmware update start operation from the engineering tool

10 PROGRAMMING

Default settings are used for parameters that are not described in this chapter.

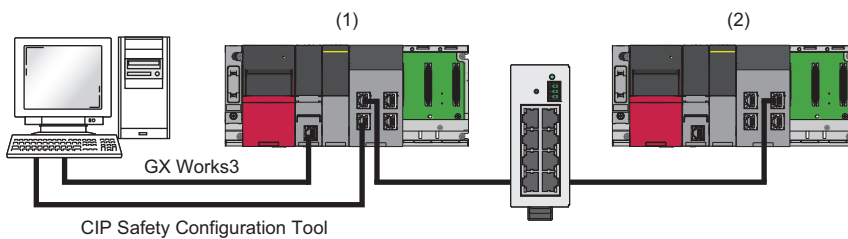
10.1 Class1 Instance Communications

This section describes examples of performing Class1 instance communications between the originator and the target.

System configuration example

The following system configuration is used for the examples of Class1 instance communications.

System configuration



(1) Programmable controller system (originator)

- Power supply module: R61P
- CPU module: R08SF CPU
- Safety function module: R6SFM
- CIP Safety module: RJ71SEIP91-T4 (P1)*¹

(2) Programmable controller system (target)

- Power supply module: R61P
- CPU module: R08SF CPU
- Safety function module: R6SFM
- CIP Safety module: RJ71SEIP91-T4 (P2)*²

*1 IP address (P1): 192.168.3.51, subnet mask: 255.255.255.0

IP address (P2): 192.168.0.5, subnet mask: 255.255.255.0

*2 IP address (P1): 192.168.0.6, subnet mask: 255.255.255.0

IP address (P2): 192.168.3.2, subnet mask: 255.255.255.0

Parameter settings

Set parameters using the engineering tool and CIP Safety Configuration Tool.

Settings using the engineering tool

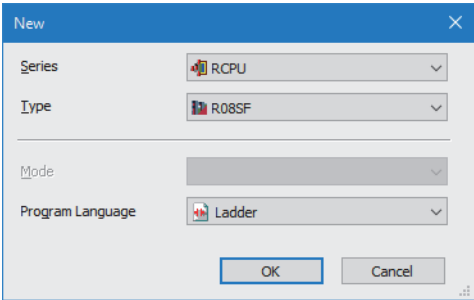
Connect the engineering tool to the CPU module and set the parameters.

■Parameter settings for the CIP Safety module (originator)

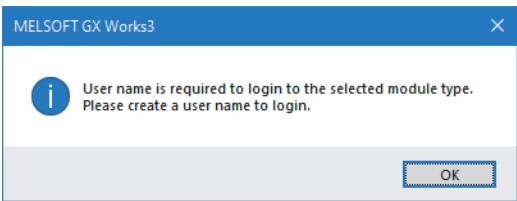
Operating procedure

1. Set the CPU module as follows.

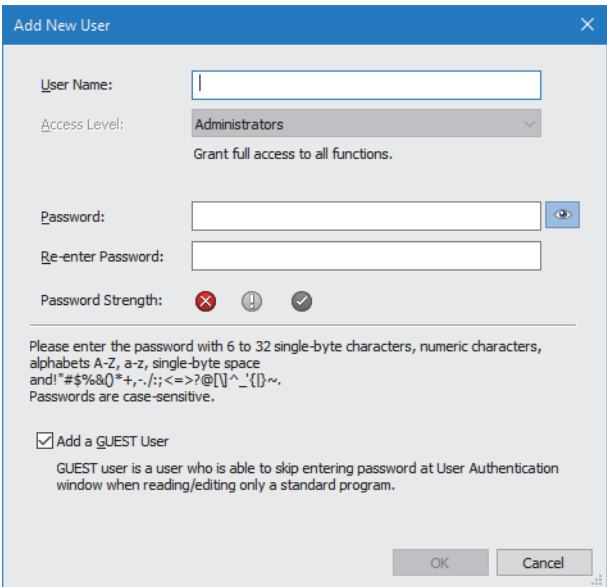
 [Project] ⇒ [New]



2. Click the [OK] button.

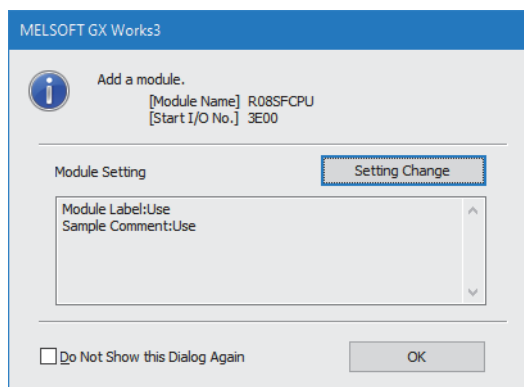


3. Set the item and click the [OK] button.



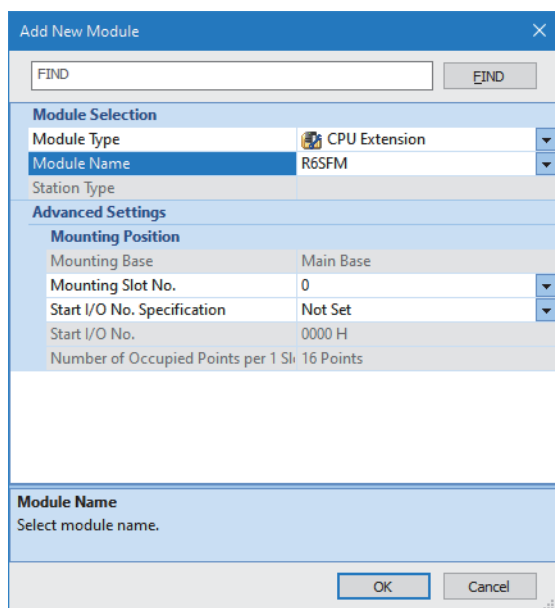
4. Set the items in the "Save as" window and click the [Save] button.

5. Click the [Setting Change] button to set to use the module label.

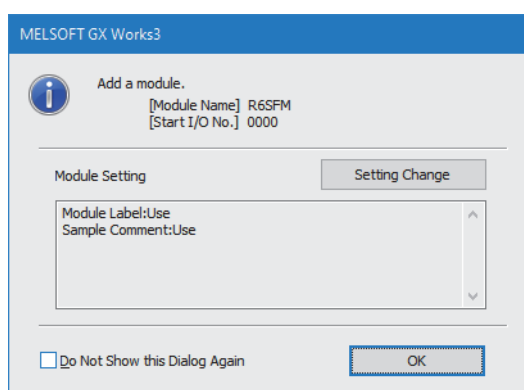


6. Set the safety function module as follows.


[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ Right-click ⇒ [Add New Module]

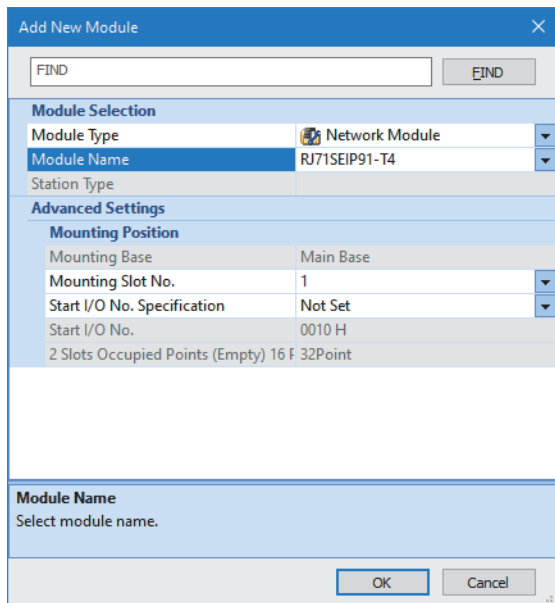


7. Click the [OK] button in the following window to add the safety function module labels of the CPU module.



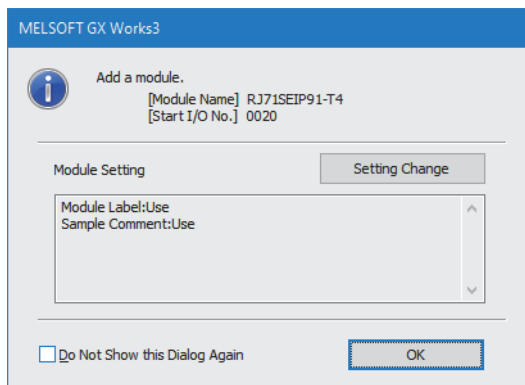
8. Set the CIP Safety module as follows.

 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ Right-click ⇒ [Add New Module]




The 'Add New Module' dialog box is shown. It has a 'FIND' input field and a 'FIND' button at the top. Below is the 'Module Selection' section with 'Module Type' set to 'Network Module' and 'Module Name' set to 'RJ71SEIP91-T4'. The 'Station Type' field is empty. The 'Advanced Settings' section includes 'Mounting Position' with 'Mounting Base' set to 'Main Base' and 'Mounting Slot No.' set to '1'. 'Start I/O No. Specification' is set to 'Not Set', and 'Start I/O No.' is set to '0010 H'. A note indicates '2 Slots Occupied Points (Empty) 16 F 32Point'. At the bottom, there is a 'Module Name' section with the text 'Select module name.' and 'OK' and 'Cancel' buttons.

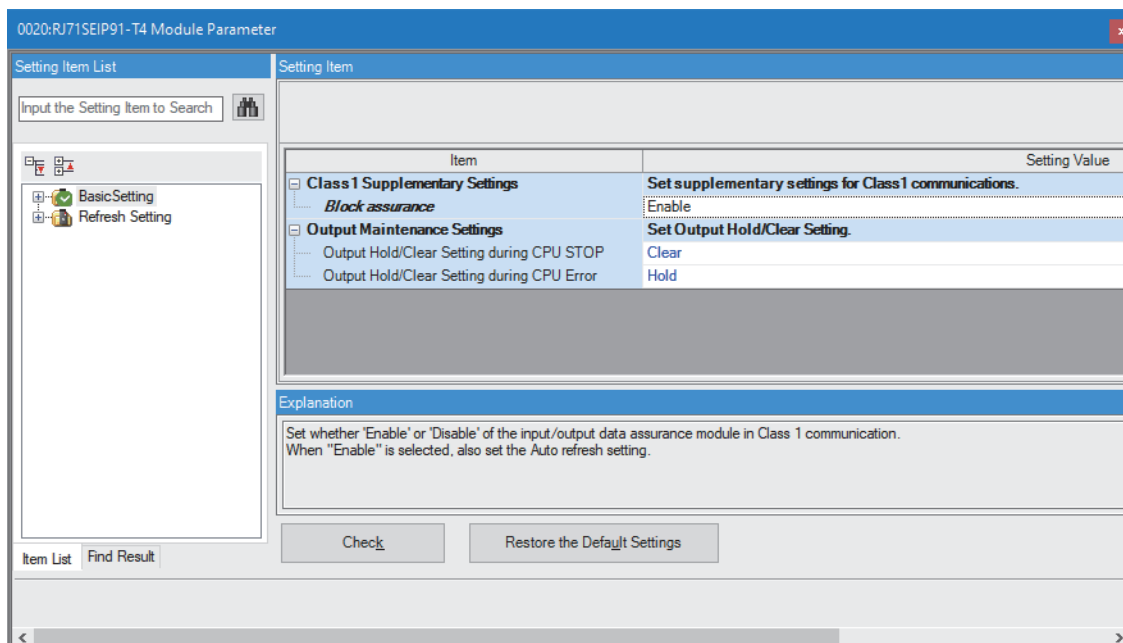
9. Click the [OK] button to add the CIP Safety module labels of the CPU module.



The 'MELSOFT GX Works3' window shows the 'Add a module.' dialog box. It displays the module name '[Module Name] RJ71SEIP91-T4' and the start I/O number '[Start I/O No.] 0020'. Below is the 'Module Setting' section with a 'Setting Change' button. The 'Module Label:Use' and 'Sample Comment:Use' fields are visible. At the bottom, there is a checkbox for 'Do Not Show this Dialog Again' and an 'OK' button.

10. Set the items in "Basic Setting" as follows.

 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [Module Parameter] ⇒ [Basic Setting]




Item	Setting Value
Class1 Supplementary Settings	Set supplementary settings for Class1 communications.
Block assurance	Enable
Output Maintenance Settings	Set Output Hold/Clear Setting.
Output Hold/Clear Setting during CPU STOP	Clear
Output Hold/Clear Setting during CPU Error	Hold

Explanation


Set whether 'Enable' or 'Disable' of the input/output data assurance module in Class 1 communication.
When "Enable" is selected, also set the Auto refresh setting.

Check Restore the Default Settings

11. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

 [Online] ⇒ [Write to PLC]

■Parameter settings for the CIP Safety module (target)

The settings are the same as the CIP Safety module (originator). ( Page 121 Parameter settings for the CIP Safety module (originator))

Settings using CIP Safety Configuration Tool

Connect CIP Safety Configuration Tool to the CIP Safety module, and set parameters.

■Parameter settings for the CIP Safety module (originator)

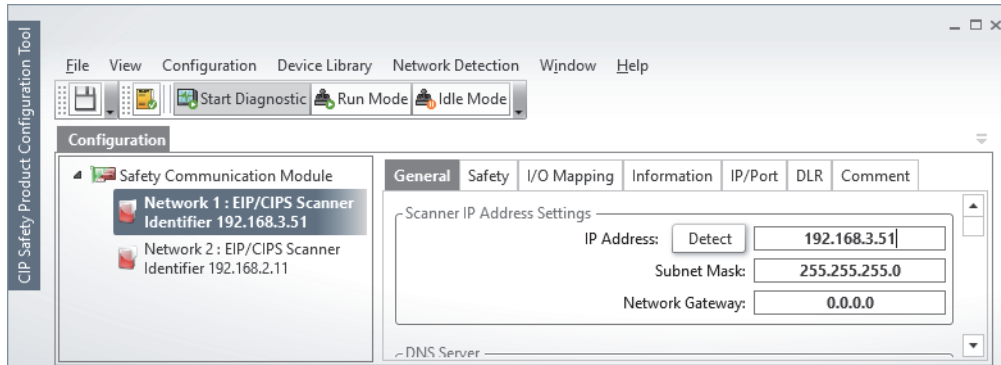
Operating procedure

1. Start CIP Safety Configuration Tool.

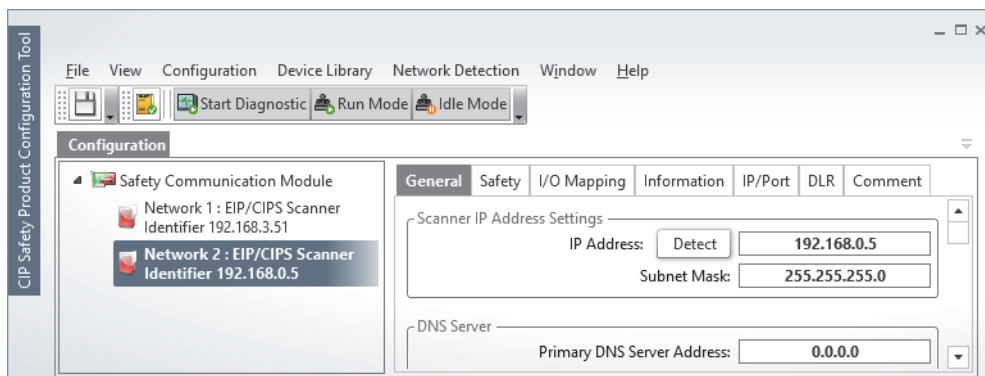
☞ [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.3.51 to "IP Address" (P1).



- Select "Network 2: EIP/CIPS Scanner" and set 192.168.0.5 to "IP Address" (P2).



3. Register an EDS file of the external device (target).

In this program example, registration of the EDS file is not required because the external device is the CIP Safety module.

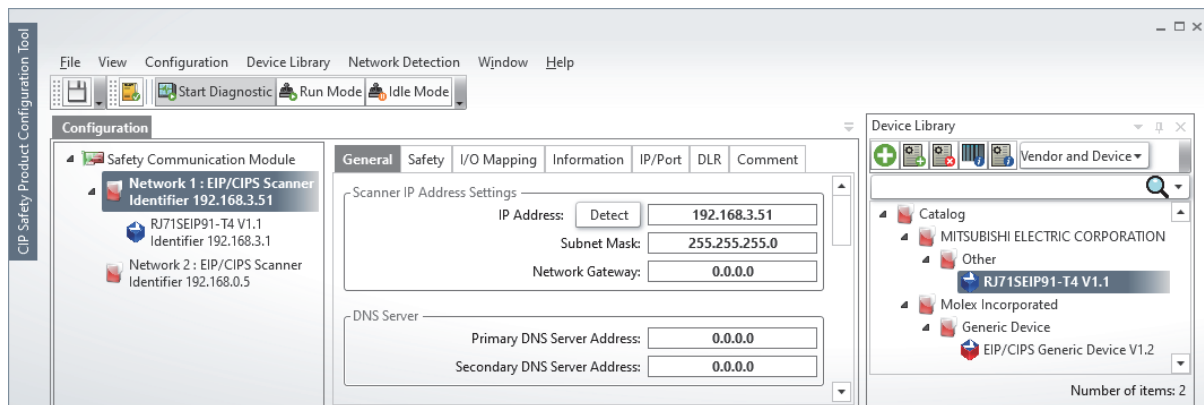


To connect an external device whose EDS file is not registered as the target, register the EDS file of the device to the library. Once the EDS file is registered, re-registration is not required.

To register the EDS file, use the [Add EDS] icon in [Device Library] in CIP Safety Configuration Tool.

☞ Page 81 Adding EDS files

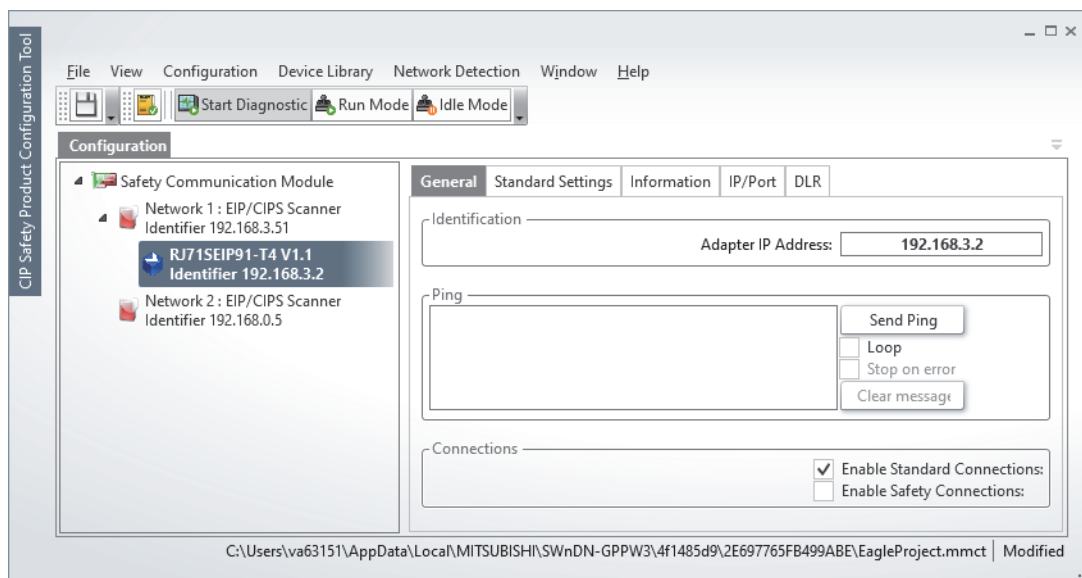
4. Add (drag and drop) the external device (target) to "Network 1: EIP/CIPS Scanner".



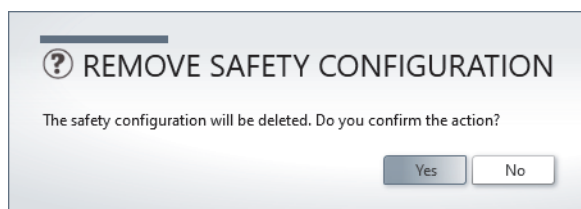
5. Set the external device (target) added.

- [General] tab

Item	Setting value
Adapter IP Address	192.168.3.2
Enable Standard Connections	Selected
Enable Safety Connections	Not selected ^{*1}



*1 When changing the tick mark from "selected" to "not selected" and if the following window appears, select "Yes".

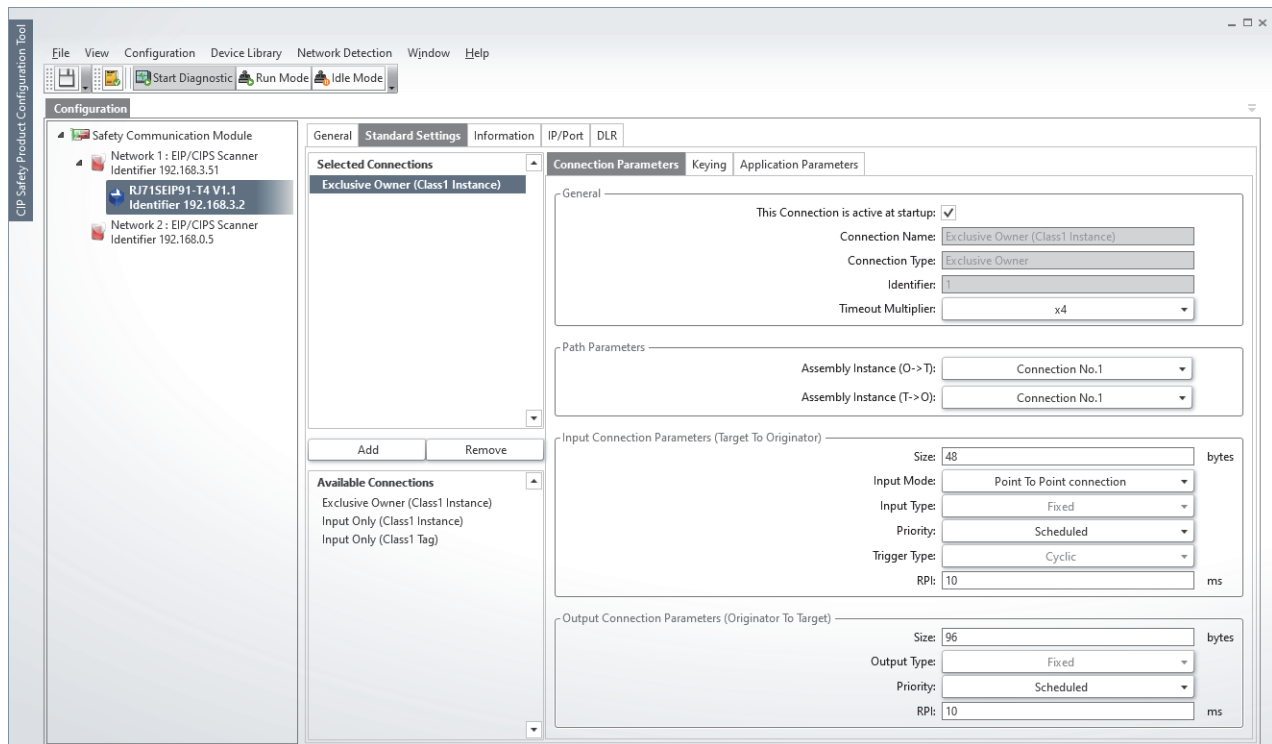


- [Standard Settings] tab

Select "Exclusive Owner (Class1 Instance)" in "Selected Connections" and set the following.

Item	Setting value	
General	This Connection is active at startup	Selected
Input Connection Parameters (Target To Originator)	Size	48
	RPI	10
Output Connection Parameters (Originator To Target)	Size	96
	RPI	10

10

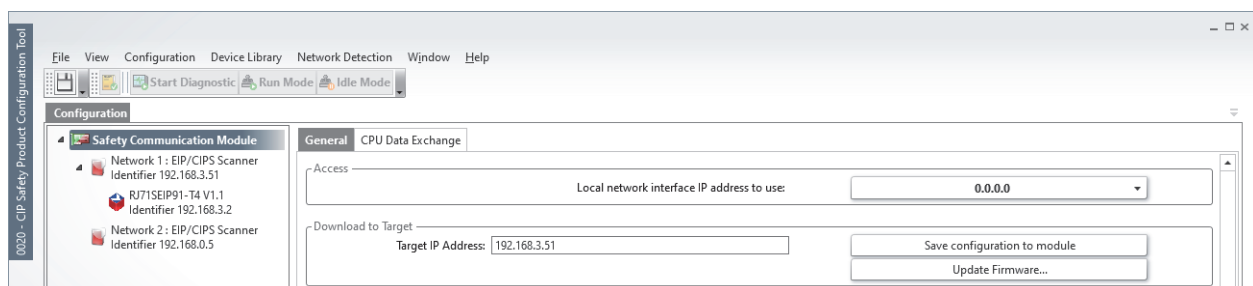


6. Select "Safety Communication Module" and set the current IP address of the CIP Safety module to "Target IP Address".

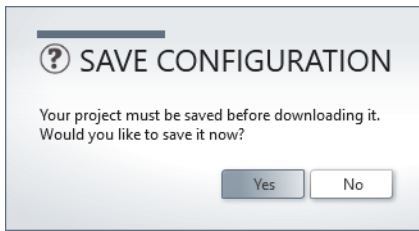


The current IP address of the CIP Safety module can be checked on the system monitor of the engineering tool.

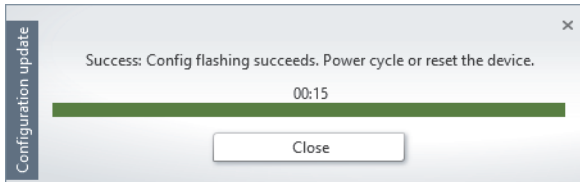
7. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



8. Click the [Yes] button in the following window to save the configuration.



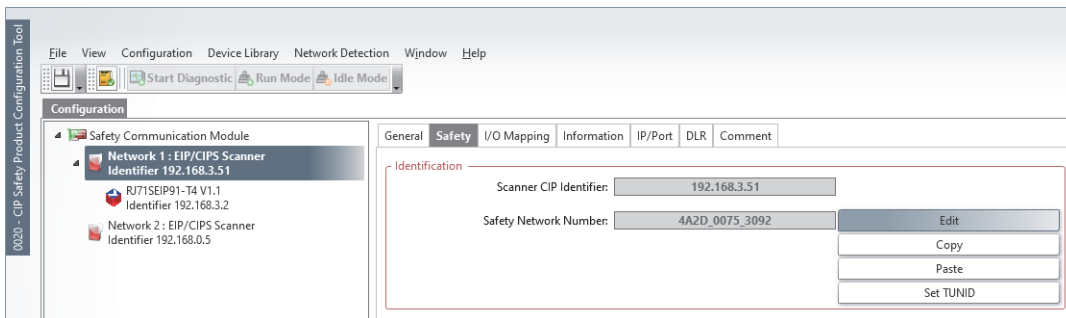
9. Click the [Close] button in the following window.



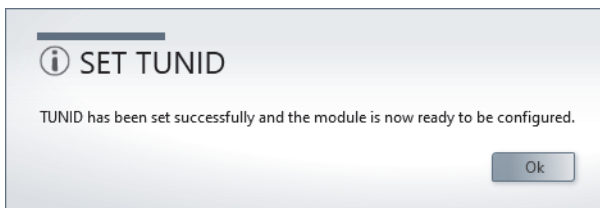
10. After downloading, reset the CPU module or power off and on the system.

11. Click the [Set TUNID] button.

🖱️ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

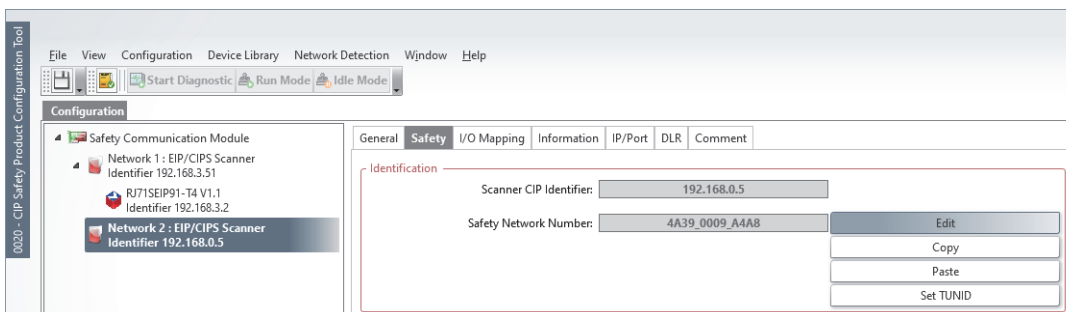


12. Click the [OK] button in the following window.

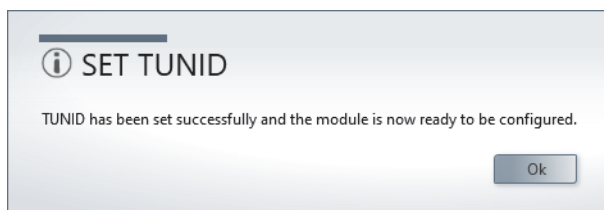


13. Click the [Set TUNID] button.

🖱️ "Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab

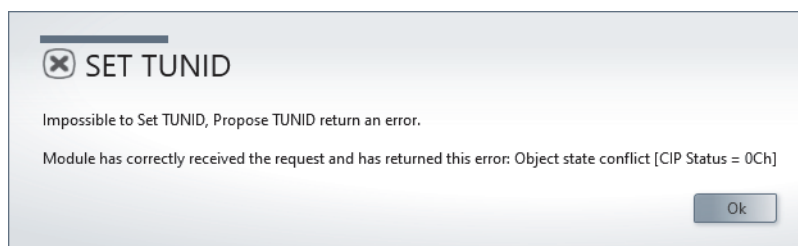


14. Click the [OK] button in the following window.



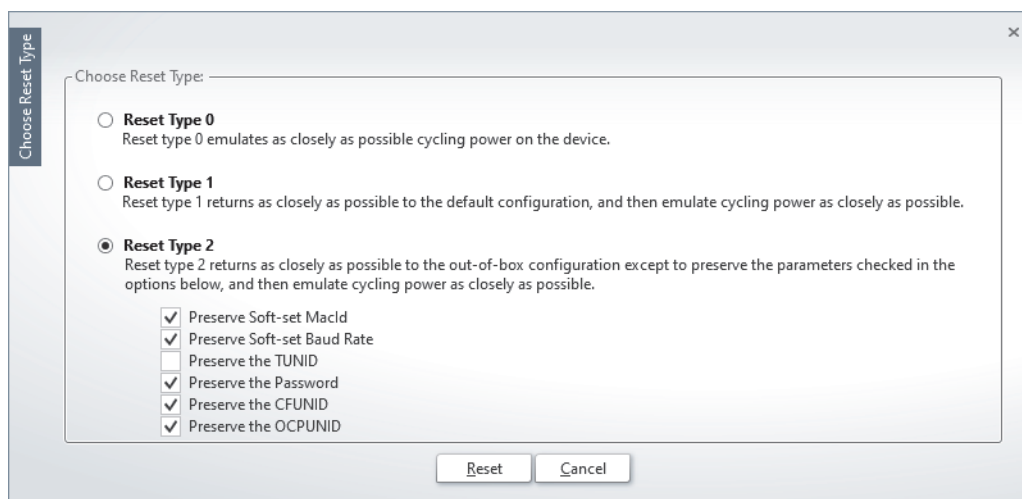
Point

If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.



(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
- When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off

(4) Reset the CPU module or power off and on the system.

15. Close CIP Safety Configuration Tool.

16. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

[Online] ⇒ [Write to PLC]

■Parameter settings for the CIP Safety module (target)

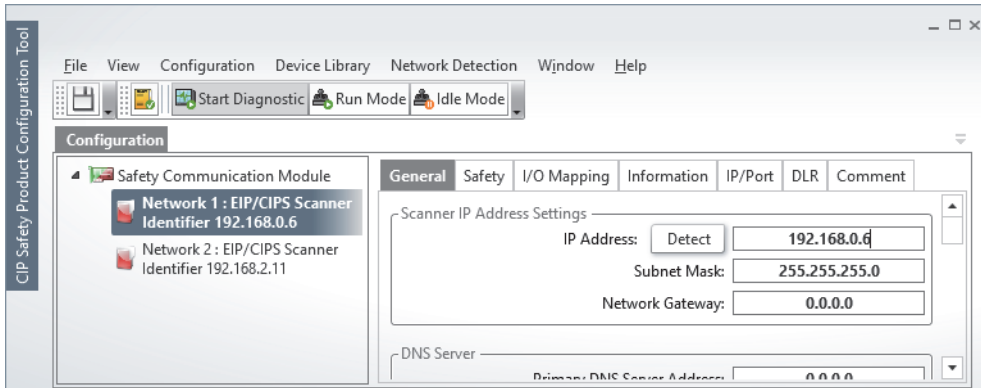
Operating procedure

1. Start CIP Safety Configuration Tool.

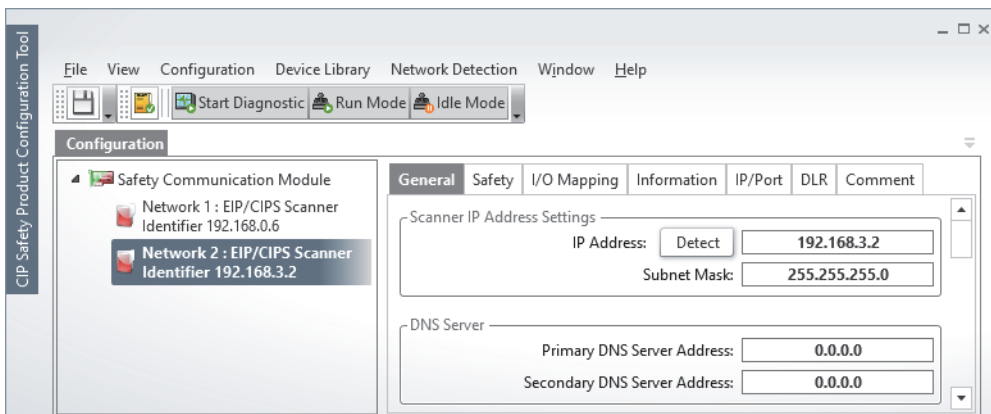
🖱️ [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.0.6 to "IP Address" (P1).



- Select "Network 2: EIP/CIPS Scanner" and set 192.168.3.2 to "IP Address" (P2).



3. Set "Network 2: EIP/CIPS Scanner".

- [General] tab

Item		Setting value
Operating Mode	Target (Class1)	Selected

The screenshot shows the 'CIP Safety Product Configuration Tool' window. The 'Configuration' tab is active, and the 'General' sub-tab is selected for 'Network 2: EIP/CIPS Scanner' (Identifier 192.168.3.2). The 'Scanner IP Address Settings' section shows 'IP Address' as '192.168.3.2' and 'Subnet Mask' as '255.255.255.0'. The 'DNS Server' section shows 'Primary DNS Server Address' and 'Secondary DNS Server Address' both as '0.0.0.0'. The 'Module Name' section has 'Host Name' and 'Domain Name' fields. The 'Ports Settings' section shows 'Port 1 baud rate' and 'Port 2 baud rate' both set to 'auto negotiation'. The 'Ping' section has a 'Send Ping' button and checkboxes for 'Loop' and 'Stop on error'. The 'Operating Mode' section shows 'Target (Class 1)' selected. The 'Configuration Summary' section shows various connection and packet limits.

- [Target (Class1)] tab

Click the [Add] button in "Target (Class1 Instance) definitions" and set the following.

Item		Setting value
Target (Class1 Instance) definitions	T->O Size	48
	O->T Size	96

The screenshot shows the 'CIP Safety Product Configuration Tool' window with the 'Target (Class 1)' tab selected. The 'Target (Class 1 Instance) definitions' section contains a table with one entry:

Connection	T->O Size	O->T Size	Active on startup
1	48	96	<input checked="" type="checkbox"/>

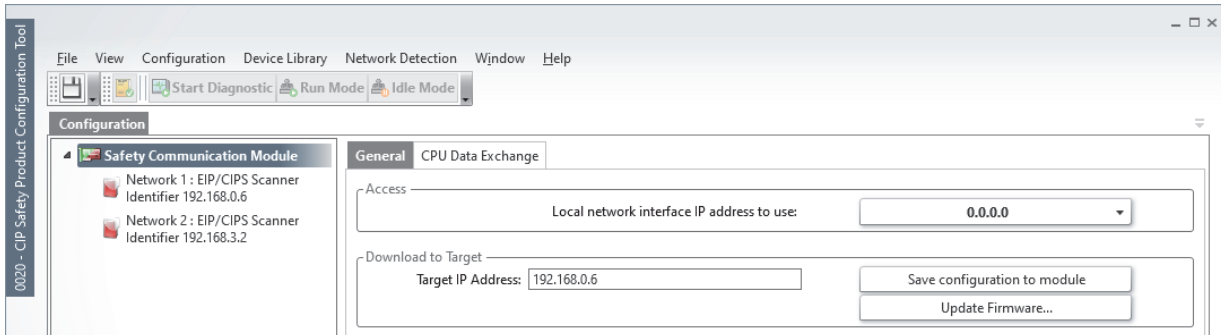
The 'Target (Class 1 Tag) definitions' section is empty. A note at the bottom states: '(O means Originator so it is an external scanner that will connect to the local slave - T means Target so this is the local slave)'.

4. Select "Safety Communication Module" and set the current IP address of the CIP Safety module to "Target IP Address".

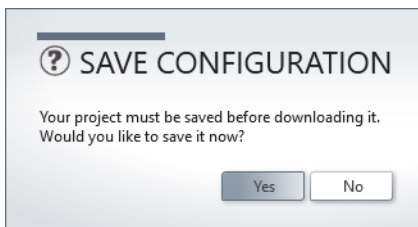


The current IP address of the CIP Safety module can be checked on the system monitor of the engineering tool.

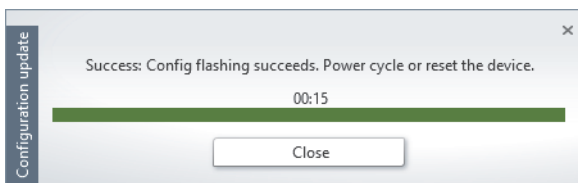
5. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



6. Click the [Yes] button in the following window to save the configuration.



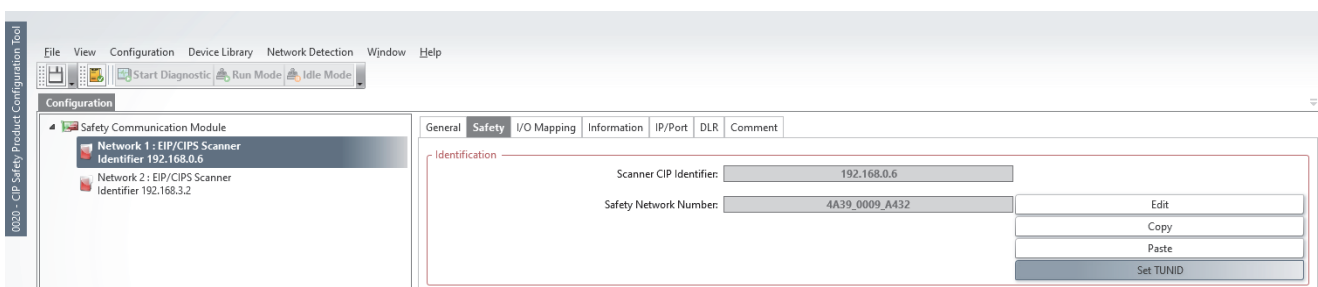
7. Click the [Close] button in the following window.



8. After downloading, reset the CPU module or power off and on the system.

9. Click the [Set TUNID] button.

"Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

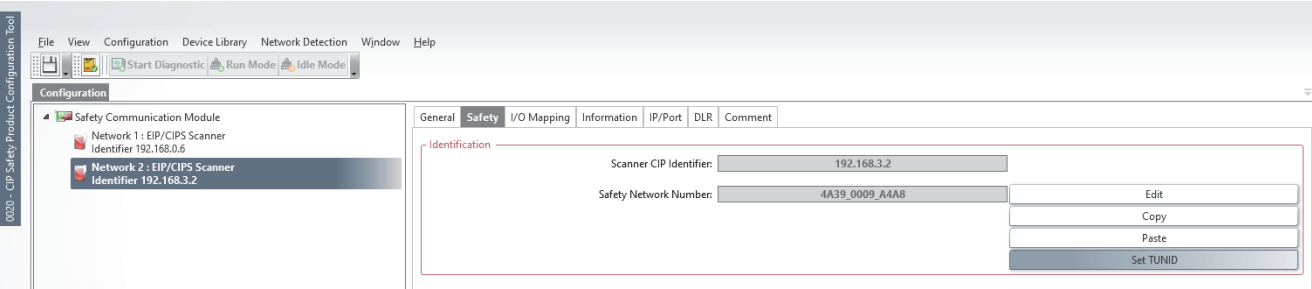


10. Click the [OK] button in the following window.



11. Click the [Set TUNID] button.

"Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab



12. Click the [OK] button in the following window.

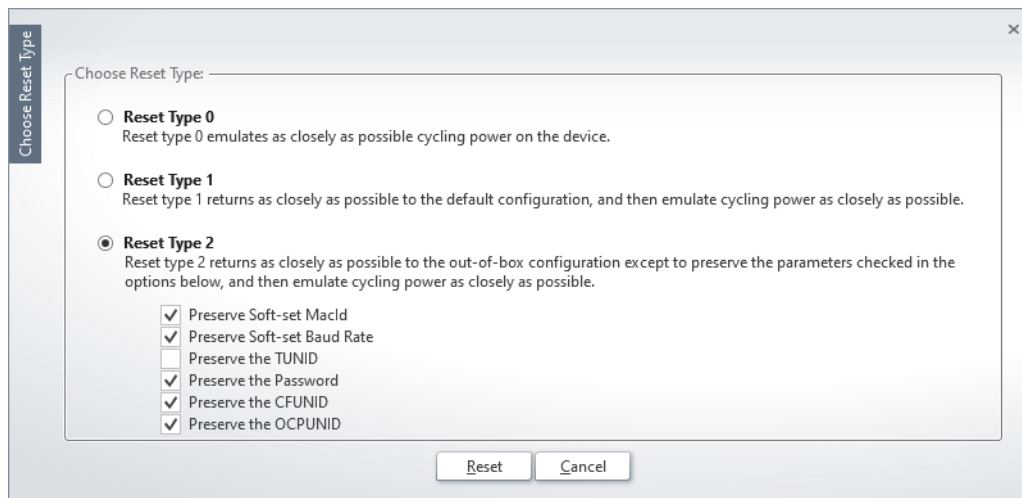


If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.



(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
- When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off

(4) Reset the CPU module or power off and on the system.

13. Close CIP Safety Configuration Tool.

14. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

[Online] ⇨ [Write to PLC]

Auto Refresh Setting

1. Set the Auto refresh setting.

☞ [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ Right-click ⇒ [Auto Refresh Setting]

2. Write the set parameter to the CPU module in the following window and reset the CPU module or power off and on the system.

☞ [Online] ⇒ [Write to PLC]

■Setting the CIP Safety module (originator)

'Class1 Input Area' (Un\G24576 to Un\G57343)	
Start Address	End Address
D0	D23

CIP Safety Module Auto Refresh Setting

User CPU Device: ☒ Assign Devices per Buffer

Output devices (IQ-R CPU -> CIP Safety) | Input devices (IQ-R CPU <- CIP Safety)

Buffer	Start Address	End Address
Class1 Status(P1)		
Class1 Status(P2)		
Class1 Input(P1)	D0	D23
Class1 Input(P2)		

OK Cancel

'Class1 Output Area' (Un\G61440 to Un\G94207)	
Start Address	End Address
D100	D147

CIP Safety Module Auto Refresh Setting

User CPU Device: ☒ Assign Devices per Buffer

Output devices (IQ-R CPU -> CIP Safety) | Input devices (IQ-R CPU <- CIP Safety)

Buffer	Start Address	End Address
Class1 Output(P1)	D100	D147
Class1 Output(P2)		

OK Cancel

■Setting the CIP Safety module (target)

'Class1 Input Area' (Un\G1073152 to Un\G1105919)	
Start Address	End Address
D1000	D1047

CIP Safety Module Auto Refresh Setting

User CPU Device: ☒ Assign Devices per Buffer

Output devices (I-Q-R CPU -> CIP Safety) | Input devices (I-Q-R CPU <- CIP Safety)

Buffer	Start Address	End Address
Class1 Status(P1)		
Class1 Status(P2)		
Class1 Input(P1)		
Class1 Input(P2)	D1000	D1047

OK Cancel

'Class1 Output Area' (Un\G1110016 to Un\G1142783)	
Start Address	End Address
D1050	D1073

CIP Safety Module Auto Refresh Setting

User CPU Device: ☒ Assign Devices per Buffer

Output devices (I-Q-R CPU -> CIP Safety) | Input devices (I-Q-R CPU <- CIP Safety)

Buffer	Start Address	End Address
Class1 Output(P1)		
Class1 Output(P2)	D1050	D1073

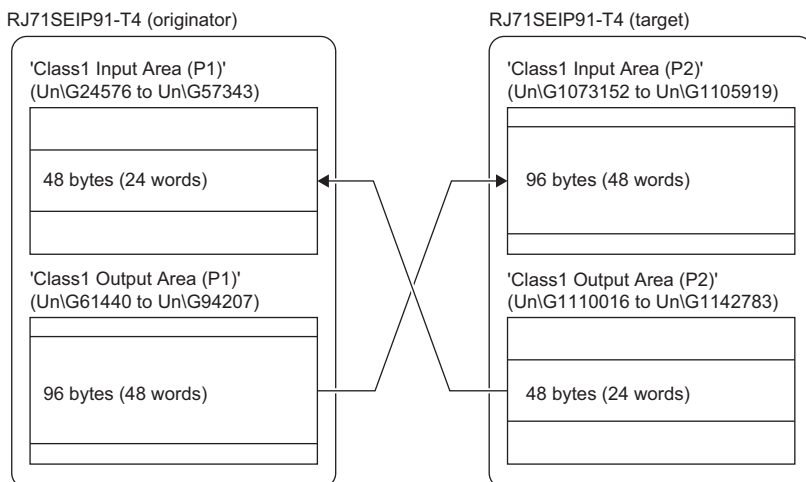
OK Cancel

Program example

48 bytes (24 words) of data are received from 'Class1 Output Area (P2)' (Un\G1110016 to Un\G1142783) of the target to 'Class1 Input Area (P1)' (Un\G24576 to Un\G57343) of the originator.

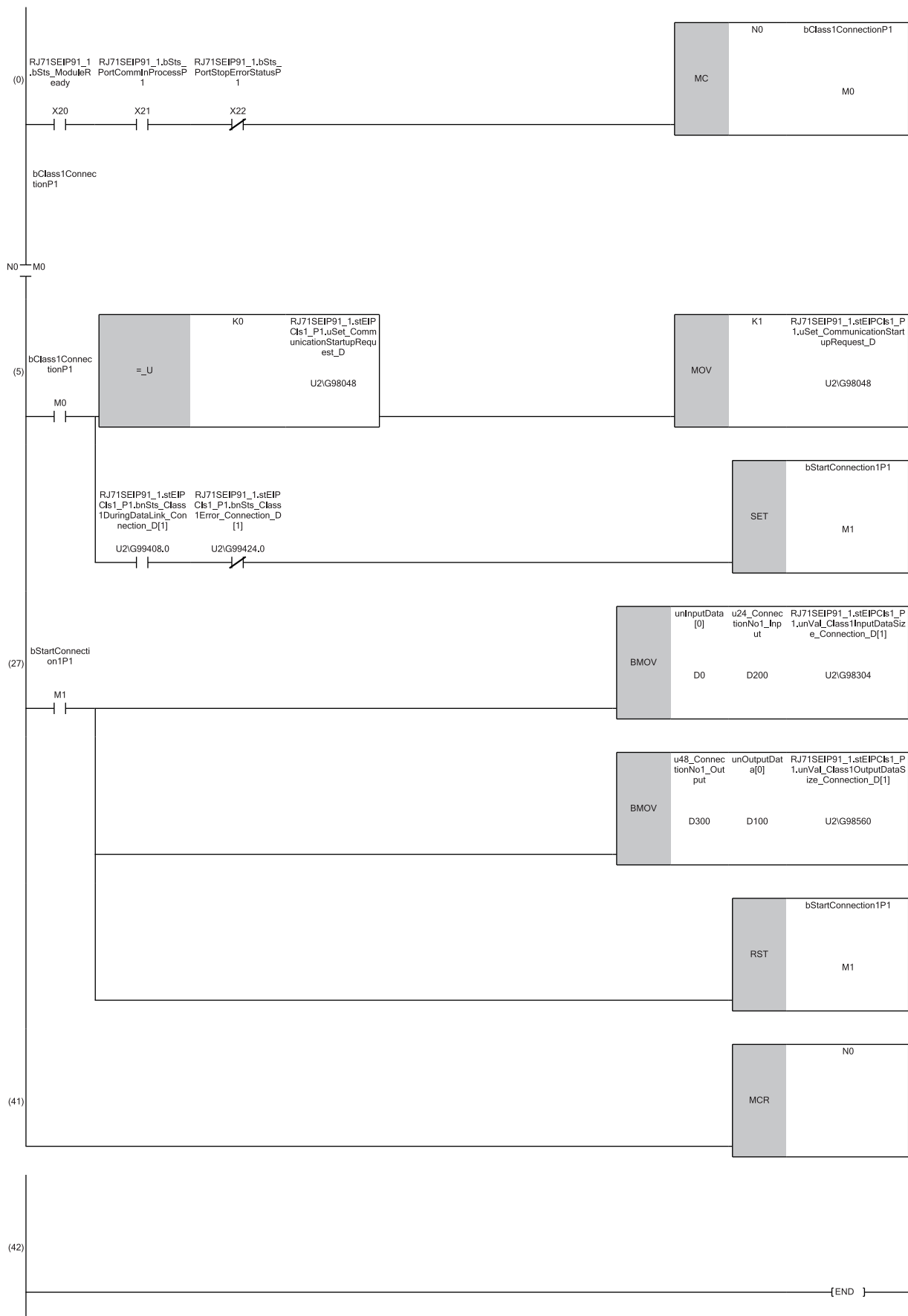
Also, 96 bytes (48 words) of data are sent from 'Class1 Output Area (P1)' (Un\G61440 to Un\G94207) of the originator to 'Class1 Input Area (P2)' (Un\G1073152 to Un\G1105919) of the target.

RPI is 10ms.



Program for the CIP Safety module (originator)

Classification	Label name	Description	Device
Module label	RJ71SEIP91_1.bSts_ModuleReady	Module READY	X20
	RJ71SEIP91_1.bSts_PortCommInProcessP1	Port start status (P1)	X21
	RJ71SEIP91_1.bSts_PortStopErrorStatusP1	Port stop error status (P1)	X22
	RJ71SEIP91_1.stEIPCls1_P1.uSet_CommunicationStartupRequest_D	EtherNet/IP communication start request	U2\G98048
	RJ71SEIP91_1.stEIPCls1_P1.bnSts_Class1DuringDataLink_Connection_D[1]	Data link status (Class1)	U2\G99408.0
	RJ71SEIP91_1.stEIPCls1_P1.bnSts_Class1Error_Connection_D[1]	Error status (Class1)	U2\G99424.0
	RJ71SEIP91_1.stEIPCls1_P1.unVal_Class1InputDataSize_Connection_D[1]	Class1 Input data size	U2\G98304
	RJ71SEIP91_1.stEIPCls1_P1.unVal_Class1OutputDataSize_Connection_D[1]	Class1 Output data size	U2\G98560
Label to be defined	Define global labels as shown below.		
	Label Name	Data Type	Class Assign (Device/Label)
	1 bClass1ConnectionP1	Bit	VAR_GLOBAL M0
	2 bStartConnection1P1	Bit	VAR_GLOBAL M1
	3 unInputData	Word [Unsigned]/Bit String [16-bit](0..23)	VAR_GLOBAL D0
	4 unOutputData	Word [Unsigned]/Bit String [16-bit](0..47)	VAR_GLOBAL D100
	5 u24_ConnectionNo1_Input	Word [Unsigned]/Bit String [16-bit](0..23)	VAR_GLOBAL D200
	6 u48_ConnectionNo1_Output	Word [Unsigned]/Bit String [16-bit](0..47)	VAR_GLOBAL D300



(0) Configure an interlock by using X20, X21, and X22.

(5) If U2\G98048 has not been requested once, a start request will be issued.

U2\G99408.0 and U2\G99424.0 are checked and the processing is started.

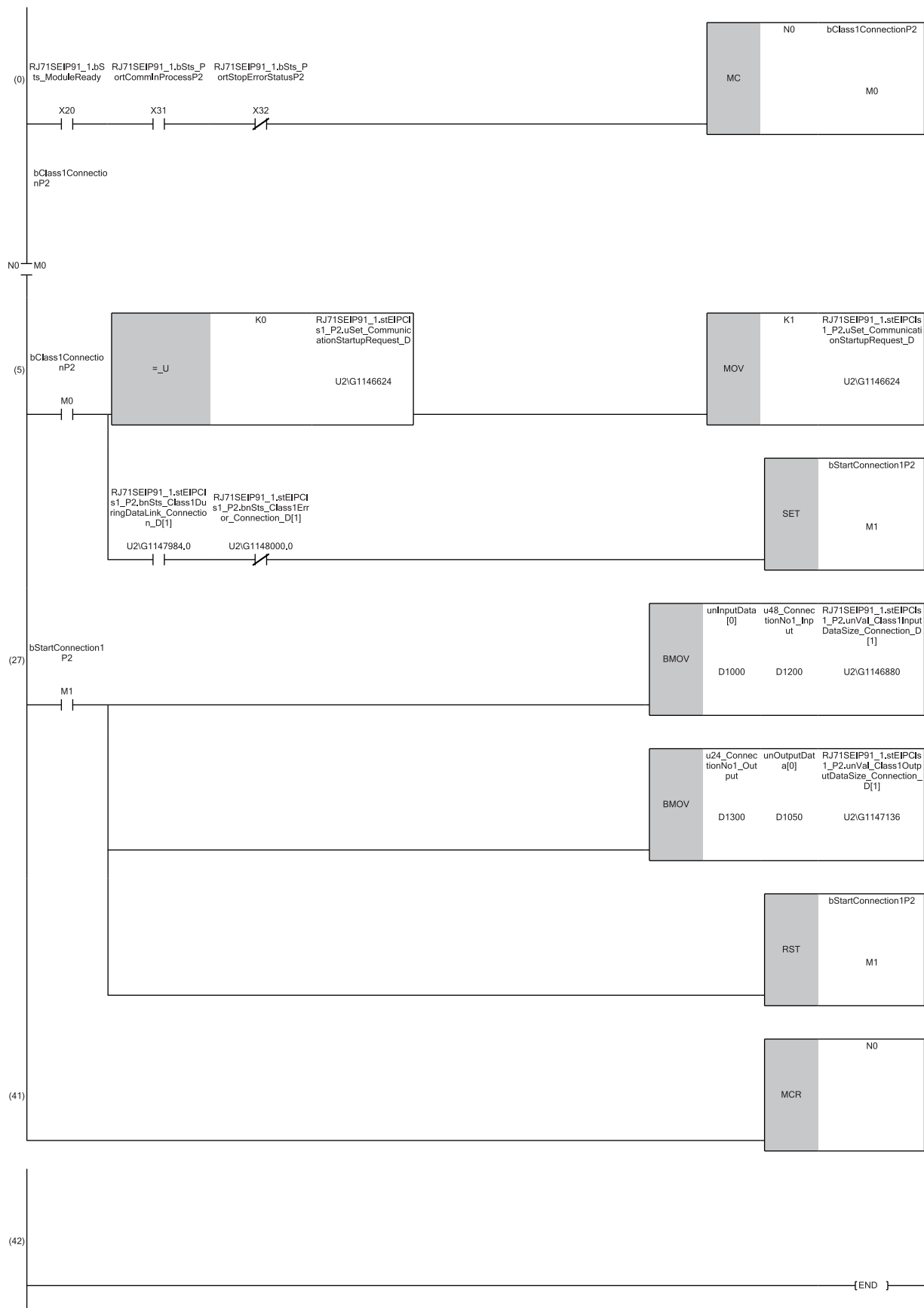
(27) Input data of D0 is acquired for D200 and output data of D300 is set to D100.

(41) The processing is completed.

Program for the CIP Safety module (target)

Classification	Label name	Description	Device
Module label	RJ71SEIP91_1.bSts_ModuleReady	Module READY	X20
	RJ71SEIP91_1.bSts_PortCommInProcessP2	Port start status (P2)	X31
	RJ71SEIP91_1.bSts_PortStopErrorStatusP2	Port stop error status (P2)	X32
	RJ71SEIP91_1.stEIPCls1_P2.uSet_CommunicationStartupRequest_D	EtherNet/IP communication start request	U2\G1146624
	RJ71SEIP91_1.stEIPCls1_P2.bnSts_Class1DuringDataLink_Connection_D[1]	Data link status (Class1)	U2\G1147984.0
	RJ71SEIP91_1.stEIPCls1_P2.bnSts_Class1Error_Connection_D[1]	Error status (Class1)	U2\G1148000.0
	RJ71SEIP91_1.stEIPCls1_P2.unVal_Class1InputDataSize_Connection_D[1]	Class1 Input data size	U2\G1146880
	RJ71SEIP91_1.stEIPCls1_P2.unVal_Class1OutputDataSize_Connection_D[1]	Class1 Output data size	U2\G1147136
Label to be defined	Define global labels as shown below.		

	Label Name	Data Type	Class	Assign (Device/Label)
1	bClass1ConnectionP2	Bit	VAR_GLOBAL	M0
2	bStartConnection1P2	Bit	VAR_GLOBAL	M1
3	unInputData	Word [Unsigned]/Bit String [16-bit](0..47)	VAR_GLOBAL	D1000
4	unOutputData	Word [Unsigned]/Bit String [16-bit](0..23)	VAR_GLOBAL	D1050
5	u48_ConnectionNo1_Input	Word [Unsigned]/Bit String [16-bit](0..47)	VAR_GLOBAL	D1200
6	u24_ConnectionNo1_Output	Word [Unsigned]/Bit String [16-bit](0..23)	VAR_GLOBAL	D1300



- (0) Configure an interlock by using X20, X31, and X32.
- (5) If U2\G1146624 has not been requested once, a start request will be issued.
U2\G1147984.0 and U2\G1148000.0 are checked and the processing is started.
- (27) Input data of D1000 is acquired for D1200 and output data of D1300 is set to D1050.
- (41) The processing is completed.

10.2 Class1 Tag Communications

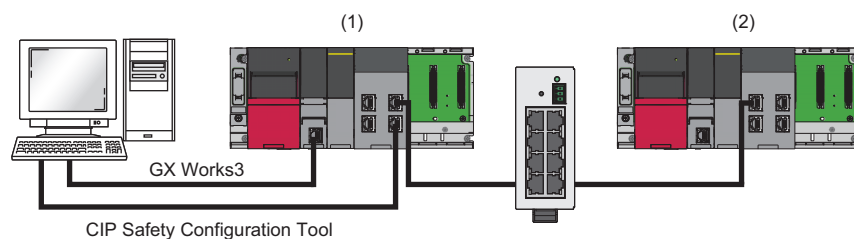
This section describes an example of Class1 tag communications between the consumer and the producer.

System configuration example

The following system configuration is used for the example of Class1 tag communications.

10

System configuration



(1) Programmable controller system (consumer)

- Power supply module: R61P
- CPU module: R08SF CPU
- Safety function module: R6SFM
- CIP Safety module: RJ71SEIP91-T4 (P2)*1

(2) Programmable controller system (producer)

- Power supply module: R61P
- CPU module: R08SF CPU
- Safety function module: R6SFM
- CIP Safety module: RJ71SEIP91-T4 (P1)*2

*1 IP address (P1): 192.168.3.51, subnet mask: 255.255.255.0

IP address (P2): 192.168.0.5, subnet mask: 255.255.255.0


*2 IP address (P1): 192.168.0.6, subnet mask: 255.255.255.0

IP address (P2): 192.168.3.2, subnet mask: 255.255.255.0

Parameter settings

Set parameters using the engineering tool and CIP Safety Configuration Tool.

Settings using the engineering tool

The settings procedure is the same as Class1 instance communications. ( Page 121 Settings using the engineering tool)
Replace the following terms.

- Originator → Consumer
- Target → Producer


Settings using CIP Safety Configuration Tool

Connect CIP Safety Configuration Tool to the CIP Safety module, and set parameters.

■Parameter settings for the CIP Safety module (consumer)

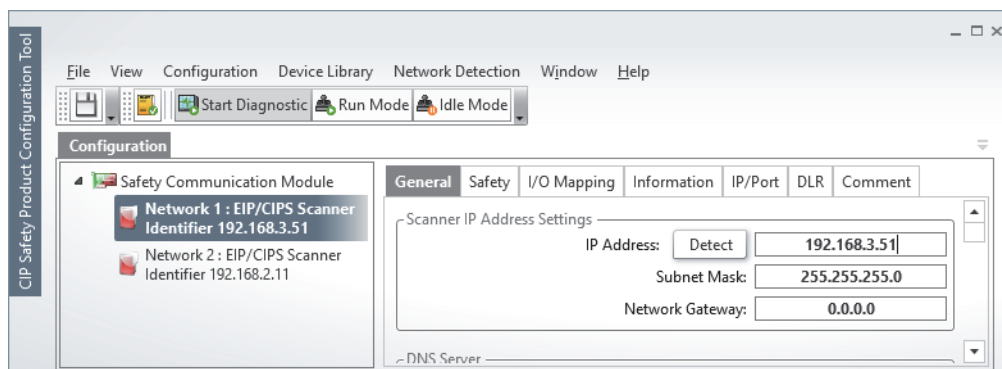
Operating procedure

1. Start CIP Safety Configuration Tool.

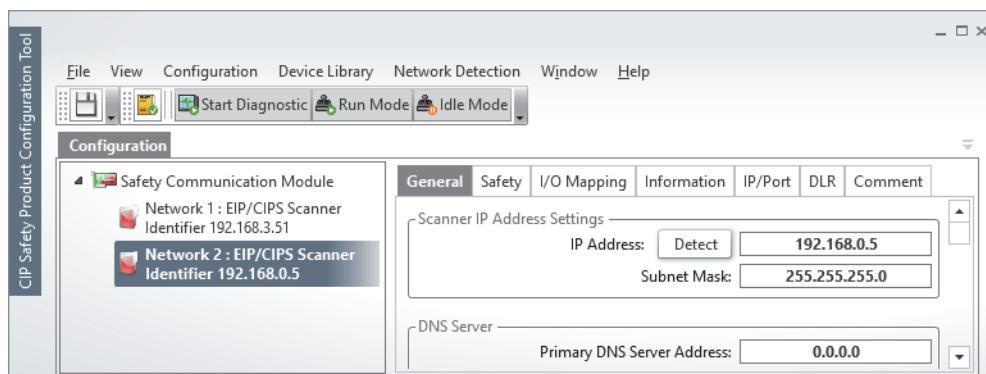
 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.3.51 to "IP Address" (P1).



- Select "Network 2: EIP/CIPS Scanner" and set 192.168.0.5 to "IP Address" (P2).



3. Register an EDS file of the external device (producer).

In this program example, registration of the EDS file is not required because the external device is the CIP Safety module.

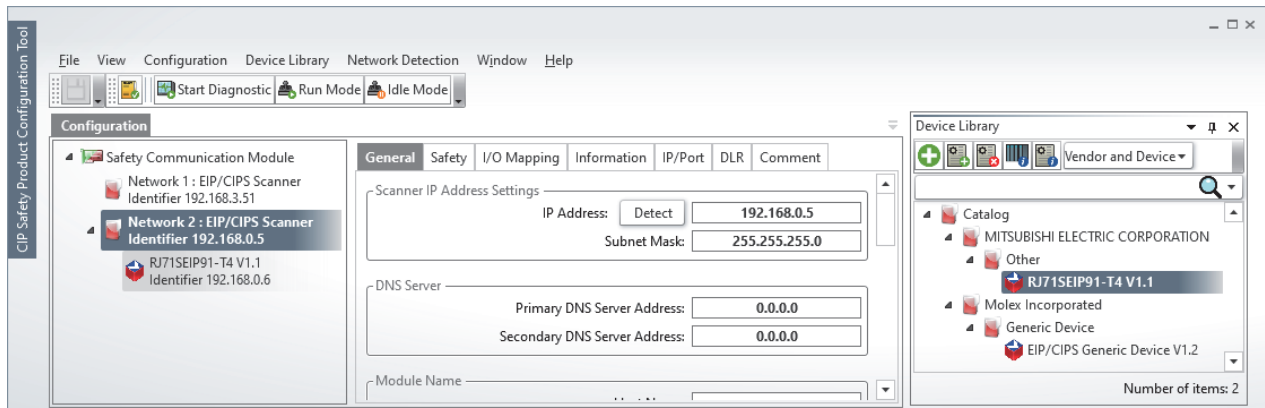
Point

To connect an external device whose EDS file is not registered as the producer, register the EDS file of the device to the library. Once the EDS file is registered, re-registration is not required.

To register the EDS file, use the [Add EDS] icon in [Device Library] in CIP Safety Configuration Tool.

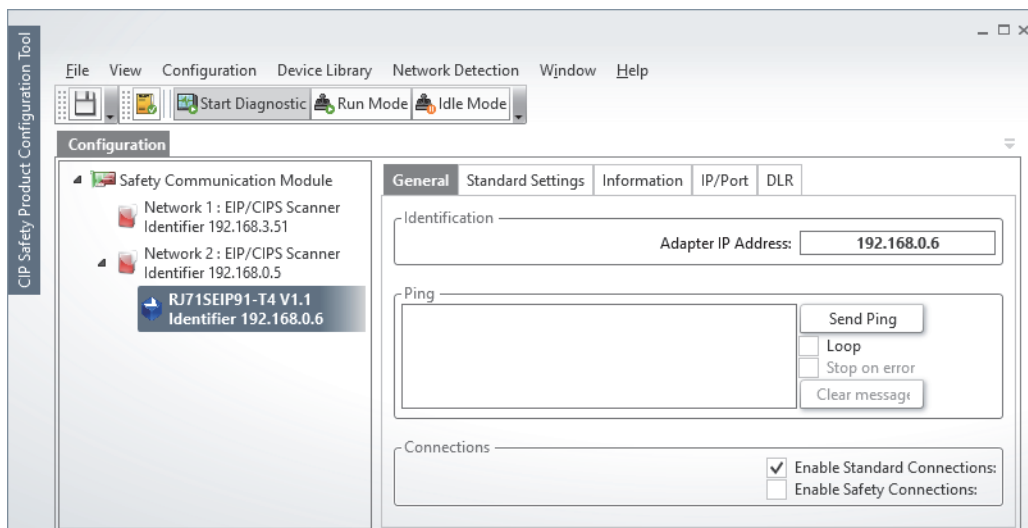
 Page 81 Adding EDS files

4. Add (drag and drop) the external device (producer) to "Network 2: EIP/CIPS Scanner".

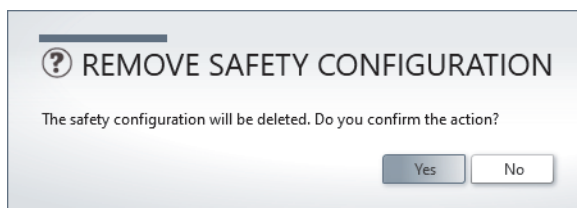


5. Set the setting values in the [General] tab.

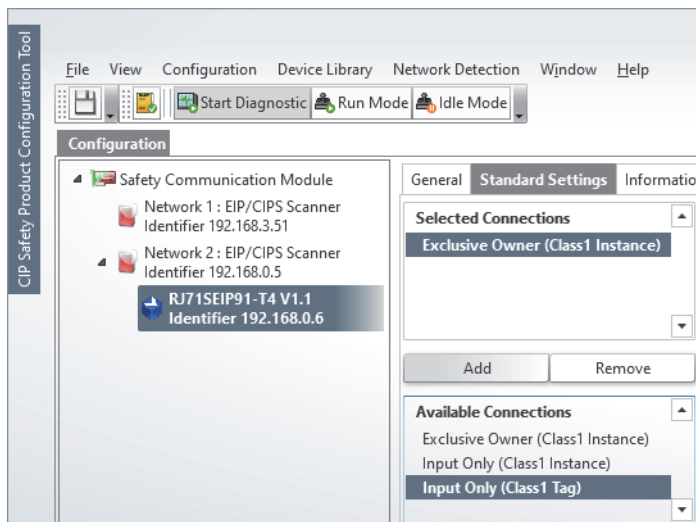
Item	Setting value
Adapter IP Address	192.168.0.6
Enable Standard Connections	Selected
Enable Safety Connections	Not selected ^{*1}



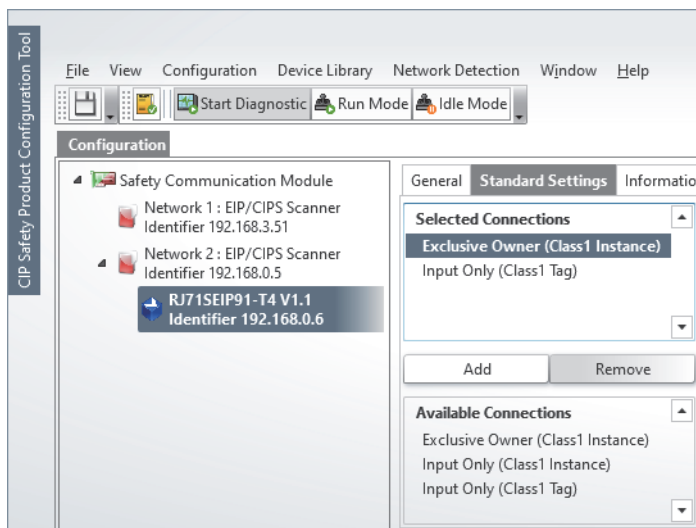
*1 When changing the tick mark from "selected" to "not selected" and if the following window appears, select "Yes".



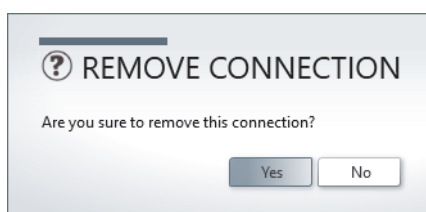
6. Select "Input Only (Class1 Tag)" in "Available Connections" in the [Standard Settings] tab and then click the [Add] button.



7. Select "Exclusive Owner (Class1 Instance)" in "Selected Connections" and click the [Remove] button.



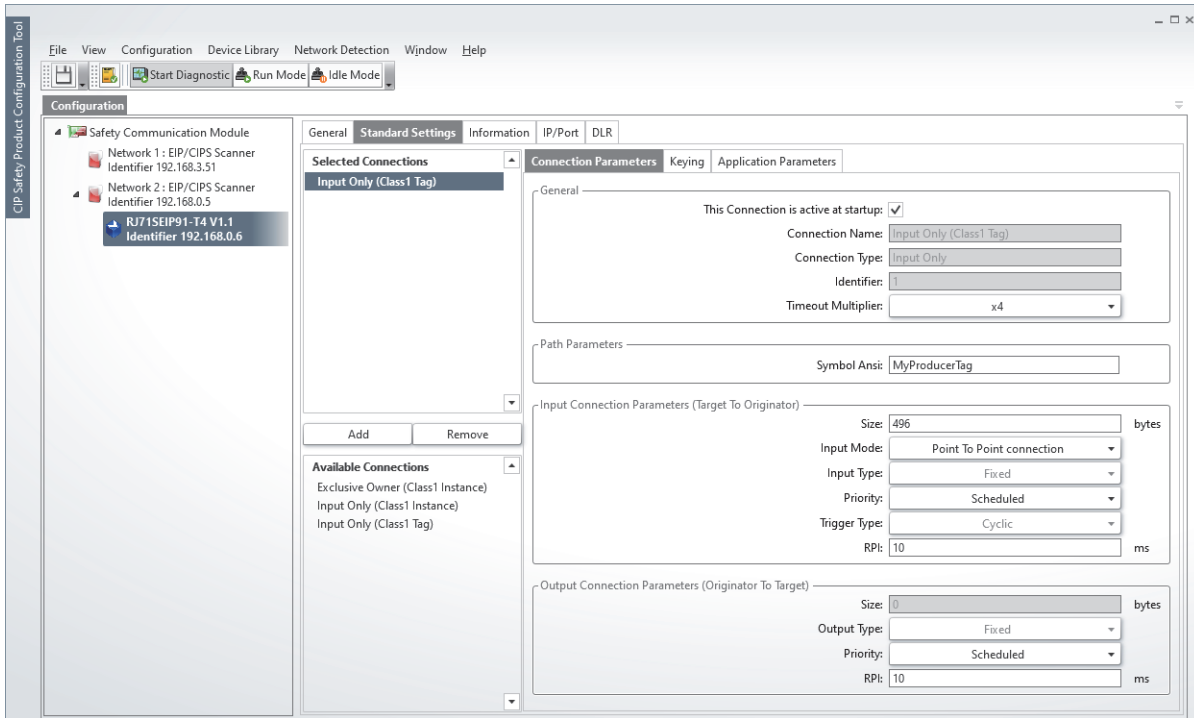
8. When the following window is displayed, click the [Yes] button.



9. Select "Input Only (Class1 Tag)" in "Selected Connections" in the [Standard Settings] tab and set the following.

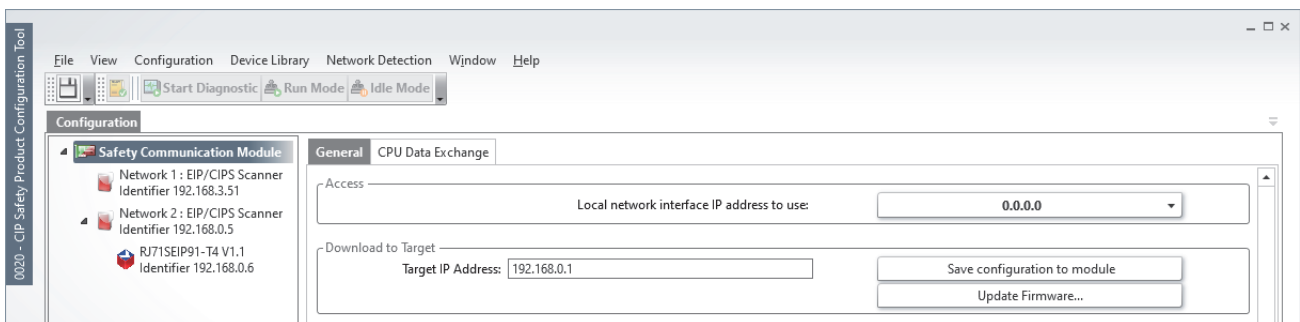
Item	Setting value	
General	This Connection is active at startup	Selected
Path Parameters	Symbol Ansi	MyProducerTag* ¹
Input Connection Parameters (Target To Originator)	Size	496
	RPI	10
Output Connection Parameters (Originator To Target)	RPI	10

*1 This tag name is for the connection destination. Set the same tag name as that of the target.

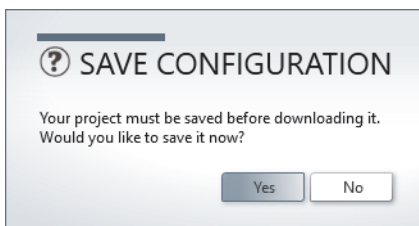


10. Select "Safety Communication Module" and set the current IP address of the CIP Safety module to "Target IP Address".

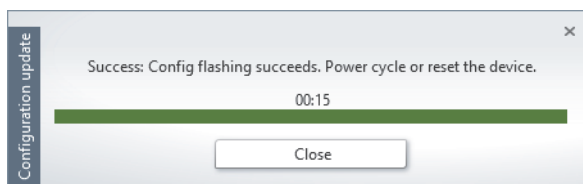
11. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



12. Click the [Yes] button in the following window to save the configuration.



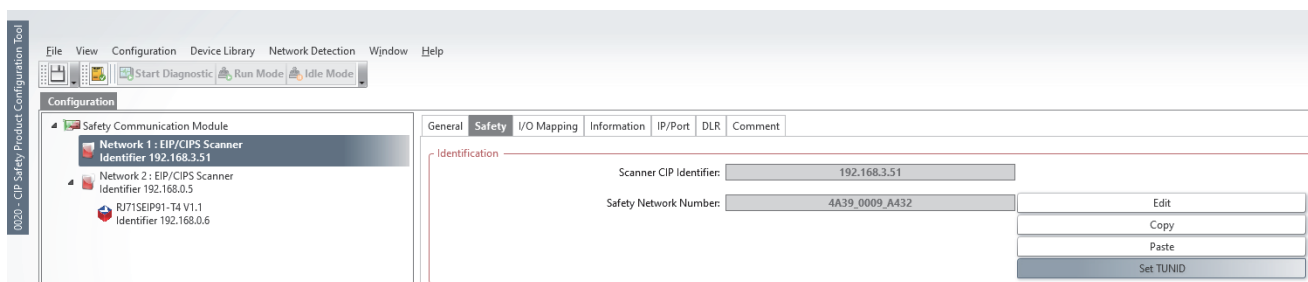
13. Click the [Close] button in the following window.



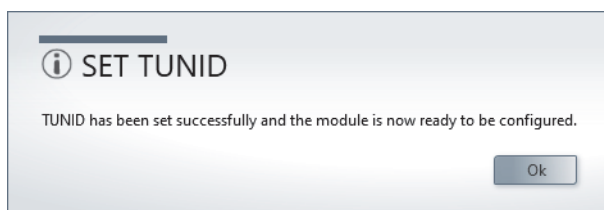
14. After downloading, reset the CPU module or power off and on the system.

15. Click the [Set TUNID] button.

☞ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

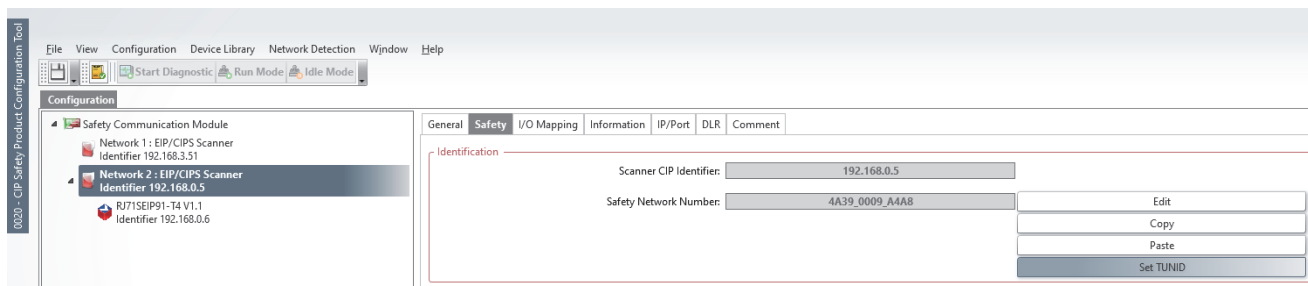


16. Click the [OK] button in the following window.

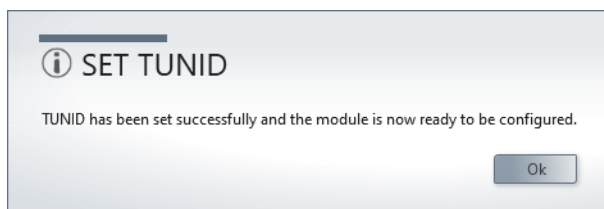


17. Click the [Set TUNID] button.

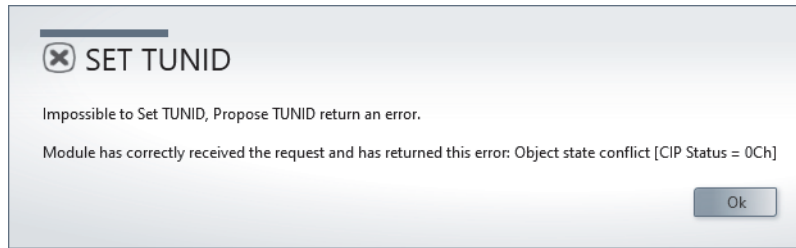
☞ "Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab



18. Click the [OK] button in the following window.



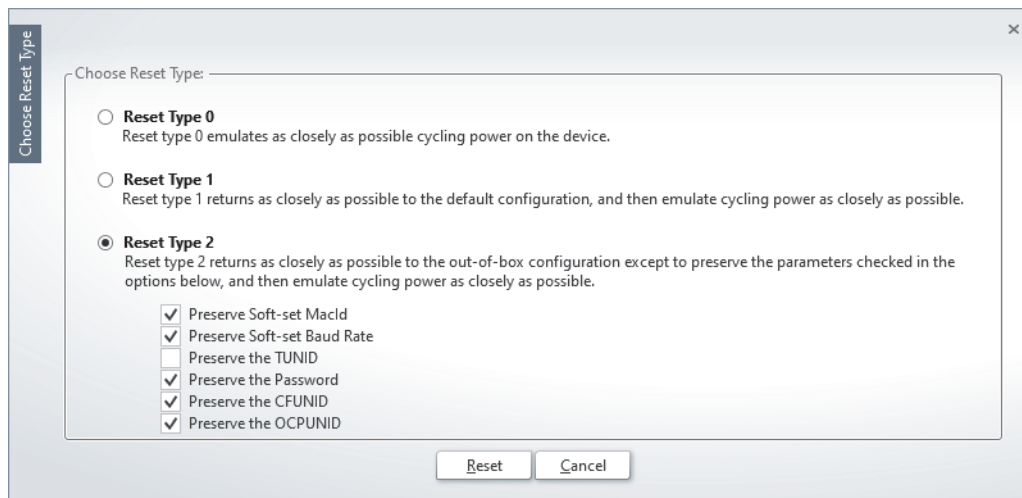
If TUNID is already set to the CIP Safety module, a following error message is displayed.



10

If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.



- (3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
- When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off

- (4) Reset the CPU module or power off and on the system.

19. Close CIP Safety Configuration Tool.

20. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

[Online] ⇒ [Write to PLC]

■Parameter settings for the CIP Safety module (producer)

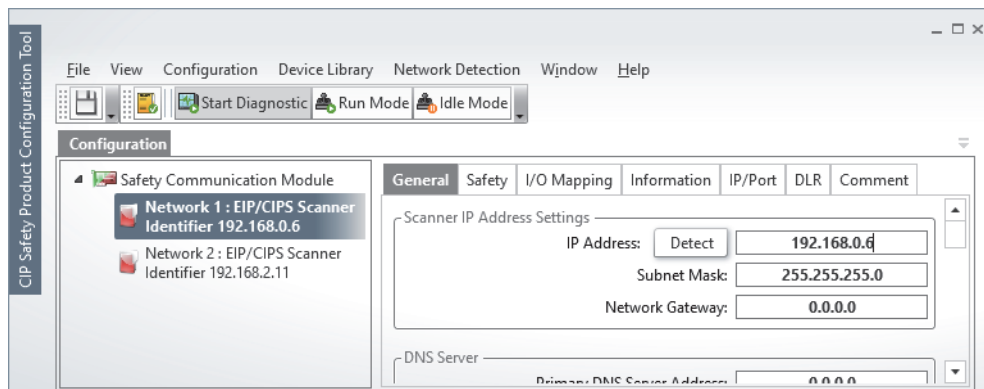
Operating procedure

1. Start CIP Safety Configuration Tool.

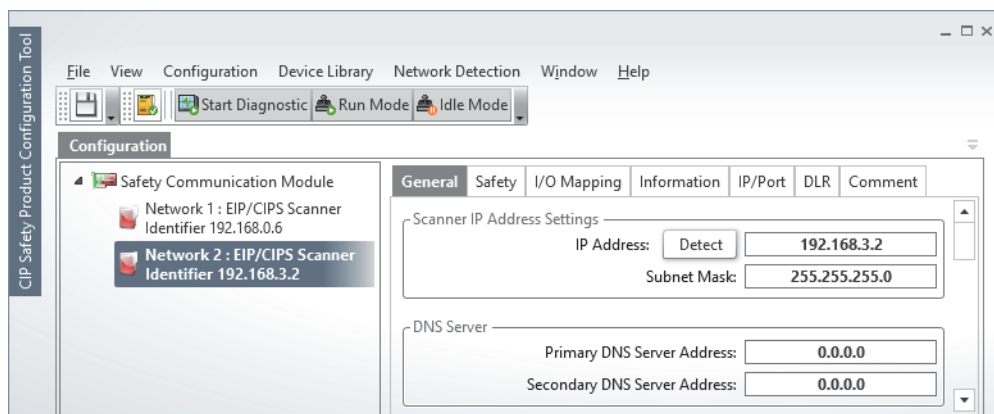
🖱️ [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.0.6 to "IP Address" (P1).



- Select "Network 2: EIP/CIPS Scanner" and set 192.168.3.2 to "IP Address" (P2).



3. Set "Network 1: EIP/CIPS Scanner".

- [General] tab

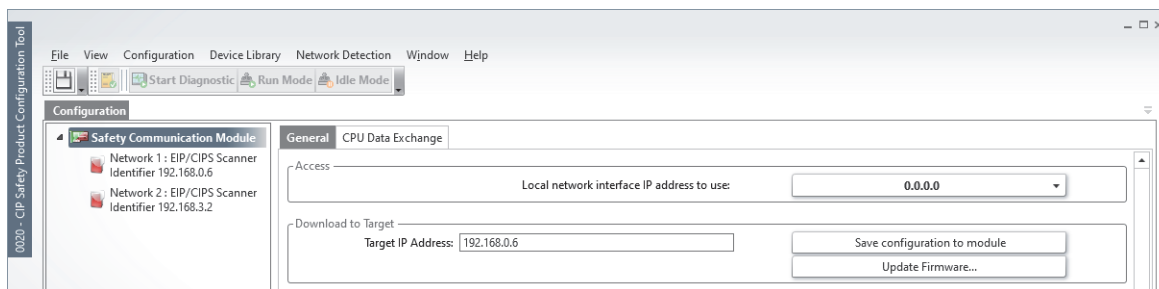
Item		Setting value
Operating Mode	Target (Class1)	Selected

- [Target (Class1)] tab

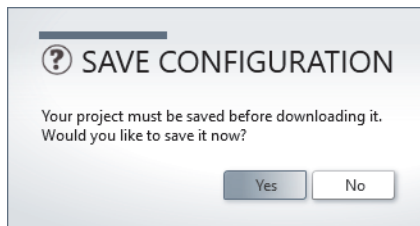
Click the [Add] button in "Target (Class1 Tag) definitions" and set the following.

Item		Setting value
Target (Class1 Tag) definitions	Name	MyProducerTag
	T->O Size	496

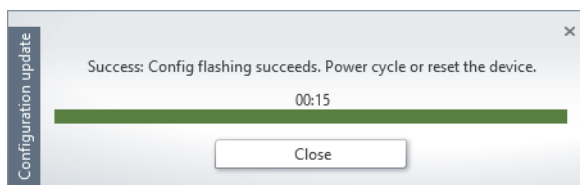
4. Select "Safety Communication Module" and set the current IP address of the CIP Safety module to "Target IP Address".
5. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



6. Click the [Yes] button in the following window to save the configuration.

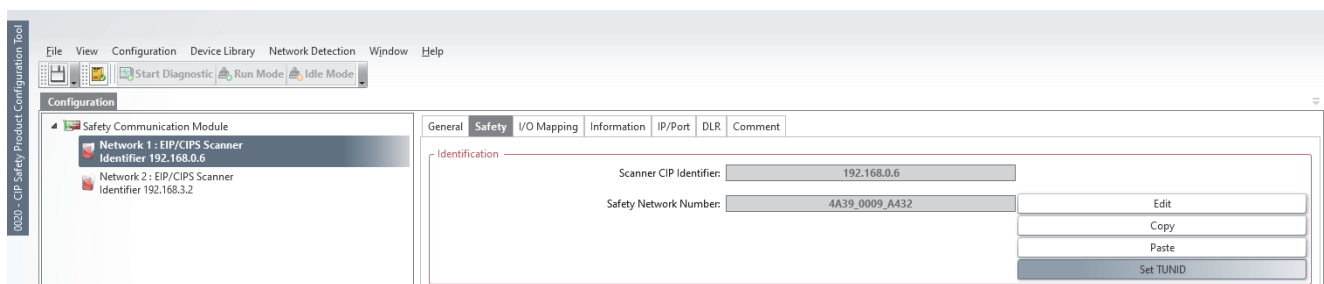


7. Click the [Close] button in the following window.

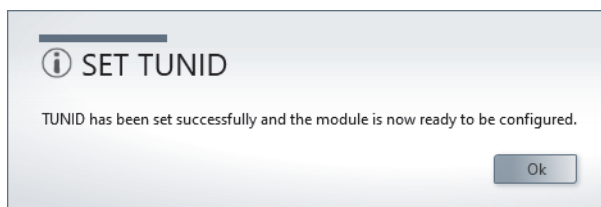


8. After downloading, reset the CPU module or power off and on the system.
9. Click the [Set TUNID] button.

🖱️ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

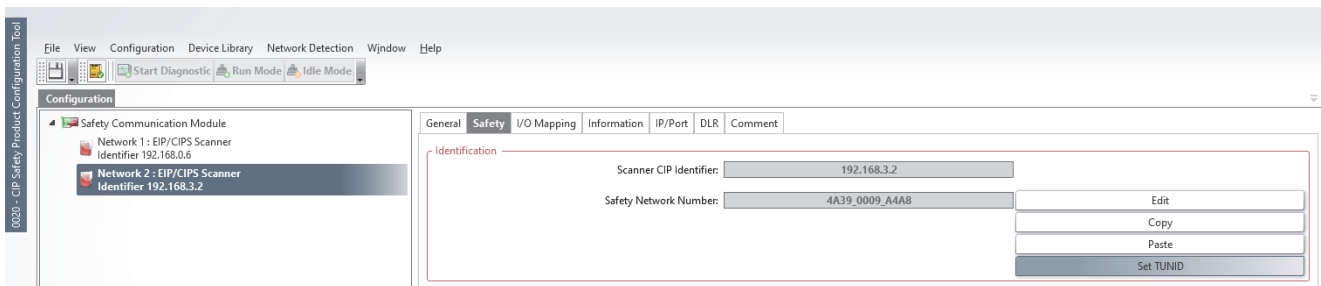


10. Click the [OK] button in the following window.

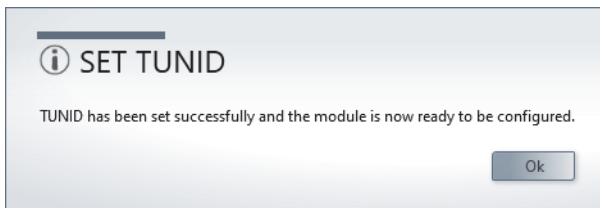


11. Click the [Set TUNID] button.

"Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab



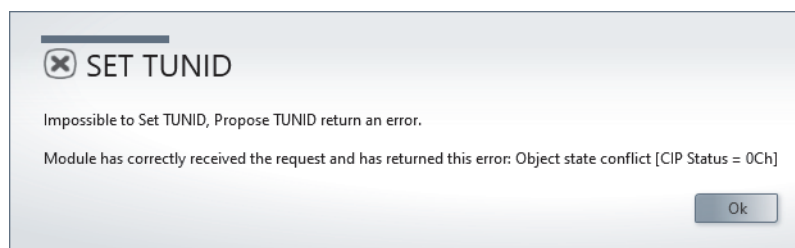
12. Click the [OK] button in the following window.



10

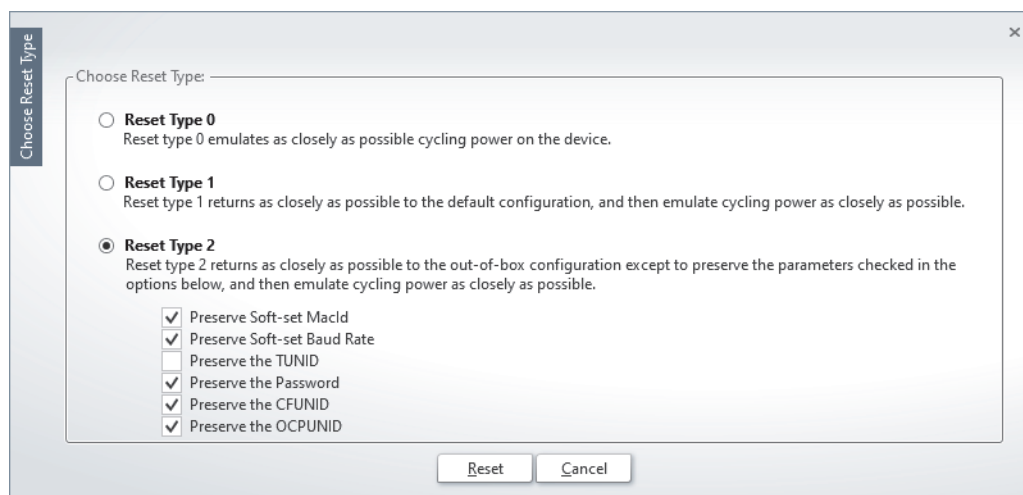


If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.




(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
 - When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off
- (4) Reset the CPU module or power off and on the system.

13. Close CIP Safety Configuration Tool.

14. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

 [Online] ⇒ [Write to PLC]

Auto Refresh Setting

1. Set the Auto refresh setting.

[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ Right-click ⇒ [Auto Refresh Setting]

2. Write the following parameters to the CPU module and reset the CPU module or power off and on the system.

[Online] ⇒ [Write to PLC]

■Settings for the CIP Safety module (consumer)

'Class1 Input Area' (Un\G1073152 to Un\G1105919)	
Start Address	End Address
D500	D747

CIP Safety Module Auto Refresh Setting

User CPU Device: ☒ Assign Devices per Buffer

Output devices (IQ-R CPU -> CIP Safety) | Input devices (IQ-R CPU <- CIP Safety)

Buffer	Start Address	End Address
Class1 Status(P1)		
Class1 Status(P2)		
Class1 Input(P1)		
Class1 Input(P2)	D500	D747

OK Cancel

■Settings for the CIP Safety module (producer)

'Class1 Output Area' (Un\G61440 to Un\G94207)	
Start Address	End Address
D0	D247

CIP Safety Module Auto Refresh Setting

User CPU Device: ☒ Assign Devices per Buffer

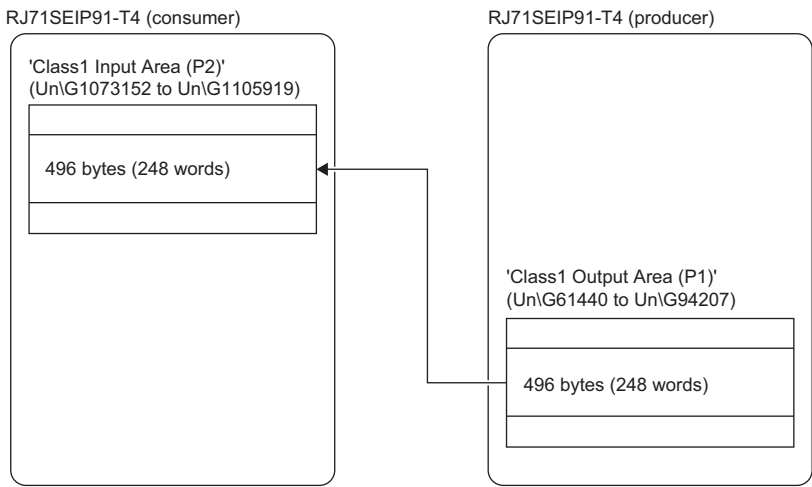
Output devices (IQ-R CPU -> CIP Safety) | Input devices (IQ-R CPU <- CIP Safety)

Buffer	Start Address	End Address
Class1 Output(P1)	D0	D247
Class1 Output(P2)		

OK Cancel

Program example

496 bytes (248 words) of data are received from 'Class1 Output Area (P1)' (Un\G61440 to Un\G94207) of the producer to 'Class1 Input Area (P2)' (Un\G1073152 to Un\G1105919) of the consumer.
RPI is 10ms.



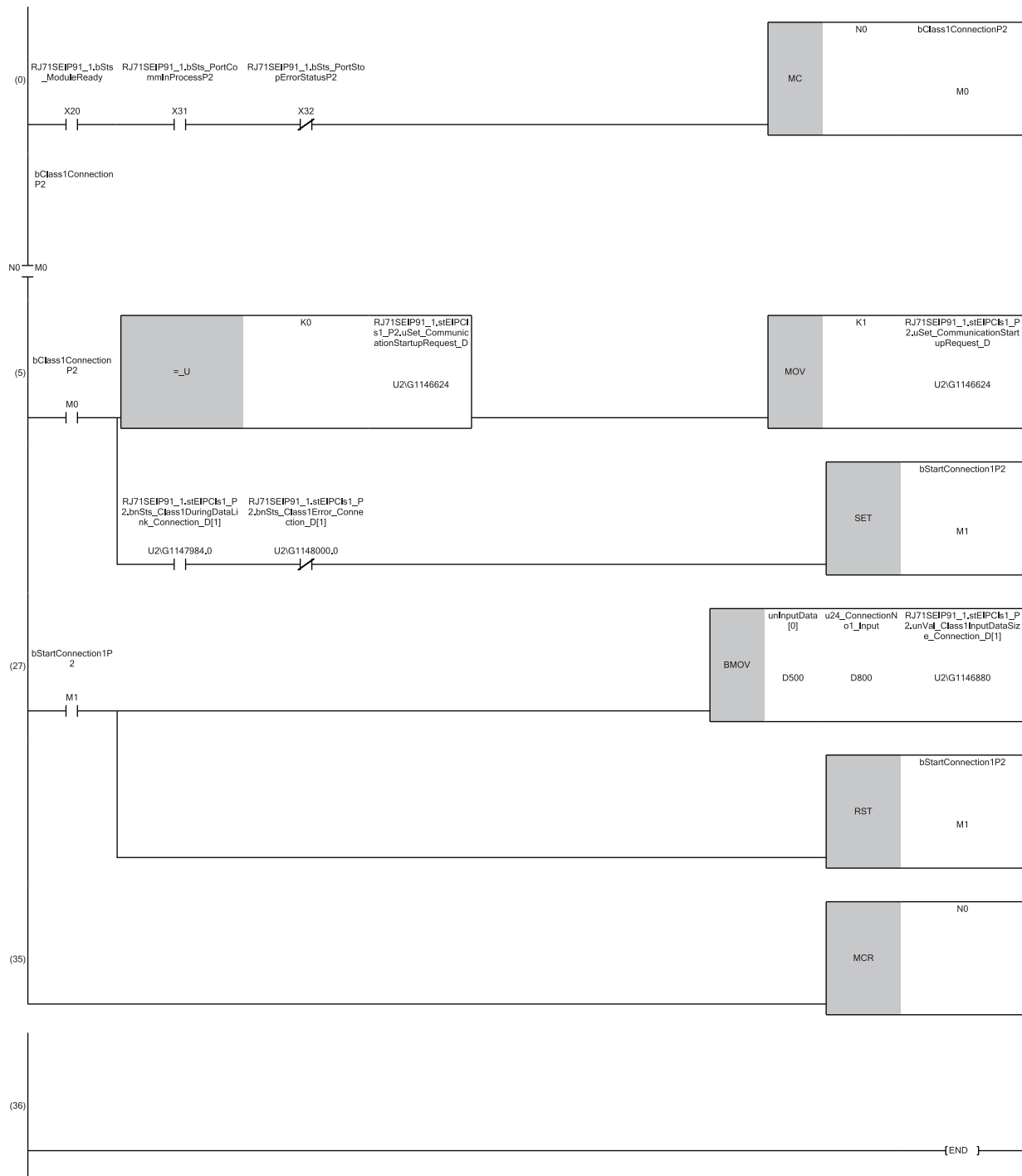
Point

Class1 tag communications cannot be communicated data with one connection, unlike Class1 instance communications. Therefore, Class1 tag communications always send data from the producer to the consumer.

To send data from the consumer to the producer, the following are required; establish another connection, configure the settings on the producer side to the consumer and configure the settings on the consumer side to the producer.

Program for the CIP Safety module (consumer)

Classification	Label name	Description	Device
Module label	RJ71SEIP91_1.bSts_ModuleReady	Module READY	X20
	RJ71SEIP91_1.bSts_PortCommInProcessP2	Port start status (P2)	X31
	RJ71SEIP91_1.bSts_PortStopErrorStatusP2	Port stop error status (P2)	X32
	RJ71SEIP91_1.stEIPCls1_P2.uSet_CommunicationStartupRequest_D	EtherNet/IP communication start request	U2\G1146624
	RJ71SEIP91_1.stEIPCls1_P2.bnSts_Class1DuringDataLink_Connection_D[1]	Data link status (Class1)	U2\G1147984.0
	RJ71SEIP91_1.stEIPCls1_P2.bnSts_Class1Error_Connection_D[1]	Error status (Class1)	U2\G1148000.0
	RJ71SEIP91_1.stEIPCls1_P2.unVal_Class1InputDataSize_Connection_D[1]	Class1 Input data size	U2\G1146880
Label to be defined	Define global labels as shown below.		
	Label Name	Data Type	Class Assign (Device/Label)
	1 bClass1ConnectionP2	Bit	VAR_GLOBAL M0
	2 bStartConnection1P2	Bit	VAR_GLOBAL M1
	3 unInputData	Word [Unsigned]/Bit String [16-bit](0..247)	VAR_GLOBAL D500
	4 u24_ConnectionNo1_Input	Word [Unsigned]/Bit String [16-bit](0..247)	VAR_GLOBAL D800

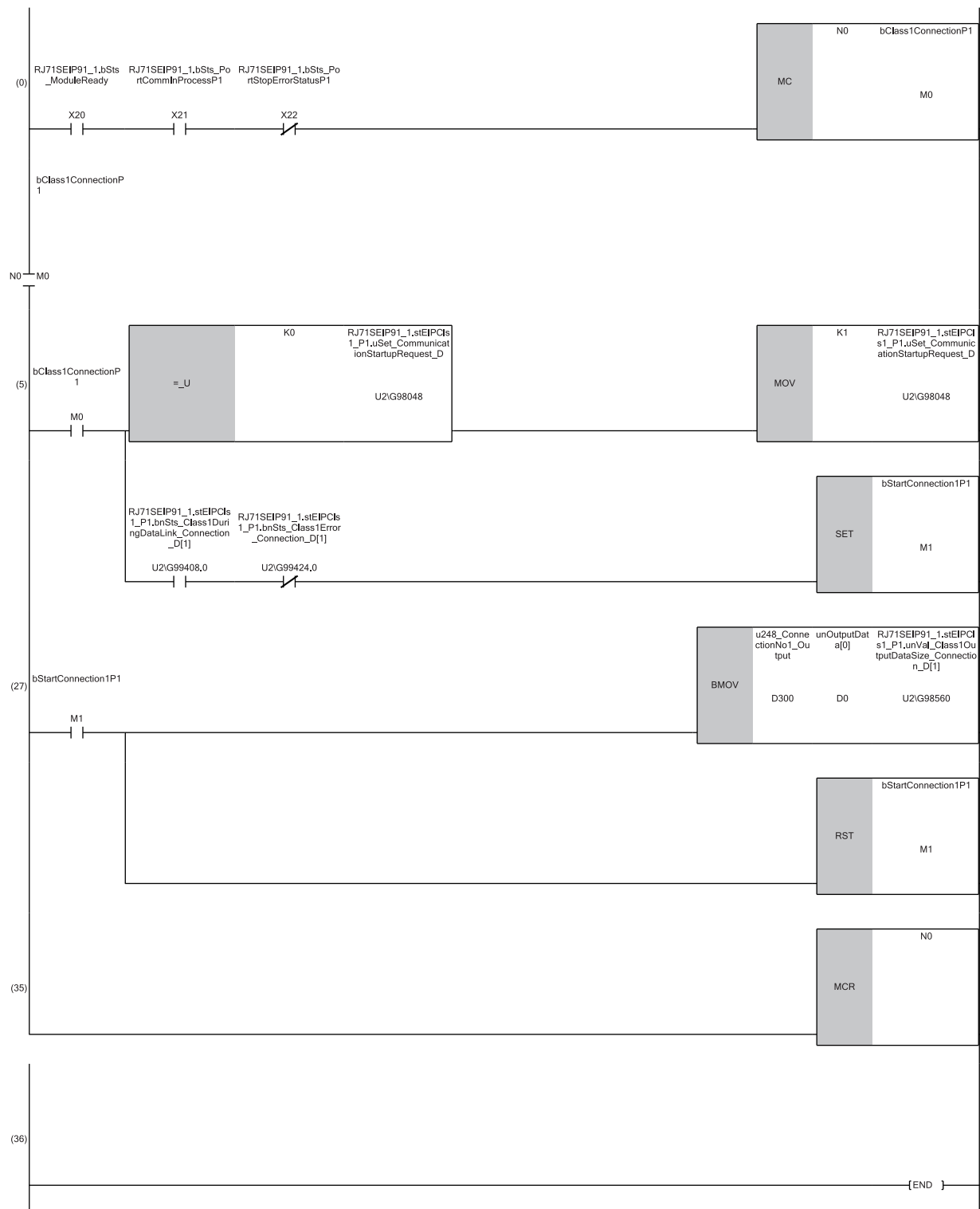


- (0) Configure an interlock by using X20, X31, and X32.
 (5) If U2/G1146624 has not been requested once, a start request will be issued.
 U2/G1147984.0 and U2/G1148000.0 are checked and the processing is started.
 (27) Input data of D500 is acquired for D800.
 (35) The processing is completed.

Program for the CIP Safety module (producer)

Classification	Label name	Description	Device
Module label	RJ71SEIP91_1.bSts_ModuleReady	Module READY	X20
	RJ71SEIP91_1.bSts_PortCommInProcessP1	Port start status (P1)	X21
	RJ71SEIP91_1.bSts_PortStopErrorStatusP1	Port stop error status (P1)	X22
	RJ71SEIP91_1.stEIPCls1_P1.uSet_CommunicationStartupRequest_D	EtherNet/IP communication start request	U2\G98048
	RJ71SEIP91_1.stEIPCls1_P1.bnSts_Class1DuringDataLink_Connection_D[1]	Data link status (Class1)	U2\G99408.0
	RJ71SEIP91_1.stEIPCls1_P1.bnSts_Class1Error_Connection_D[1]	Error status (Class1)	U2\G99424.0
	RJ71SEIP91_1.stEIPCls1_P1.unVal_Class1OutputDataSize_Connection_D[1]	Class1 Output data size	U2\G98560
Label to be defined	Define global labels as shown below.		

	Label Name	Data Type	Class	Assign (Device/Label)
1	bClass1ConnectionP1	Bit	VAR_GLOBAL	M0
2	bStartConnection1P1	Bit	VAR_GLOBAL	M1
3	unOutputData	Word [Unsigned]/Bit String [16-bit](0..247)	VAR_GLOBAL	D0
4	u248_ConnectionNo1_Output	Word [Unsigned]/Bit String [16-bit](0..247)	VAR_GLOBAL	D300



- (0) Configure an interlock by using X20, X21, and X22.
- (5) If U2\G98048 has not been requested once, a start request will be issued.
U2\G99408.0 and U2\G99424.0 are checked and the processing is started.
- (27) Output data of D300 is set to D0.
- (35) The processing is completed.

10.3 UCMM message communications

This section describes an example of UCMM message communications between the client and the server.

System configuration example

The system configuration example is the same as Class1 instance communications. (☞ Page 120 System configuration example)

Replace the following terms.

- Originator → Client
- Target → Server

Parameter settings

Settings using the engineering tool

The settings procedure is the same as Class1 instance communications. (☞ Page 121 Settings using the engineering tool)

Settings using CIP Safety Configuration Tool

Connect CIP Safety Configuration Tool to the CIP Safety module, and set parameters.

■Parameter settings for the CIP Safety module (client)

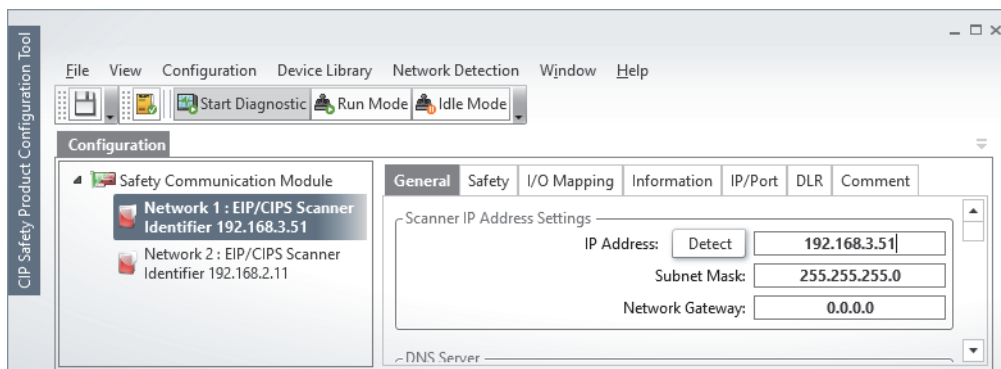
Operating procedure

1. Start CIP Safety Configuration Tool.

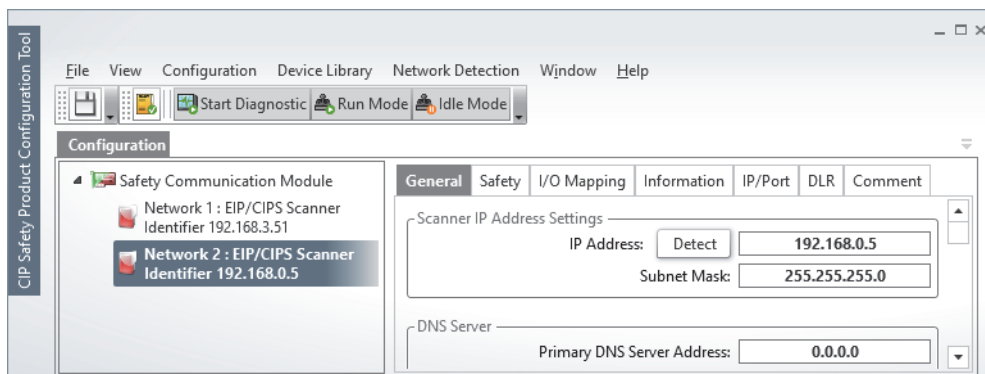
☞ [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

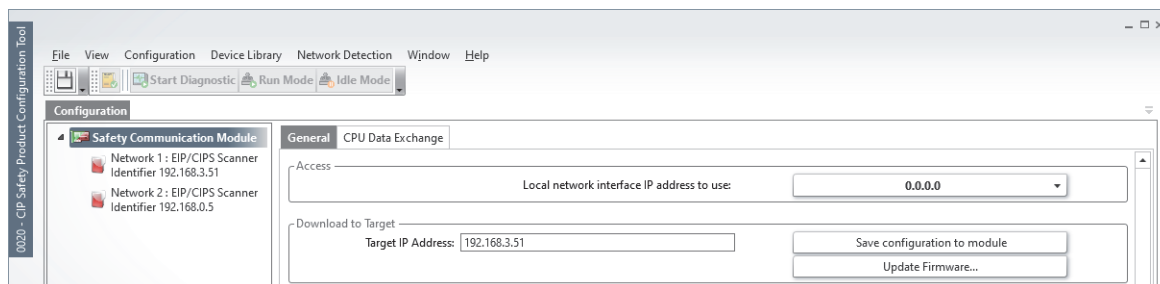
- Select "Network 1: EIP/CIPS Scanner" and set 192.168.3.51 to "IP Address" (P1).



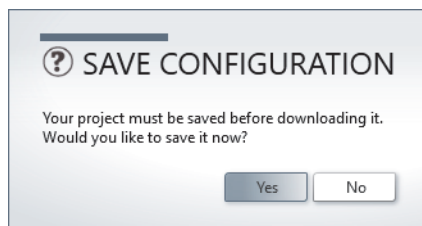
- Select "Network 2: EIP/CIPS Scanner" and set 192.168.0.5 to "IP Address" (P2).



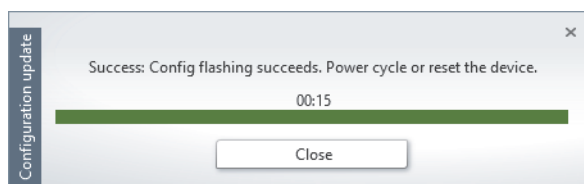
3. Select "Safety Communication Module" and set the current IP address of the CIP Safety module to "Target IP Address".
4. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



5. Click the [Yes] button in the following window to save the configuration.



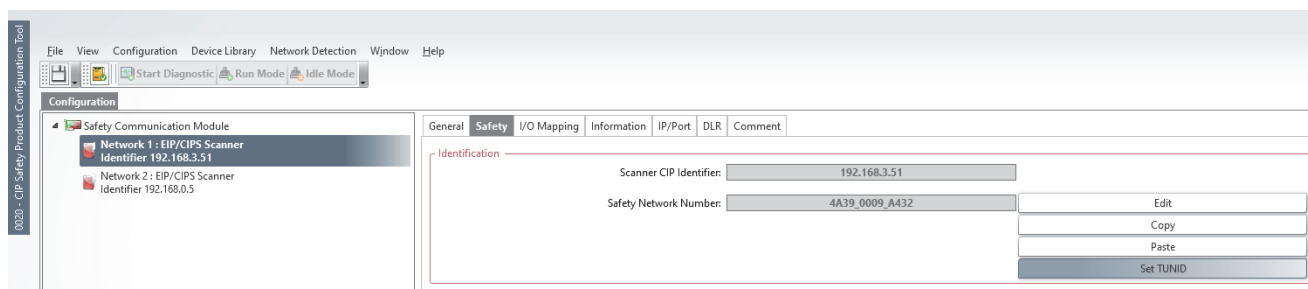
6. Click the [Close] button in the following window.



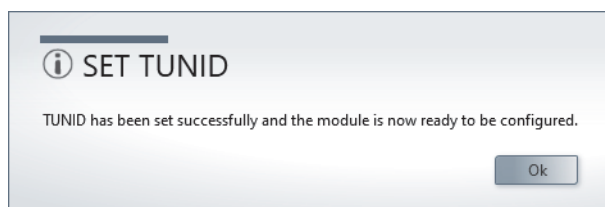
7. After downloading, reset the CPU module or power off and on the system.

8. Click the [Set TUNID] button.

🖱️ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

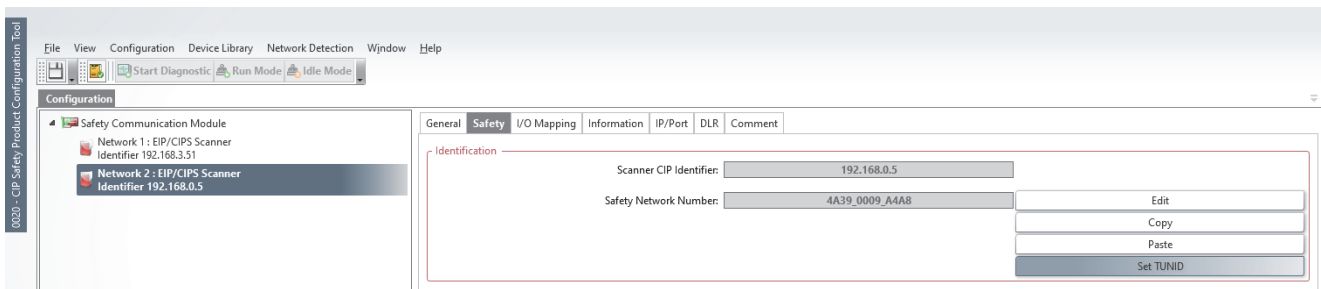


9. Click the [OK] button in the following window.

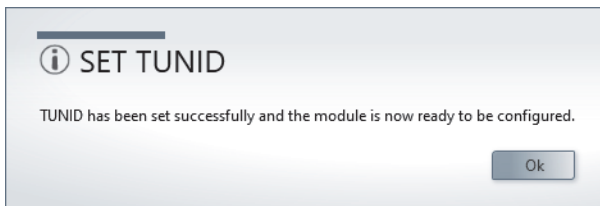


10. Click the [Set TUNID] button.

"Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab



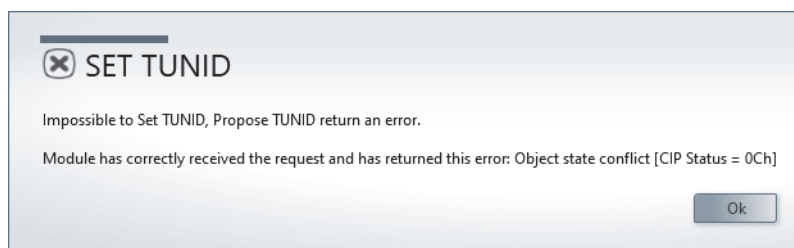
11. Click the [OK] button in the following window.



10

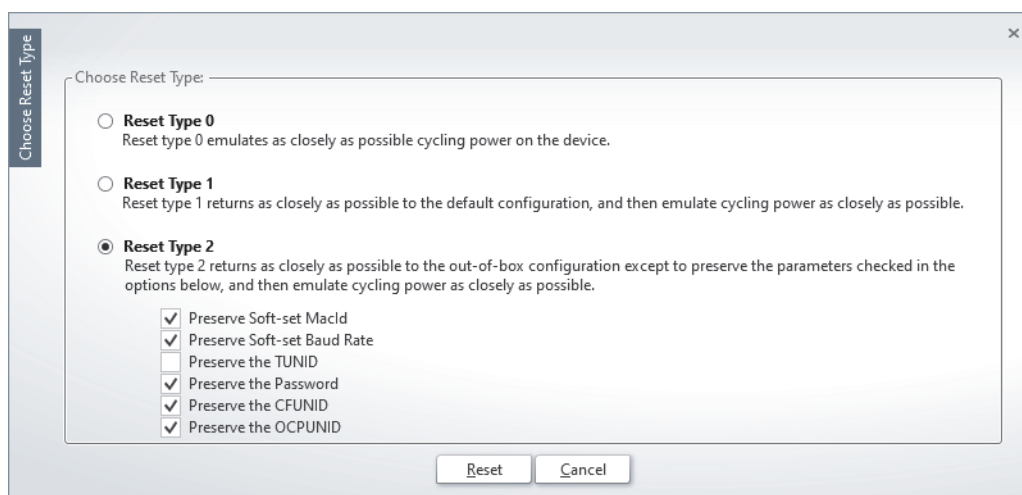


If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.




(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
 - When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off
- (4) Reset the CPU module or power off and on the system.

12. Close CIP Safety Configuration Tool.

13. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

 [Online] ⇒ [Write to PLC]

■Parameter settings for the CIP Safety module (server)

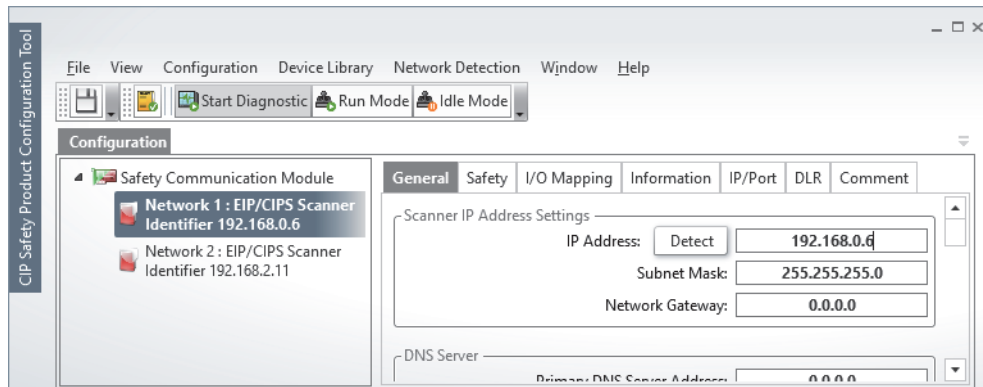
Operating procedure

1. Start CIP Safety Configuration Tool.

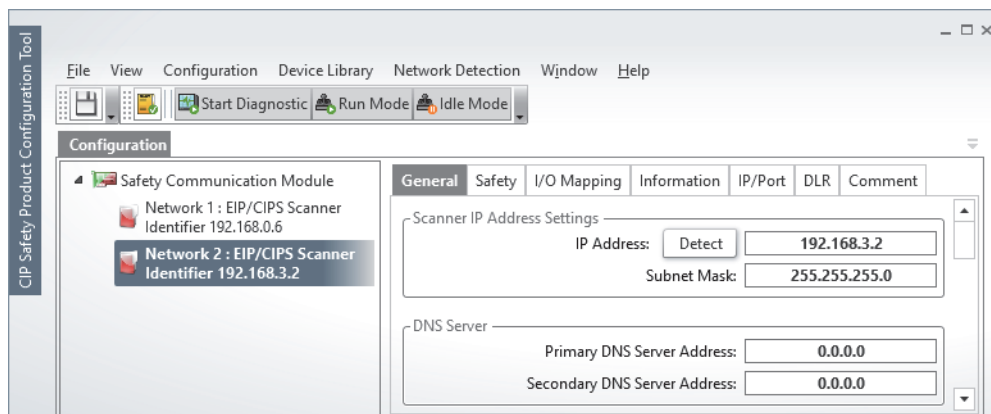
[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.0.6 to "IP Address" (P1).

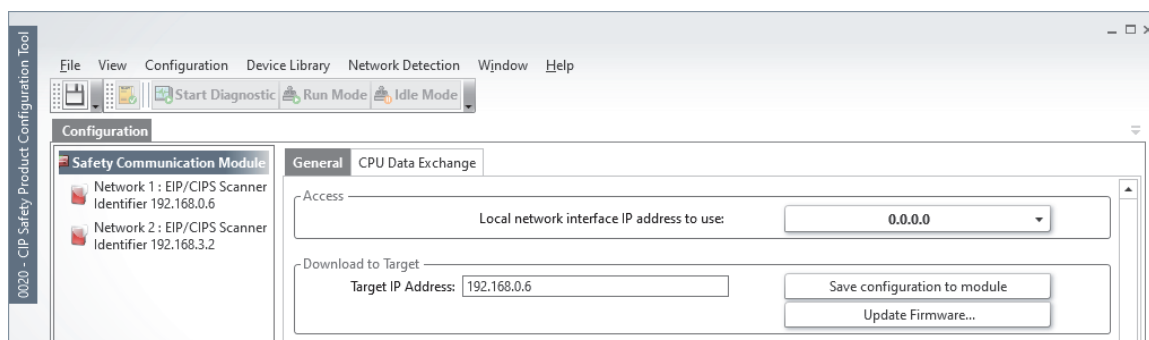


- Select "Network 2: EIP/CIPS Scanner" and set 192.168.3.2 to "IP Address" (P2).

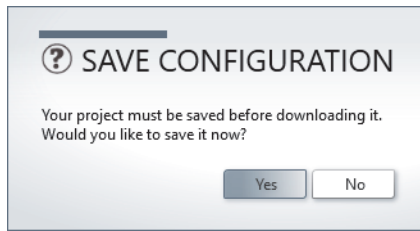


3. Select "Safety Communication Module" and set the current IP address of the CIP Safety module to "Target IP Address".

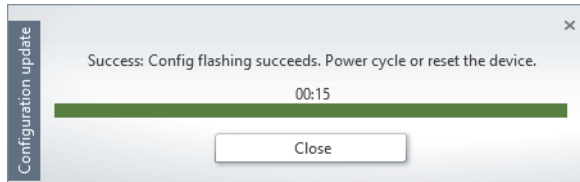
4. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



5. Click the [Yes] button in the following window to save the configuration.



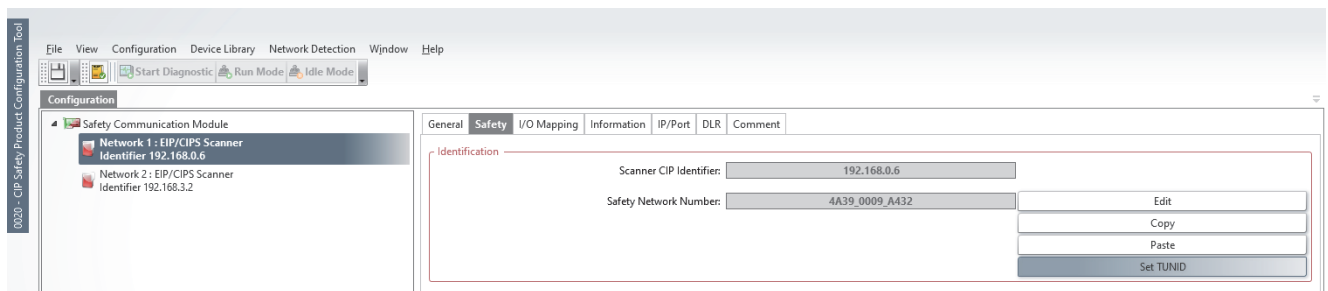
6. Click the [Close] button in the following window.



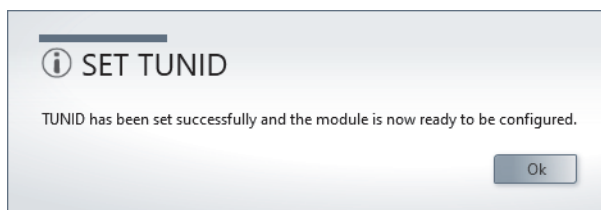
7. After downloading, reset the CPU module or power off and on the system.

8. Click the [Set TUNID] button.

🖱️ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

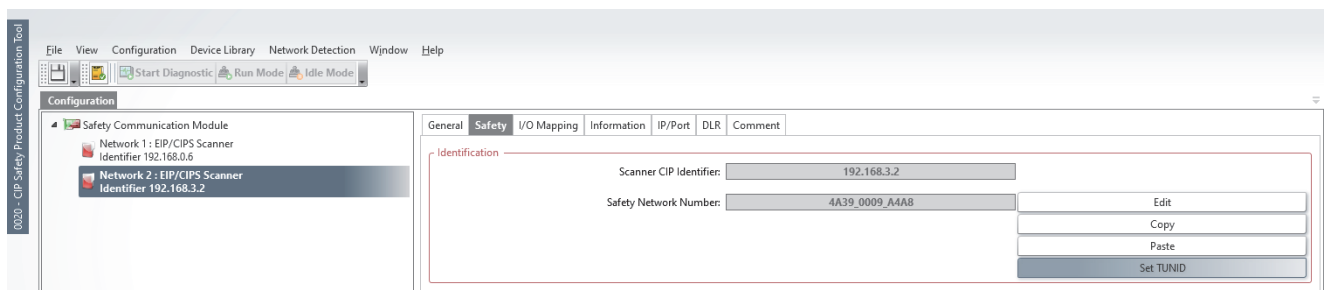


9. Click the [OK] button in the following window.

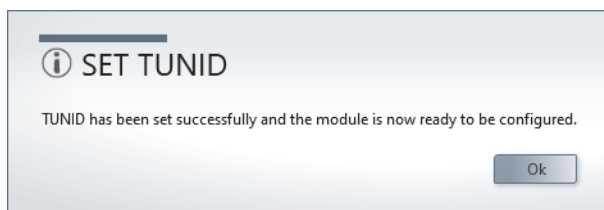


10. Click the [Set TUNID] button.

🖱️ "Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab

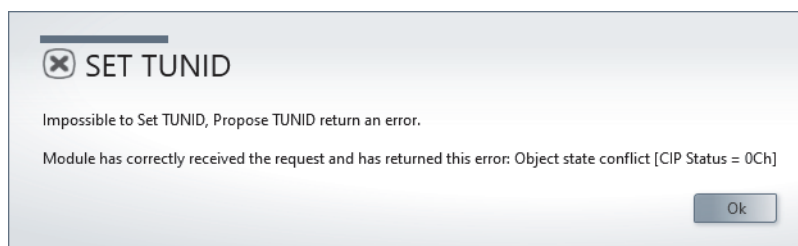


11. Click the [OK] button in the following window.



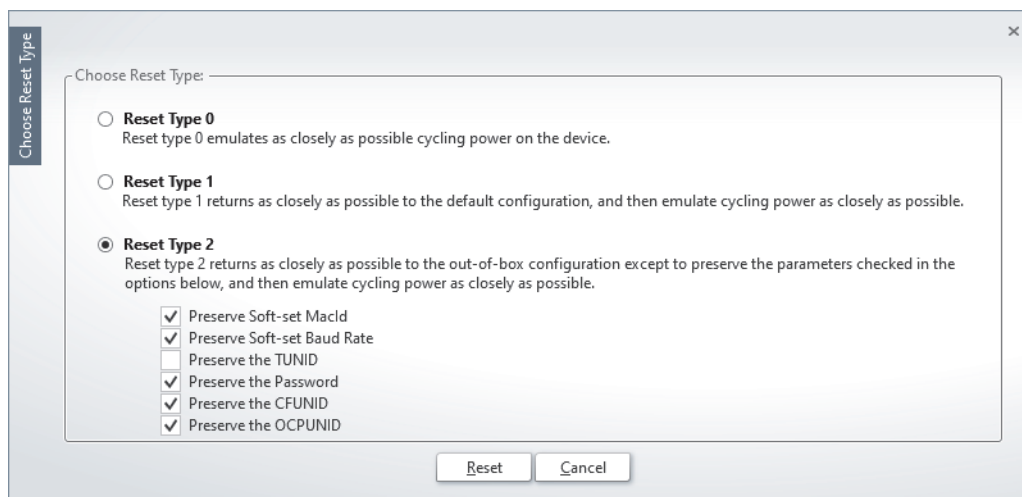
Point

If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.



(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
- When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off

(4) Reset the CPU module or power off and on the system.

12. Close CIP Safety Configuration Tool.

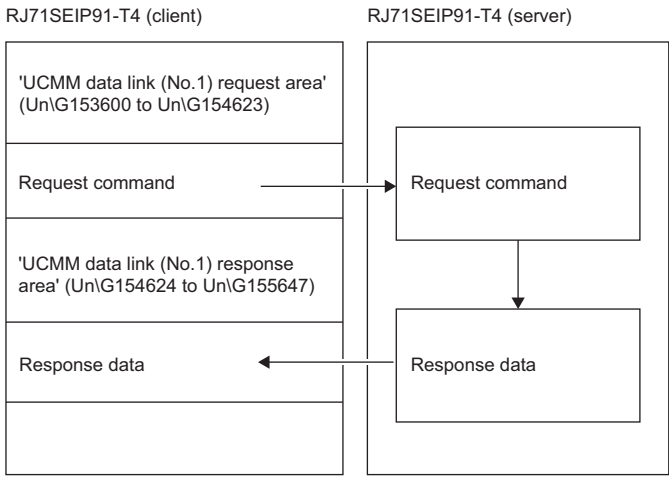
13. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

 [Online] ⇒ [Write to PLC]

Program example

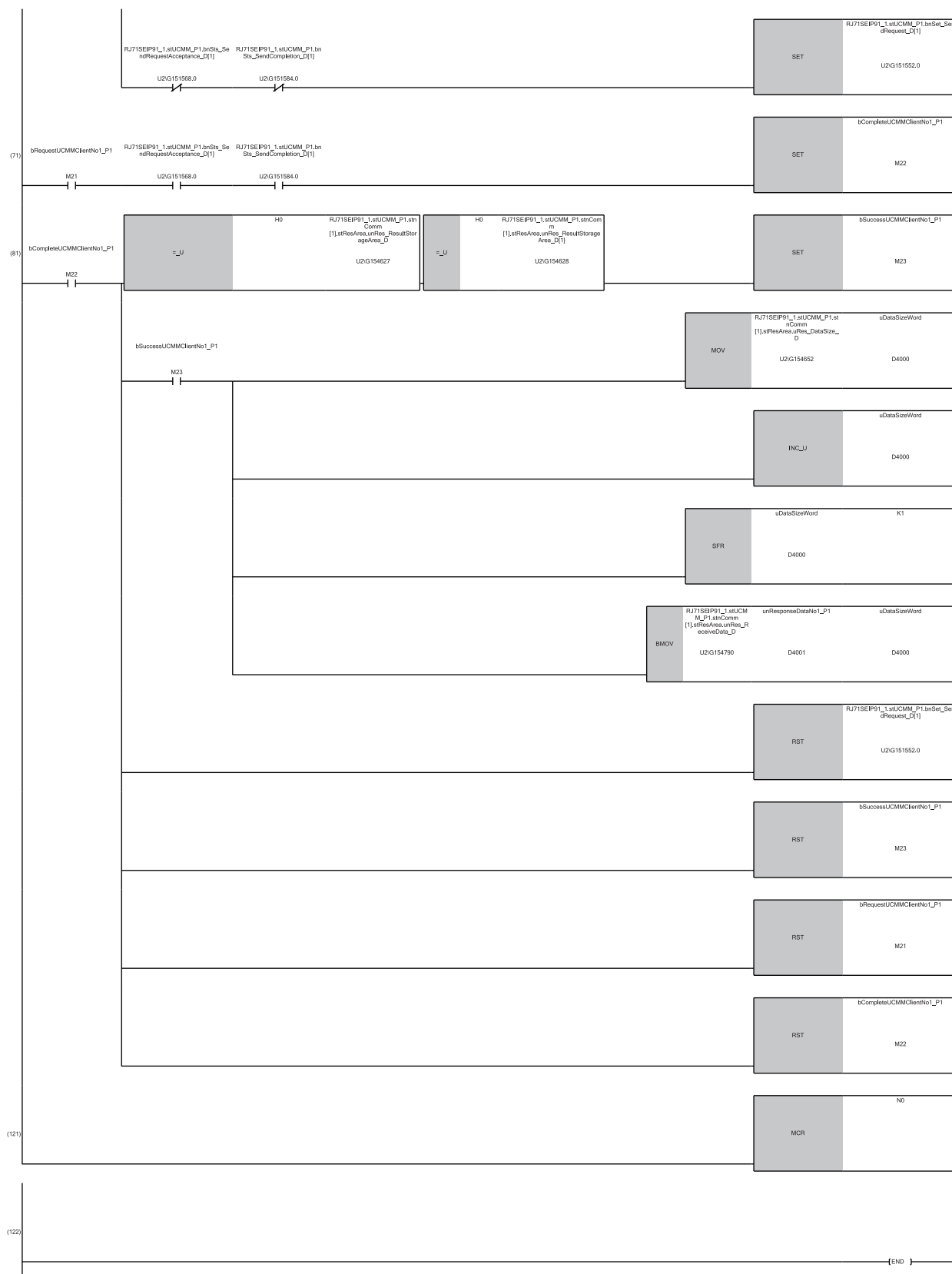
'UCMM data link (No.1) request area (P1)' (Un\G153600 to Un\G154623) of the client is used to send the request command to the server.

The server generates a response data and sends the response data to 'UCMM data link (No.1) response area' (Un\G154624 to Un\G155647).



Program for the CIP Safety module (client)

Classification	Label name	Description		Device
Module label	RJ71SEIP91_1.bSts_ModuleReady	Module READY		X20
	RJ71SEIP91_1.bSts_PortCommInProcessP1	Port start status (P1)		X21
	RJ71SEIP91_1.bSts_PortStopErrorStatusP1	Port stop error status (P1)		X22
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_CommunicationMethod_D	Request area	Communication method specification	U2\G153600
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_CommunicationStyle_D		Communication method specification	U2\G153601
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_Service_D		Service	U2\G153605
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.unSet_IpAddress_D[0]		IP Address	U2\G153606
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.unSet_IpAddress_D[1]		IP Address	U2\G153607
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_Class_D		Class	U2\G153630
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_Instance_D		Instance	U2\G153631
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_Attribute_D		Attribute	U2\G153632
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.uSet_DataSize_D		Data Size	U2\G153628
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stReqArea.unSet_RequestData_D		Request data	U2\G153766
	RJ71SEIP91_1.stUCMM_P1.bnSts_SendRequestAcceptance_D[1]	UCMM data link execution request acceptance		U2\G151568.0
	RJ71SEIP91_1.stUCMM_P1.bnSts_SendCompletion_D[1]	UCMM data link execution completion		U2\G151584.0
	RJ71SEIP91_1.stUCMM_P1.bnSet_SendRequest_D[1]	UCMM data link execution request		U2\G151552.0
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stResArea.unRes_ResultStorageArea_D[0]	Response area	Result storage area	U2\G154627
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stResArea.unRes_ResultStorageArea_D[1]		Result storage area	U2\G154628
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stResArea.unRes_ReceiveData_D		Response data	U2\G154790
	RJ71SEIP91_1.stUCMM_P1.stnComm[1].stResArea.uRes_DataSize_D		Data Size	U2\G154652
Label to be defined	Define global labels as shown below.			



- (0) Configure an interlock by using X20, X21, and X22.
- (5) By turning off and on the execution request, the send command is written to the buffer memory area and if the first area is not reception or completion status, Data link execution request is turned on.
- (71) Wait until the processing is completed.
- (81) When processing is completed, if the execution result is normal, the response data is acquired.
- (121) The processing is completed.

Program for the CIP Safety module (server)

A program is not required on the server side.

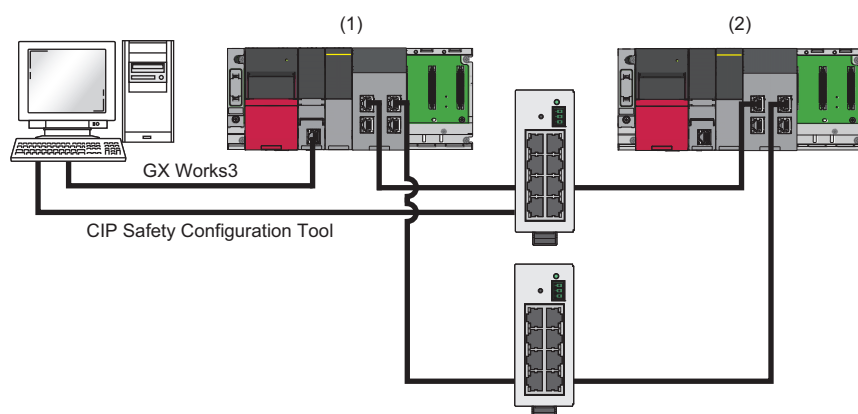
10.4 Safety Program

When using this program, I/O data is enabled when the safety communication status changes from abnormal to normal. To enable I/O data at intended timing, use the devices of the CPU module or others to perform the interlock.

System configuration example

The following system configuration is used for the example of performing a safety program that uses the interlock.

System configuration



(1) Programmable controller system (originator)

- Power supply module: R61P
- CPU module: R08SF CPU
- Safety function module: R6SFM
- CIP Safety module: RJ71SEIP91-T4^{*1}

(2) Programmable controller system (target)

- Power supply module: R61P
- CPU module: R08SF CPU
- Safety function module: R6SFM
- CIP Safety module: RJ71SEIP91-T4^{*2}

^{*1} IP address (P1): 192.168.0.1, subnet mask: 255.255.255.0

IP address (P2): 192.168.1.1, subnet mask: 255.255.255.0


^{*2} IP address (P1): 192.168.0.10, subnet mask: 255.255.255.0

IP address (P2): 192.168.1.10, subnet mask: 255.255.255.0

Parameter settings

Set parameters using the engineering tool and CIP Safety Configuration Tool.

Settings using the engineering tool

The settings procedure is the same as Class1 instance communications. ( Page 121 Settings using the engineering tool)

Settings using CIP Safety Configuration Tool

Connect CIP Safety Configuration Tool to the CIP Safety module, and set parameters.

■Parameter settings for the CIP Safety module (target)

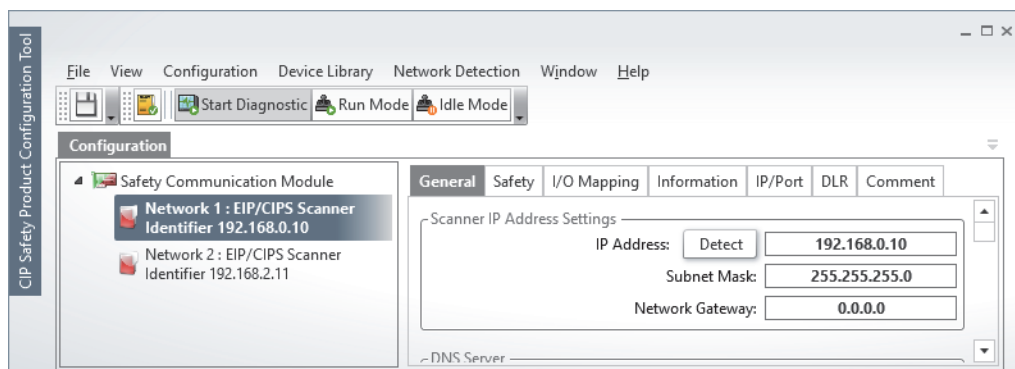
Operating procedure

1. Start CIP Safety Configuration Tool.

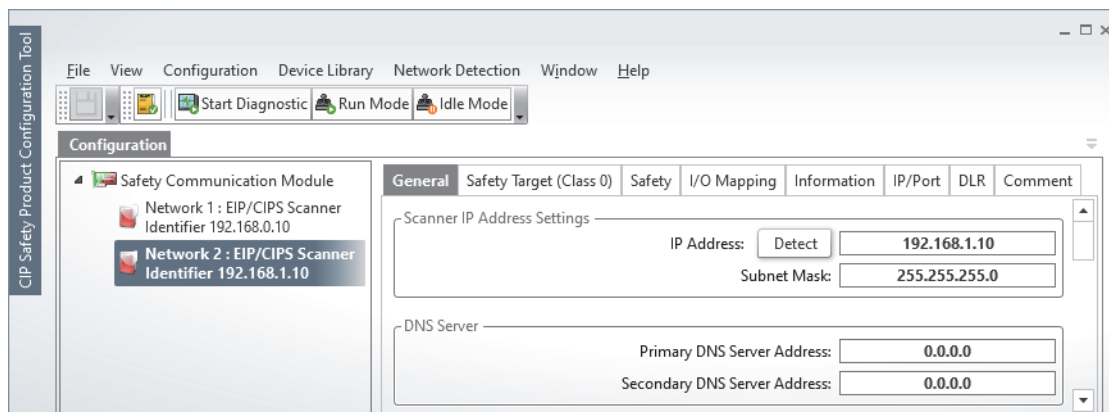
 [Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.0.10 to "IP Address" (P1).



- Select "Network 2: EIP/CIPS Scanner" and set 192.168.1.10 to "IP Address" (P2).



3. Set "Network 1: EIP/CIPS Scanner".

- [General] tab

Item		Setting value
Operating Mode	Safety Target (Class 0)	Selected

0020 - CIP Safety Product Configuration Tool

File View Configuration Device Library Network Detection Window Help

Start Diagnostic Run Mode Idle Mode

Configuration

Safety Communication Module

- Network 1: EIP/CIPS Scanner Identifier 192.168.0.10
- Network 2: EIP/CIPS Scanner Identifier 192.168.1.10

General Safety Target (Class 0) Safety I/O Mapping Information IP/Port DLR Comment

Scanner IP Address Settings

IP Address: Detect 192.168.0.10

Subnet Mask: 255.255.255.0

Network Gateway: 0.0.0.0

DNS Server

Primary DNS Server Address: 0.0.0.0

Secondary DNS Server Address: 0.0.0.0

Module Name

Host Name:

Domain Name:

Ports Settings

Port 1 baud rate: auto negotiation

Port 2 baud rate: auto negotiation

DLR Supervisor Configuration

Ring Supervisor Enabled: ☐

Ring Supervisor Precedence: 0

Beacon Interval: 400 μ s

Beacon Timeout: 1960 μ s

DLR VLAN ID: 0

Ping

Send Ping

Loop ☐

Stop on error ☐

Clear message log

Operating Mode

☐ Target (Class 1)

☒ Safety Target (Class 0)

Configuration Summary

Number of Class 1 connections (current / max): 0 / 64

- [Safety Target (Class 0)] tab

Item		Setting value
Target (Class 0) instance definitions	Direction	T->O
	Instance	540
	Size	8
	Max Subscribers	1
Target (Class 0) tag definitions	Direction	T->O
	Name	MyTag
	Tag Size	14
	Max Subscribers	1

The screenshot shows the 'CIP Safety Product Configuration Tool' window. The 'Configuration' tab is active, and the 'Safety Target (Class 0)' sub-tab is selected. On the left, a tree view shows 'Safety Communication Module' with two networks: 'Network 1 : EIP/CIPS Scanner Identifier 192.168.0.10' and 'Network 2 : EIP/CIPS Scanner Identifier 192.168.1.10'. The main area displays two configuration sections:

- Target (Class 0 Instance) definitions:** Contains an 'Add' and 'Remove' button, and a table with columns 'Direction', 'Instance', 'Size', and 'Max Subscribers'. The values are 'T->O', '540', '8', and '1' respectively.
- Target (Class 0 Tag) definitions:** Contains an 'Add' and 'Remove' button, and a table with columns 'Direction', 'Name', 'Tag Size', and 'Max Subscribers'. The values are 'T->O', 'MyTag', '14', and '1' respectively.

At the bottom, a note states: '(O means Originator so it is an external scanner that will connect to the local slave - T means Target so this is the local slave)'.

4. Set "Network 2: EIP/CIPS Scanner".

- [General] tab

Item		Setting value
Operating Mode	Safety Target (Class 0)	Selected

0020 - CIP Safety Product Configuration Tool

File View Configuration Device Library Network Detection Window Help

Start Diagnostic Run Mode Idle Mode

Configuration

Safety Communication Module

Network 1: EIP/CIPS Scanner Identifier 192.168.0.10

Network 2: EIP/CIPS Scanner Identifier 192.168.1.10

General Safety Target (Class 0) Safety I/O Mapping Information IP/Port DLR Comment

Scanner IP Address Settings

IP Address: Detect 192.168.1.10

Subnet Mask: 255.255.255.0

DNS Server

Primary DNS Server Address: 0.0.0.0

Secondary DNS Server Address: 0.0.0.0

Module Name

Host Name:

Domain Name:

Ports Settings

Port 1 baud rate: auto negotiation

Port 2 baud rate: auto negotiation

DLR Supervisor Configuration

Ring Supervisor Enabled: ☐

Ring Supervisor Precedence: 0

Beacon Interval: 400 μ s

Beacon Timeout: 1960 μ s

DLR VLAN ID: 0

Ping

Send Ping

Loop

Stop on error

Clear message log

Operating Mode

☐ Target (Class 1)

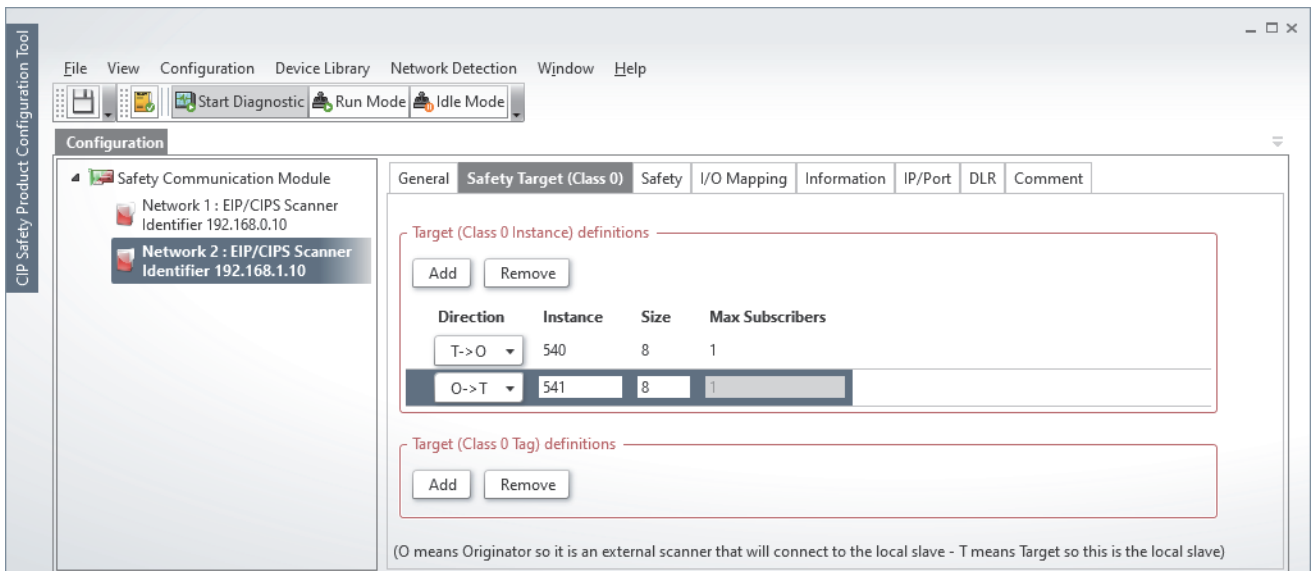
☒ Safety Target (Class 0)

Configuration Summary

Number of Class 1 connections (current / max): 0 / 64

- [Safety Target (Class 0)] tab

Item	Setting value	
Target (Class 0) instance definitions	Direction	T->O
	Instance	540
	Size	8
	Max Subscribers	1
	Direction	O->T
	Instance	541
	Size	8
	Max Subscribers	1

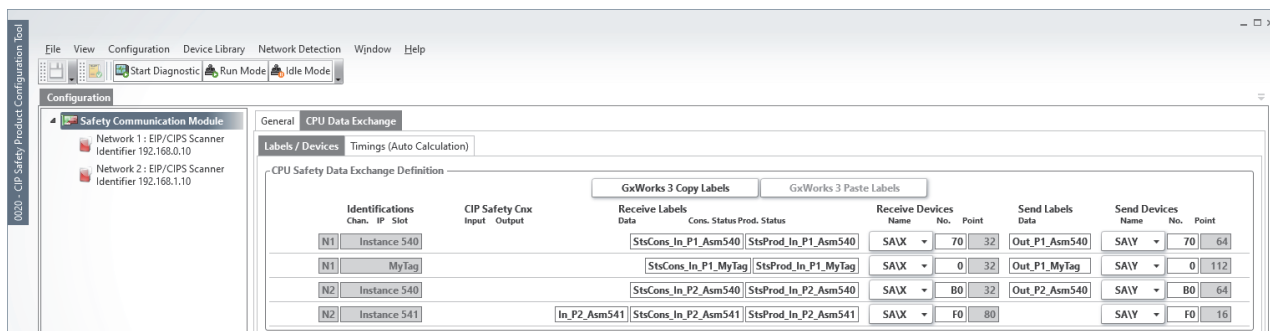


5. Select "Safety Communication Module" and set the details in the [CPU Data Exchange] tab.

- [Labels/Devices] tab

Receive Labels			Receive Devices	Send Labels	Send Devices
Data	Cons. Status	Prod. Status	No.	Data	No.
—	StsCons_In_P1_Asm540	StsProd_In_P1_Asm540	70	Out_P1_Asm540	70
—	StsCons_In_P1_MyTag	StsProd_In_P1_MyTag	0	Out_P1_MyTag	0
—	StsCons_In_P2_Asm540	StsProd_In_P2_Asm540	B0	Out_P2_Asm540	B0
In_P2_Asm541	StsCons_In_P2_Asm541	StsProd_In_P2_Asm541	F0	—	F0

10



- In this example, set the device in order of (SA\X) F0 → B0 → 70 → 0, (SA\Y) F0 → B0 → (Out_P1_MyTag is 140) → 70 → 0 to avoid duplication.
- The following is an example of when a safety device other than SA\X and SA\Y is assigned. (When using a program example, review the assignment of global labels to avoid duplicating the assignment with other devices.)

Receive Devices			Send Labels	Send Devices		
Name	No.	Point	Data	Name	No.	Point
SA\D	0	4	Out_P1_Asm540	SA\D	257	4
SA\M	0	112	Out_P1_MyTag	SA\M	272	112
SA\B	0	64	Out_P2_Asm540	SA\B	110	64
SA\W	0	5		SA\W	100	5

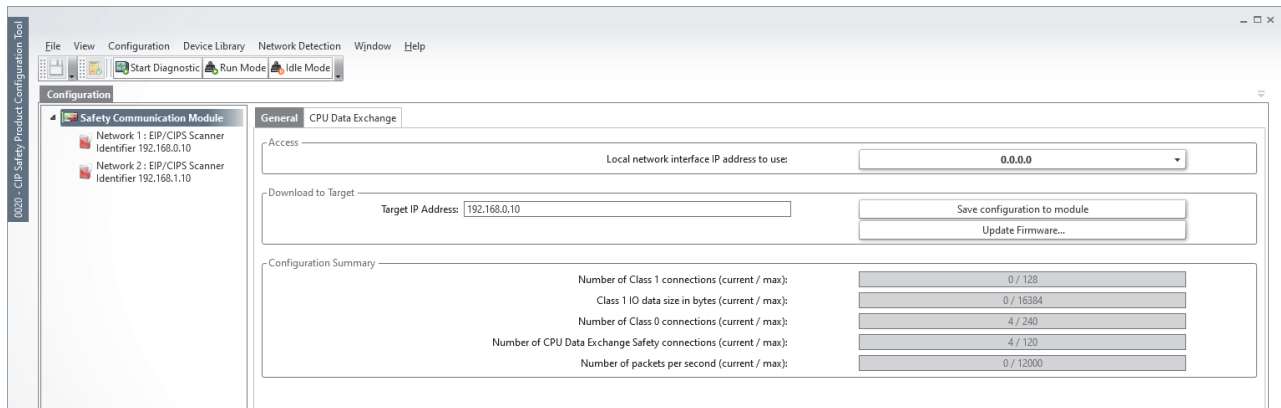
- [Timings (Auto Calculation)] tab

Receive (Input)		Send (Output)	
EPI (ms)	Timeout Mult.	EPI (ms)	Timeout Mult.
12	2	12	2
12	2	12	2
12	2	12	2
12	2	12	2

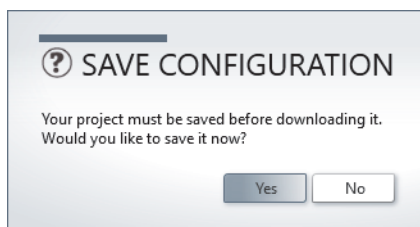


- Take notes of the value in safety cycle time to set it to the engineering tool later. (🔍 Page 197 Settings using the engineering tool)
- Entering the setting values is required for EPI and Timeout Multiplier in the connection on the target side because values are not set for those parameters, unlike the originator.

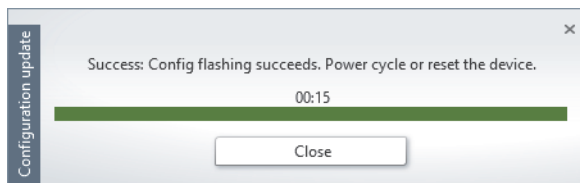
6. Set the current IP address of the CIP Safety module to "Target IP Address" in the [Safety Communication Module Access] tab.
7. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



8. Click the [Yes] button in the following window to save the configuration.



9. Click the [Close] button in the following window to close CIP Safety Configuration Tool.



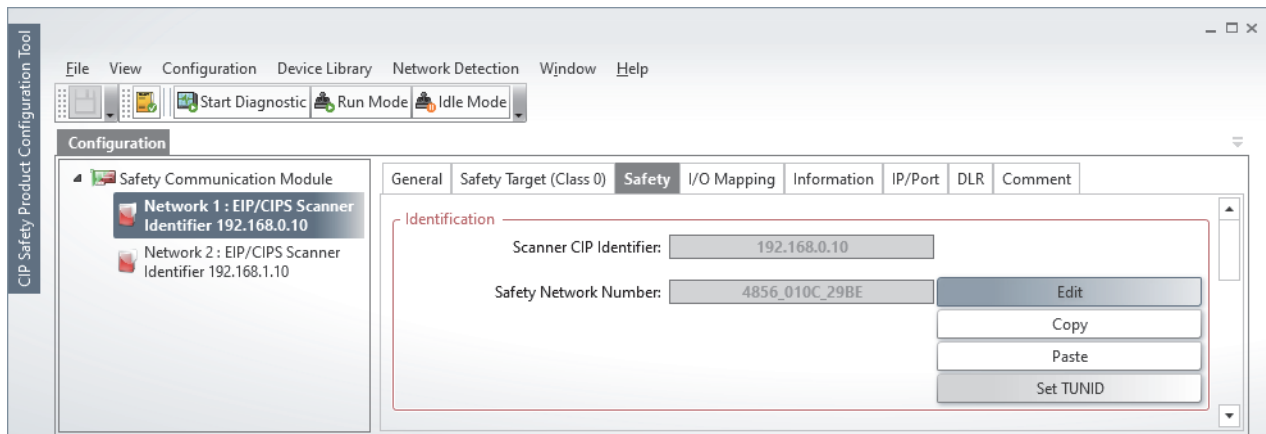
10. After downloading, reset the CPU module or power off and on the system.

11. Start CIP Safety Configuration Tool.

[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

12. Click the [Set TUNID] button.

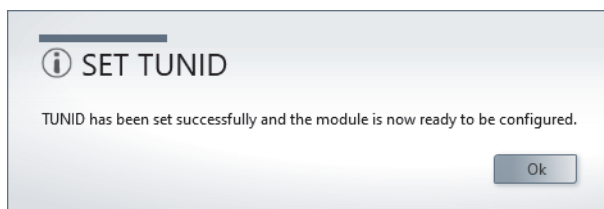
 "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab



Point

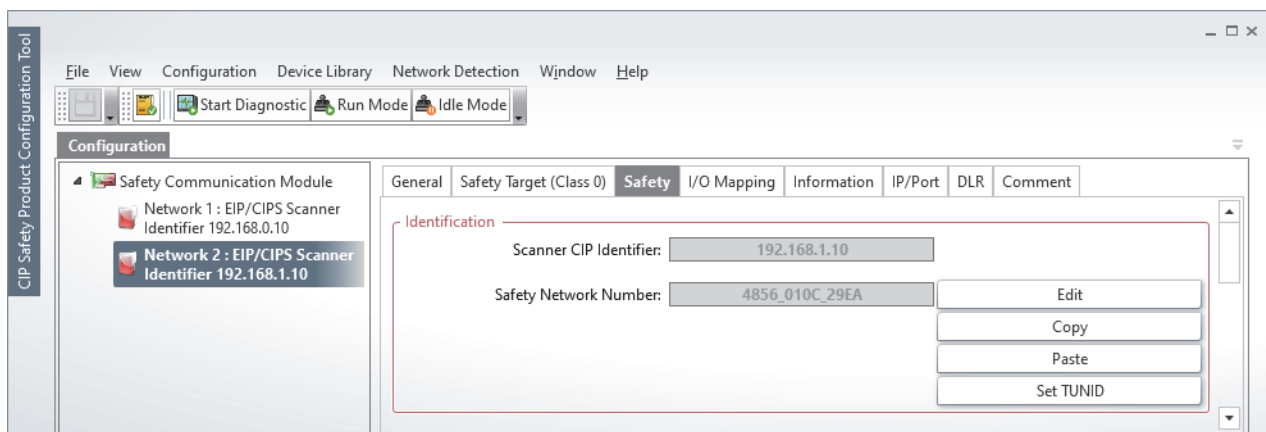
Take notes of the value in "Safety Network Number" to set it to the parameter of CIP Safety module (originator).

13. Click the [OK] button in the following window.

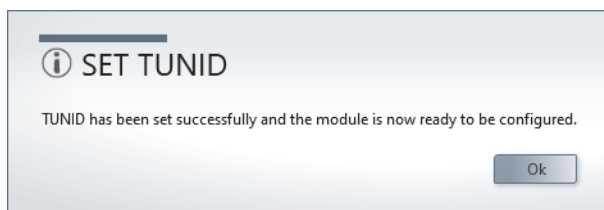


14. Click the [Set TUNID] button.

 "Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab

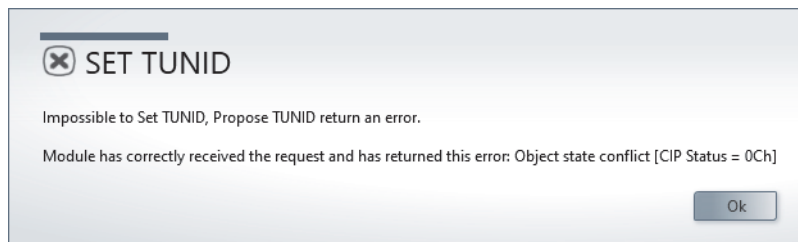


15. Click the [OK] button in the following window.



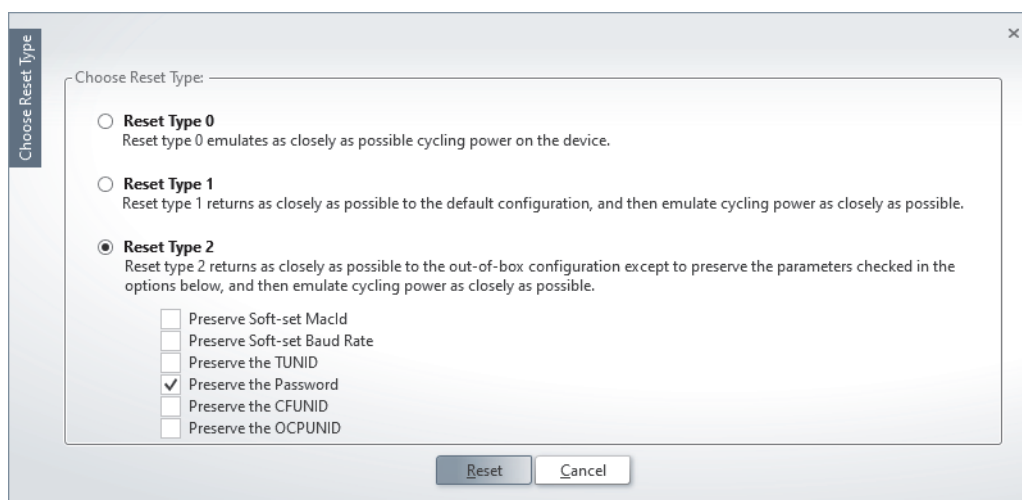
Point

If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.



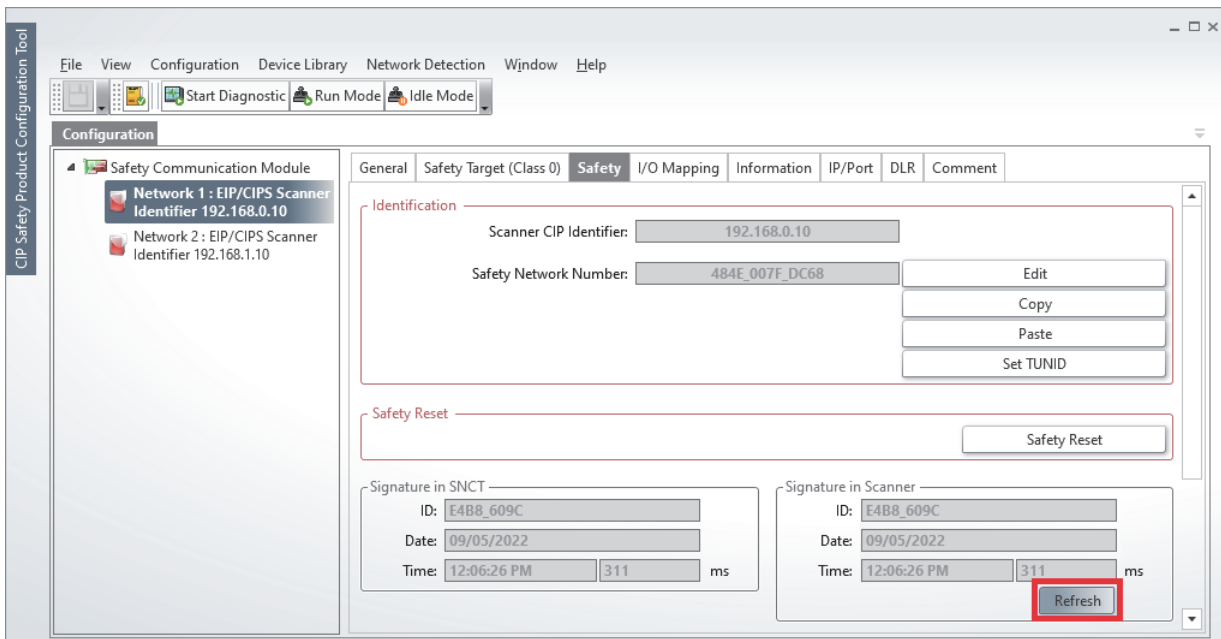
(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
- When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off

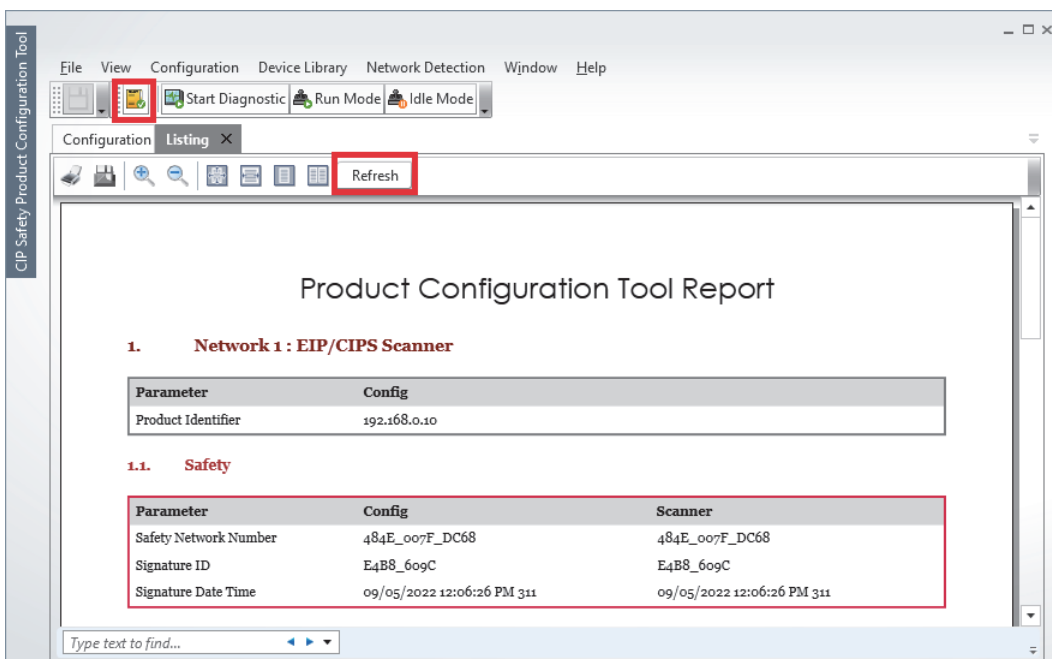
(4) Reset the CPU module or power off and on the system.

16. Check that the values in "Signature in SNCT" and those of "Signature in Scanner" are the same.

🔑 "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab ⇒ [Refresh] button (same procedure for "Network 2: EIP/CIPS Scanner")



17. Click the [Display listing information on the current project] button and check that the parameters in the [Listing] tab is changed to the required settings. (Same procedure for "Network 2: EIP/CIPS Scanner")



Point

- Steps 17 and 18 must be performed for each port for which parameters have been set.
- To output a list, close the [Listing] tab being displayed, then output the list. (Or, click the [Refresh] button in the tab.)
- "Signature ID" and "Signature Date Time" in the [Config] column are displayed when "Enable Signature" is selected.

🔑 Page 77 [Safety Settings] tab

18. Close CIP Safety Configuration Tool.

19. Reset the CPU module or power off and on the system.

■Parameter settings for the CIP Safety module (originator)

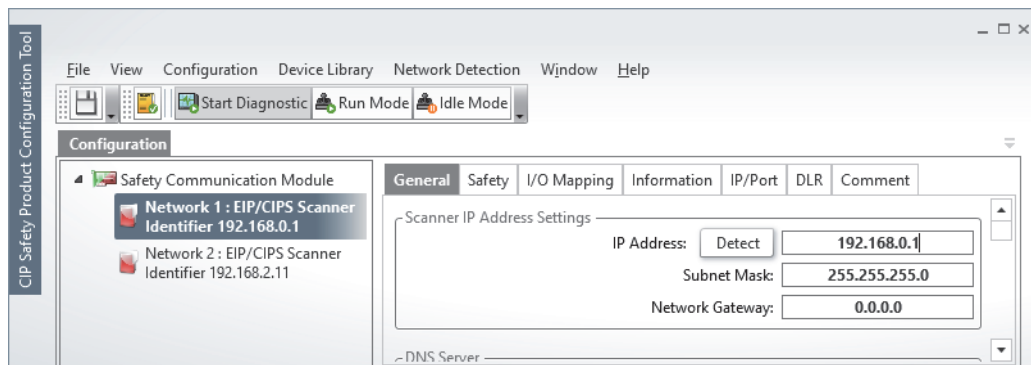
Operating procedure

1. Start CIP Safety Configuration Tool.

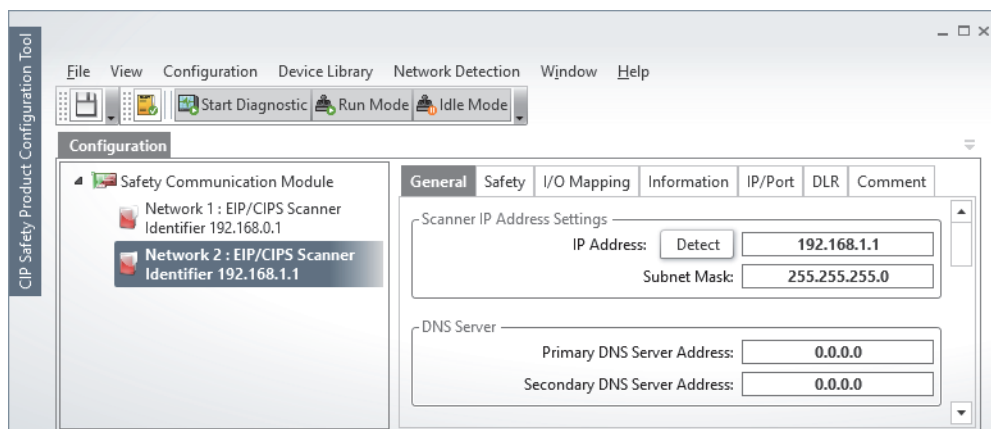
[Navigation window] ⇒ [Parameter] ⇒ [Module Information] ⇒ [RJ71SEIP91-T4] ⇒ [CIP Safety Configuration Tool]

2. Set the IP addresses.

- Select "Network 1: EIP/CIPS Scanner" and set 192.168.0.1 to "IP Address" (P1).



- Select "Network 2: EIP/CIPS Scanner" and set 192.168.1.1 to "IP Address" (P2).



3. Register an EDS file of the external device (target).

In this program example, registration of the EDS file is not required because the external device is the CIP Safety module.

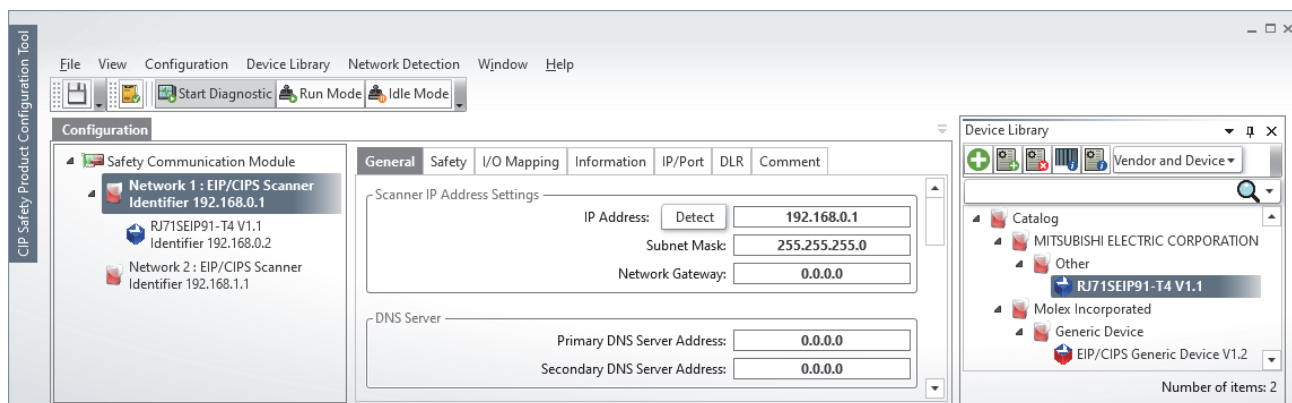
Point

To connect an external device whose EDS file is not registered as the target, register the EDS file of the device to the library. Once the EDS file is registered, re-registration is not required.

To register the EDS file, use the [Add EDS] icon in [Device Library] in CIP Safety Configuration Tool.

☞ Page 81 Adding EDS files

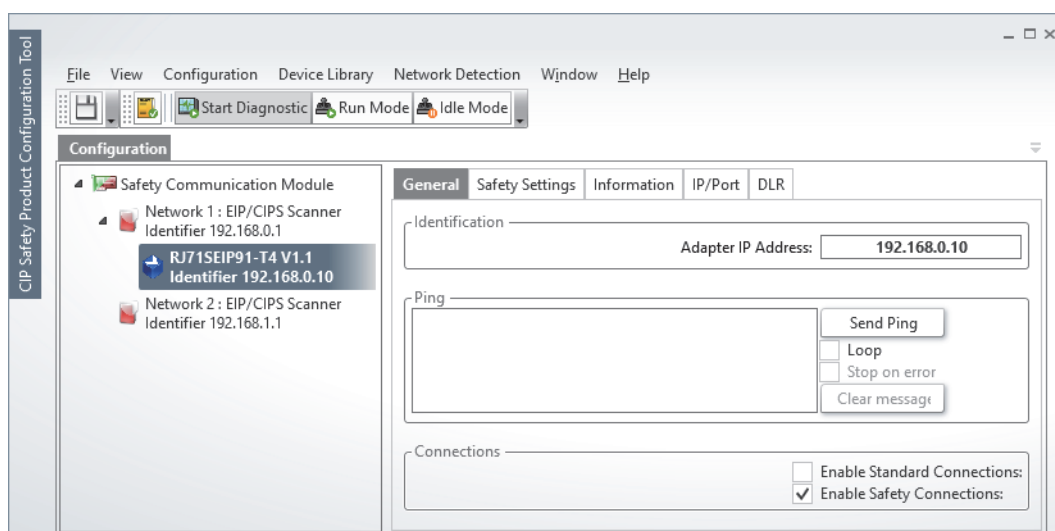
4. Add (drag and drop) the external device (target) to "Network 1: EIP/CIPS Scanner". (Connection No.1)



5. Set the external device (target) added.

- [General] tab

Item	Setting value
Adapter IP Address	192.168.0.10
Enable Standard Connections	Not selected
Enable Safety Connections	Selected



• [Safety Settings] ⇒ [Safety Parameters] tab

Item		Setting value
Identification	Safety Network Number	A value in "Safety Network Number" of the target
Signature in SNCT	Enable Signature	Not selected

CIP Safety Product Configuration Tool

File View Configuration Device Library Network Detection Window Help

Start Diagnostic Run Mode Idle Mode

Configuration

Safety Communication Module

- Network 1 : EIP/CIPS Scanner Identifier 192.168.0.1
- RJ71SEIP91-T4 V1.1 Identifier 192.168.0.10**
- Network 2 : EIP/CIPS Scanner Identifier 192.168.1.1

General Safety Settings Information IP/Port DLR

Safety Parameters Safety Connections

General

Configuration Type: Externally Initialized

Identification

Adapter CIP identifier: 192.168.0.10

Safety Network Number: 4856_010C_298E

Edit

Copy

Paste

Set TUNID

Safety Reset

Safety Reset

Signature in SNCT

☐ Enable Signature

ID: ###

Date: ###

Time: ### ms

Copy Paste

Signature in Device

ID: ###

Date: ###

Time: ### ms

Copy Refresh

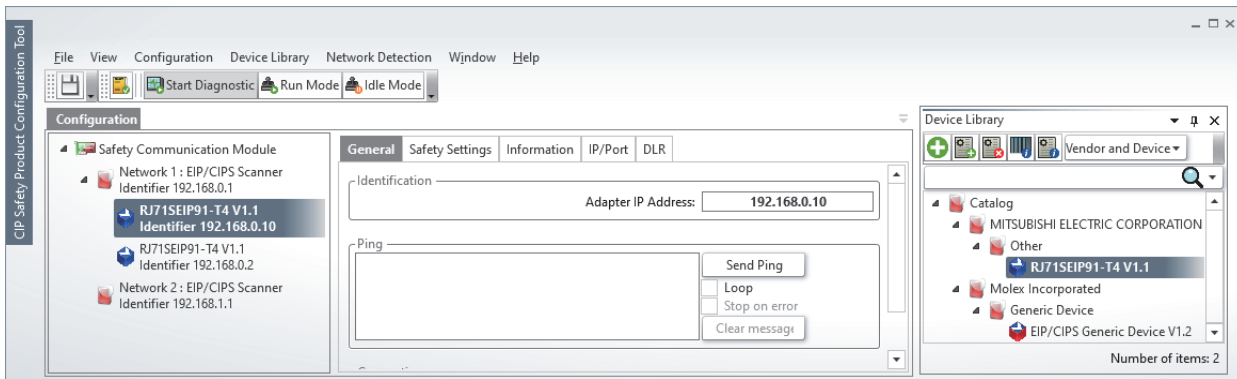
- [Safety Settings] ⇒ [Safety Connections] tab

Item		Setting value
Connection Type	Input Format	Safety Input Class0 Tag
	Output Format	None
	Input Connection Parameters (Target To Originator)	Safety Input
		EPI
		14
		12
	Symbol Ansi	MyTag ^{*1}

*1 This tag name is for the connection destination. Set the same tag name as that of the target.

The screenshot shows the '0020 - CIP Safety Product Configuration Tool' window. The 'Configuration' pane on the left lists the 'Safety Communication Module' and two networks: 'Network 1: EIP/CIPS Scanner Identifier 192.168.0.1' and 'Network 2: EIP/CIPS Scanner Identifier 192.168.1.1'. The 'Safety Connections' tab is active, displaying various configuration options. The 'General Parameters' section shows 'Safety Format' set to 'Extended'. The 'Keying' section shows 'Check Type' set to 'Compatible Module'. The 'Identification' section shows 'Vendor ID' as 161, 'Product Type' as 140, 'Product Code' as 11, 'Major Version' as 1, and 'Minor Version' as 1. The 'Connection Type' section shows 'Input Format' set to 'Safety Input Class0 Tag' and 'Output Format' set to 'None'. The 'Input Connection Parameters (Target to Originator)' section shows 'Identifier' as 1, 'Safety Input' as 14 bytes, 'Input Mode' as 'Point-to-Point', 'EPI' as 12 ms, 'Input Priority' as 'High', 'Timeout Multiplier' as 2, 'Network Multiplier' as 200, and 'Network Reaction Time' as 60 ms. The 'Input Path Parameters' section shows 'Symbol Ansi' set to 'My Tag'.

6. Add (drag and drop) the external device (target) to "Network 1: EIP/CIPS Scanner". (Connection No.2)

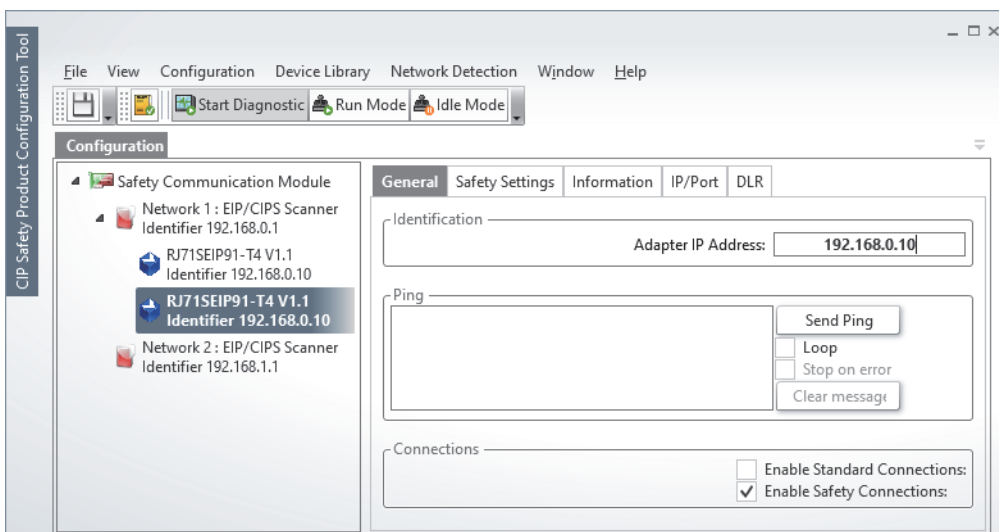


For safety connection, only one connection can be set per external device. Therefore, to add a connection for the same IP address, an external device must be added as well.

7. Set the external device (target) added.

- [General] tab

Item	Setting value
Adapter IP Address	192.168.0.10
Enable Standard Connections	Not selected
Enable Safety Connections	Selected



- [Safety Settings] ⇒ [Safety Parameters] tab

Item		Setting value
Identification	Safety Network Number	A value in "Safety Network Number" of the target
Signature in SNCT	Enable Signature	Not selected

CIP Safety Product Configuration Tool

File View Configuration Device Library Network Detection Window Help

Start Diagnostic Run Mode Idle Mode

Configuration

- Safety Communication Module
 - Network 1 : EIP/CIPS Scanner Identifier 192.168.0.1
 - RJ71SEIP91-T4 V1.1 Identifier 192.168.0.10
 - RJ71SEIP91-T4 V1.1 Identifier 192.168.0.10
 - Network 2 : EIP/CIPS Scanner Identifier 192.168.1.1

General Safety Settings Information IP/Port DLR

Safety Parameters Safety Connections

General

Configuration Type: Externally Initialized

Identification

Adapter CIP identifier: 192.168.0.10

Safety Network Number: 4856_010C_29BE Edit Copy Paste Set TUNID

Safety Reset

Safety Reset

Signature in SNCT

☐ Enable Signature

ID: ###

Date: ###

Time: ### ms Copy Paste

Signature in Device

ID: ###

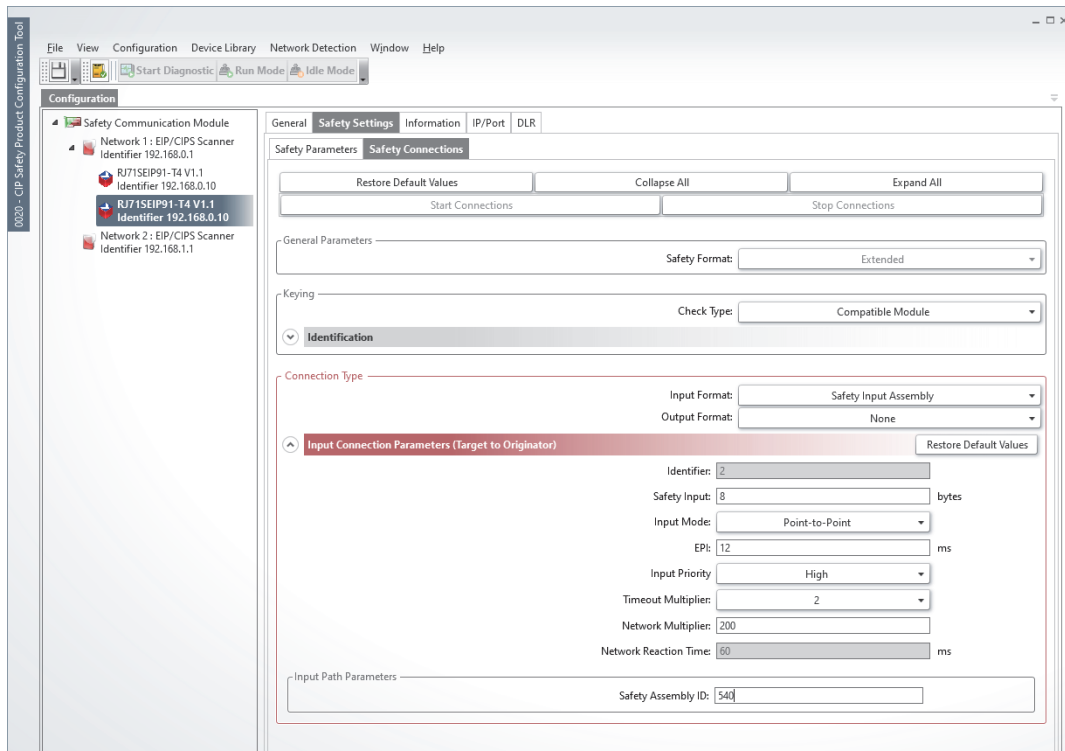
Date: ###

Time: ### ms Copy Refresh

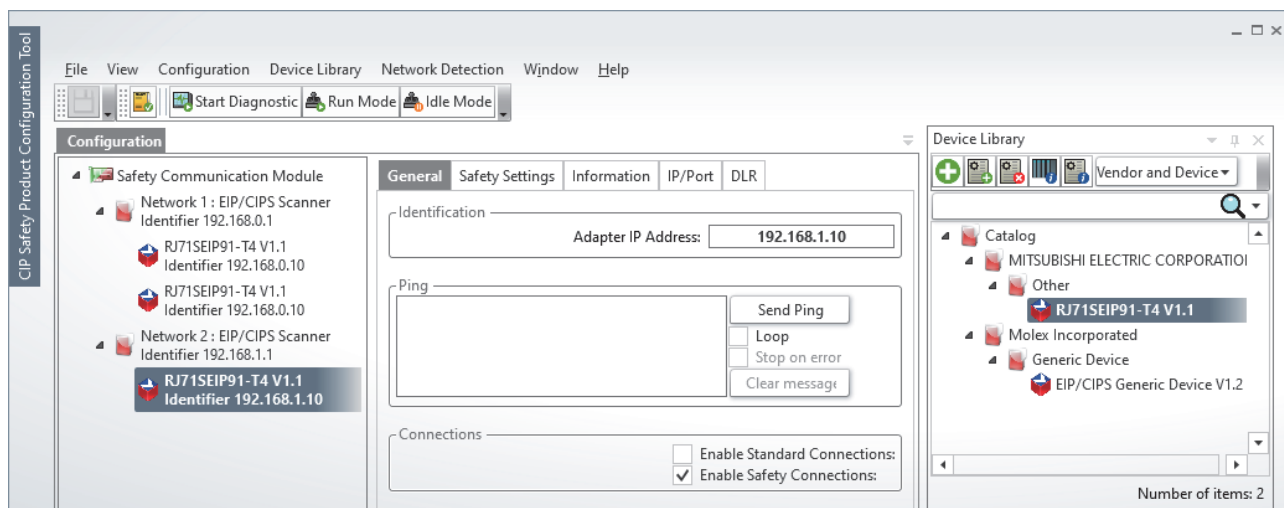
- [Safety Settings] ⇒ [Safety Connections] tab

Item		Setting value
Connection Type	Output Format	None
	Input Connection Parameters (Target To Originator)	Safety Input
		EPI
		Safety Assembly ID
		8
		12
		540 ^{*1}

*1 This Assembly ID is for the connection destination. Set the same value as Assembly ID (instance) of the target.



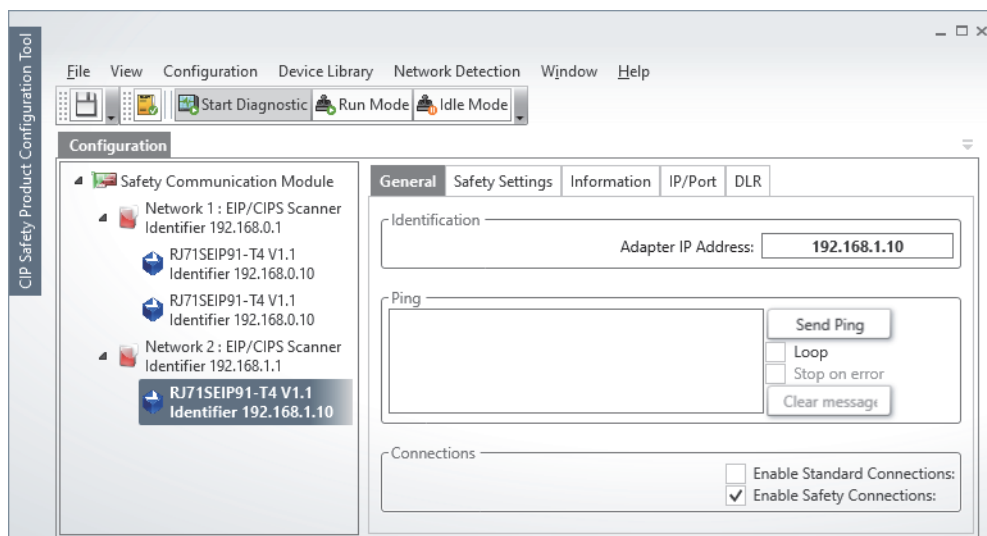
8. Add (drag and drop) the external device (target) to "Network 2: EIP/CIPS Scanner". (Connection No.3)



9. Set the external device (target) added.

- [General] tab

Item	Setting value
Adapter IP Address	192.168.1.10
Enable Standard Connections	Not selected
Enable Safety Connections	Selected



- [Safety Settings] ⇒ [Safety Parameters] tab

Item		Setting value
Identification	Safety Network Number	A value in "Safety Network Number" of the target
Signature in SNCT	Enable Signature	Not selected

CIP Safety Product Configuration Tool

File View Configuration Device Library Network Detection Window Help

Start Diagnostic Run Mode Idle Mode

Configuration

- Safety Communication Module
 - Network 1 : EIP/CIPS Scanner Identifier 192.168.0.1
 - RJ71SEIP91-T4 V1.1 Identifier 192.168.0.10
 - RJ71SEIP91-T4 V1.1 Identifier 192.168.0.10
 - Network 2 : EIP/CIPS Scanner Identifier 192.168.1.1
 - RJ71SEIP91-T4 V1.1 Identifier 192.168.1.10

General Safety Settings Information IP/Port DLR

Safety Parameters Safety Connections

General

Configuration Type: Externally Initialized

Identification

Adapter CIP identifier: 192.168.1.10

Safety Network Number: 4856_010C_29EA Edit Copy Paste Set TUNID

Safety Reset

Safety Reset

Signature in SNCT

☐ Enable Signature

ID: ###

Date: ###

Time: ### ms

Copy Paste

Signature in Device

ID: ###

Date: ###

Time: ### ms

Copy Refresh

- [Safety Settings] ⇒ [Safety Connections] tab

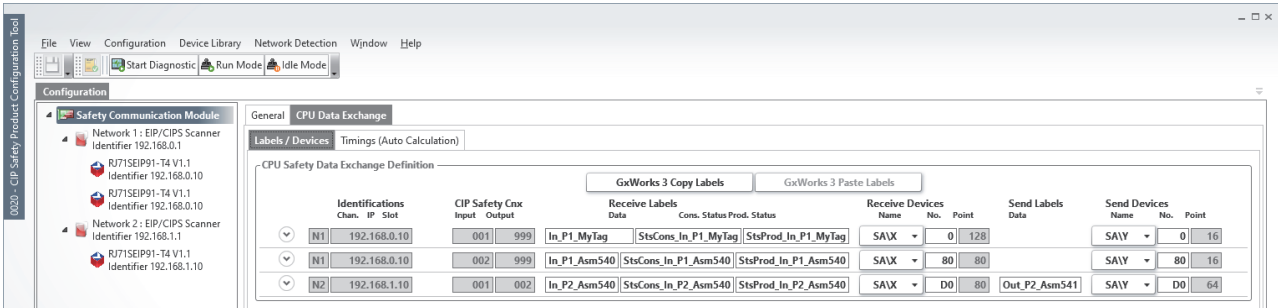
Item		Setting value	
Connection Type	Input Connection Parameters (Target To Originator)	Safety Input	8
		EPI	12
		Safety Assembly ID	540 ^{*1}
	Output Connection Parameters (Originator To Target)	Safety Output	8
		EPI	12
		Safety Assembly ID	541 ^{*1}

*1 This Assembly ID is for the connection destination. Set the same value as Assembly ID (instance) of the target.

The screenshot displays the 'CIP Safety Product Configuration Tool' interface. On the left, a tree view shows the 'Safety Communication Module' configuration, including 'Network 1: EIP/CIPS Scanner' and 'Network 2: EIP/CIPS Scanner'. The main window is divided into tabs: 'General', 'Safety Settings', 'Information', 'IP/Port', and 'DLR'. The 'Safety Settings' tab is active, and the 'Safety Connections' sub-tab is selected. The 'Safety Connections' section contains two main configuration areas: 'Input Connection Parameters (Target to Originator)' and 'Output Connection Parameters (Originator to Target)'. Each area includes fields for 'Identifier', 'Safety Input/Output', 'EPI', 'Input/Output Mode', 'Input/Output Priority', 'Timeout Multiplier', 'Network Multiplier', and 'Network Reaction Time'. The 'Input Path Parameters' section shows 'Safety Assembly ID' set to 540, and the 'Output Path Parameters' section shows 'Safety Assembly ID' set to 541.

10. Select "Safety Communication Module" and set the details in the [CPU Data Exchange] tab.

Receive Labels			Receive Devices	Send Labels	Send Devices
Data	Cons. Status	Prod. Status	No.	Data	No.
In_P1_MyTag	StsCons_In_P1_MyTag	StsProd_In_P1_MyTag	0	—	0
In_P1_Asm540	StsCons_In_P1_Asm540	StsProd_In_P1_Asm540	80	—	80
In_P2_Asm540	StsCons_In_P2_Asm540	StsProd_In_P2_Asm540	D0	Out_P2_Asm541	D0

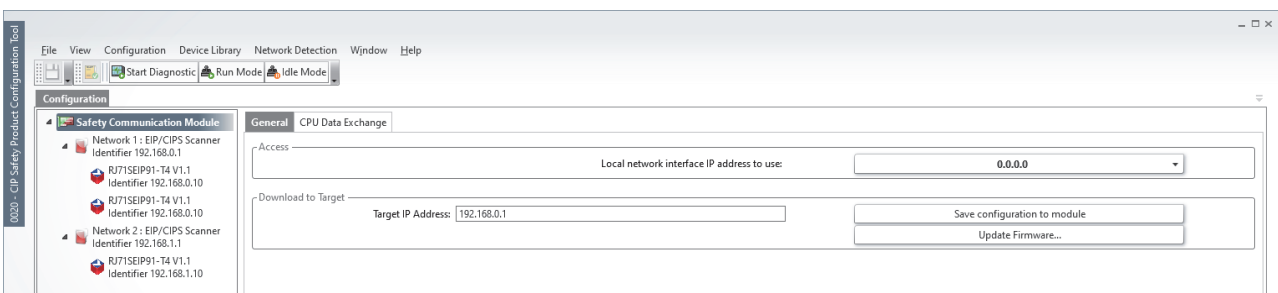


- Since the setting values for EPI and Timeout Multiplier in the connection on the originator side are automatically calculated, entering the values is not required.
- In this example, set the device in order of (SA\X, SA\Y) D0 → 80 → 0 to avoid duplication.
- The following is an example of when a safety device other than SA\X and SA\Y is assigned. (When using a program example, review the assignment of global labels to avoid duplicating the assignment with other devices.)

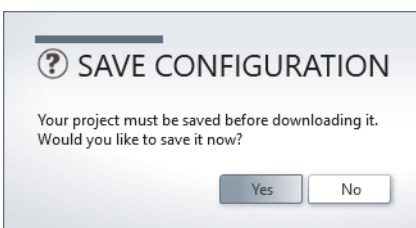
Receive Devices			Send Labels	Send Devices
Name	No.	Point	Data	Name No. Point
SA\D	256	8		SA\D 0 8
SA\M	256	80		SA\M 0 80
SA\B	100	80	Out_P2_Asm541	SA\W 1 4

11. Set the current IP address of the CIP Safety module to "Target IP Address" in the [Safety Communication Module Access] tab.

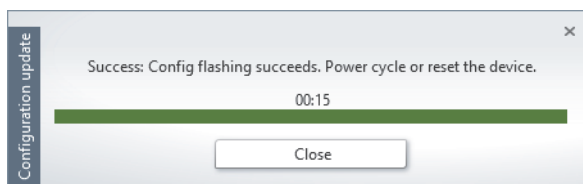
12. Click the [Save configuration to module] button to write the set parameters to the CIP Safety module.



13. Click the [Yes] button in the following window to save the configuration.



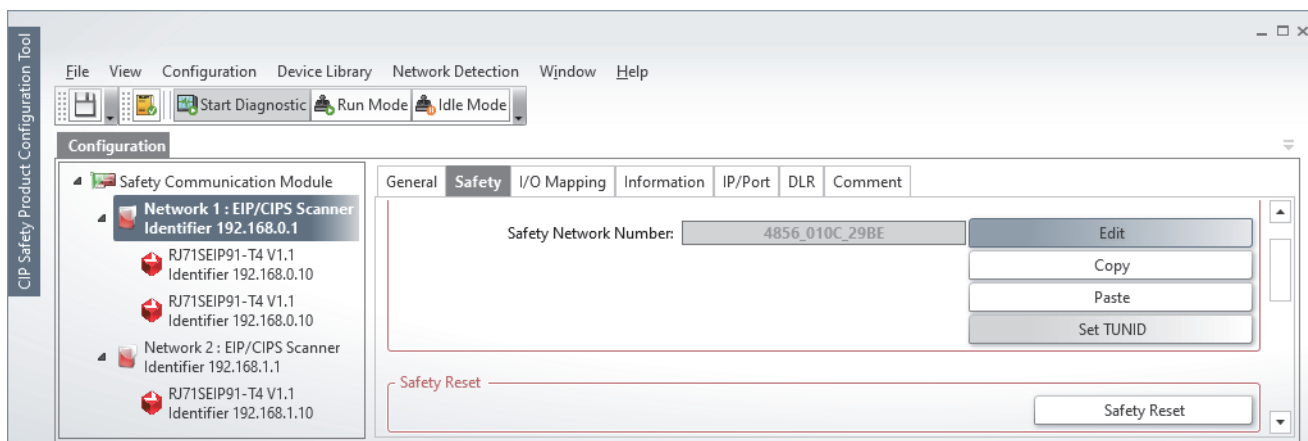
14. Click the [Close] button in the following window to close CIP Safety Configuration Tool.



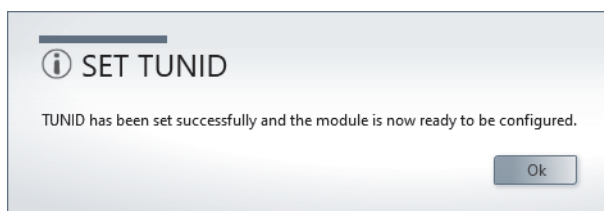
15. After downloading, reset the CPU module or power off and on the system.

16. Click the [Set TUNID] button.

🖱️ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab

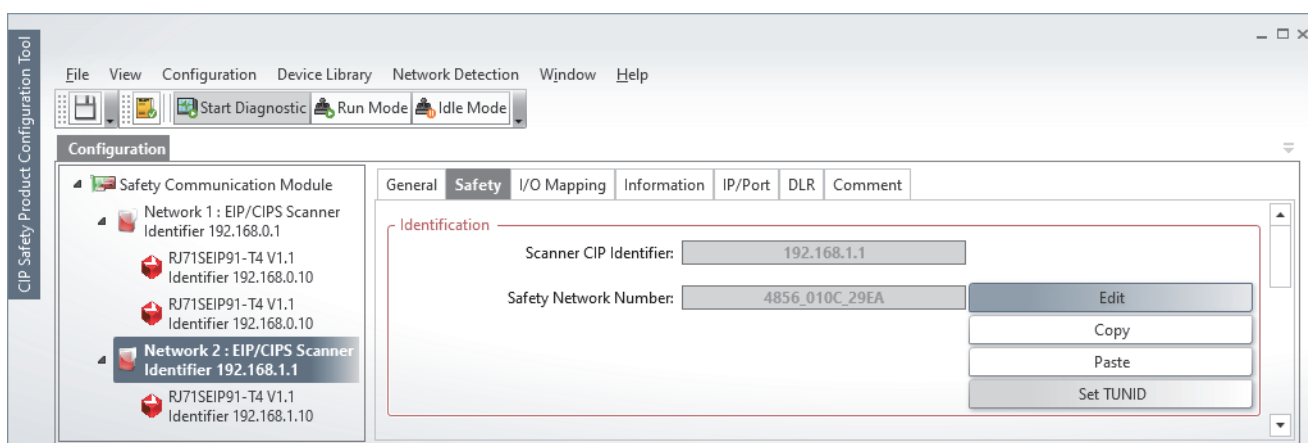


17. Click the [OK] button in the following window.

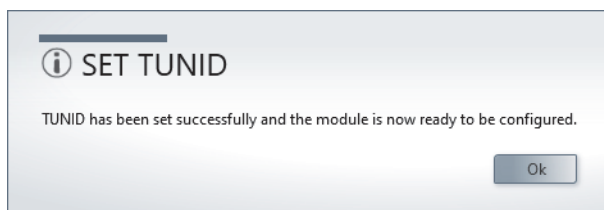


18. Click the [Set TUNID] button.

🖱️ "Network 2: EIP/CIPS Scanner" ⇒ [Safety] tab

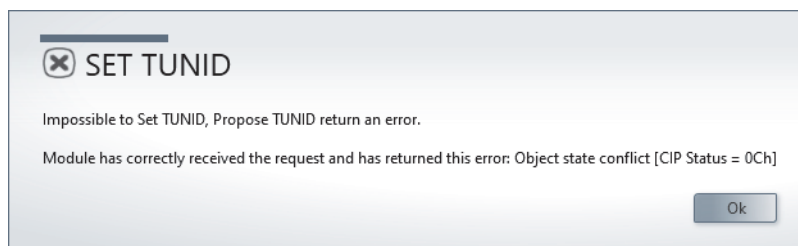


19. Click the [OK] button in the following window.



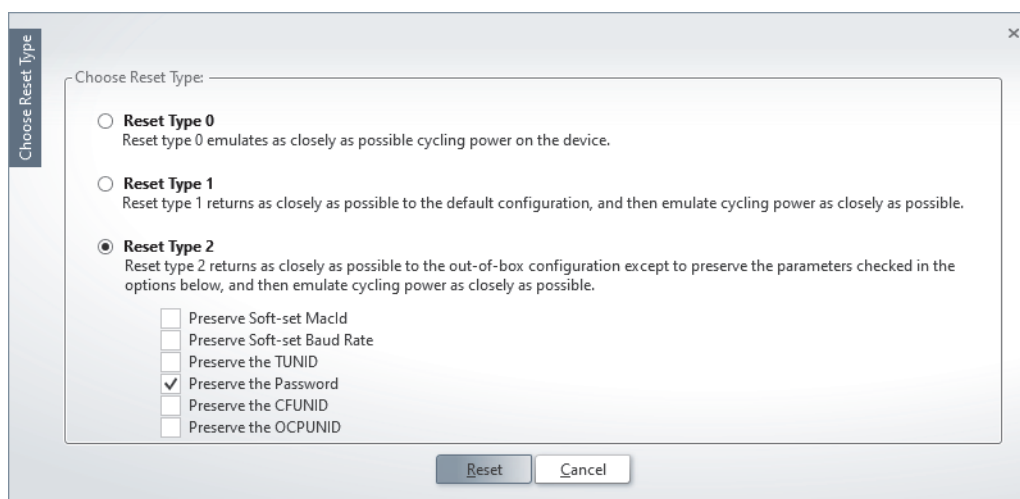
Point

If TUNID is already set to the CIP Safety module, a following error message is displayed.



If the error message is displayed, execute Safety Reset with the following procedure, then set TUNID.

- (1) Reset the CPU module or power off and on the system.
- (2) Click the [Safety Reset] button in the [Safety] tab. When a window appears, select [Reset Type 2] as shown below and click the [Reset] button in the displayed window.



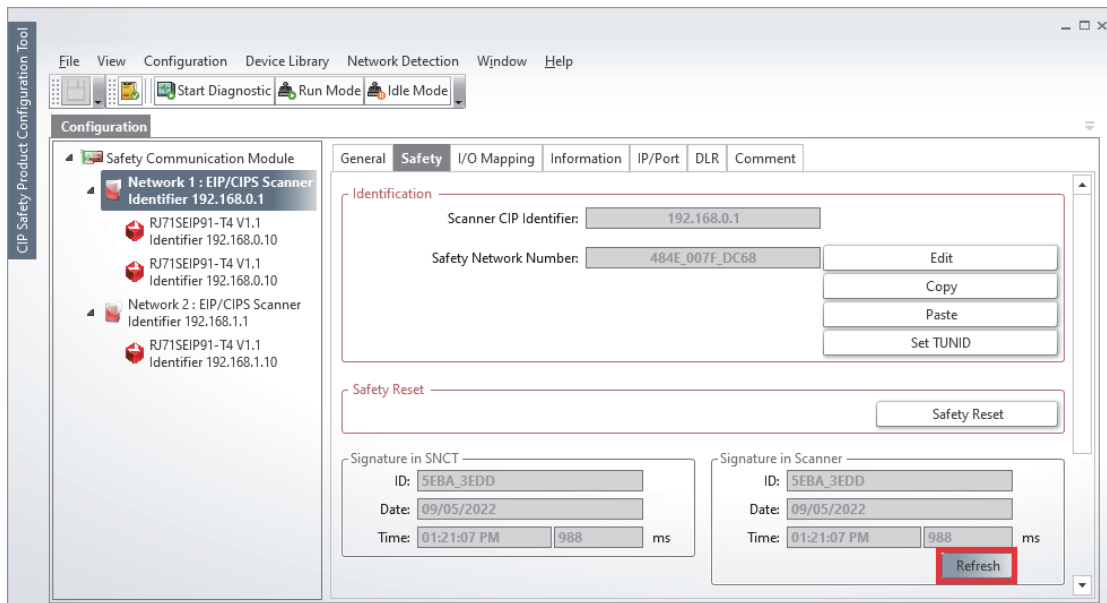
(3) After 10 seconds, the LED status will be as follows.

- Firmware version of the CIP Safety module is "01": MS LED lights up in green, and other LEDs are turned off
- When the firmware version of the CIP Safety module is "02" or later: MS LED lights up in red, and other LEDs are turned off

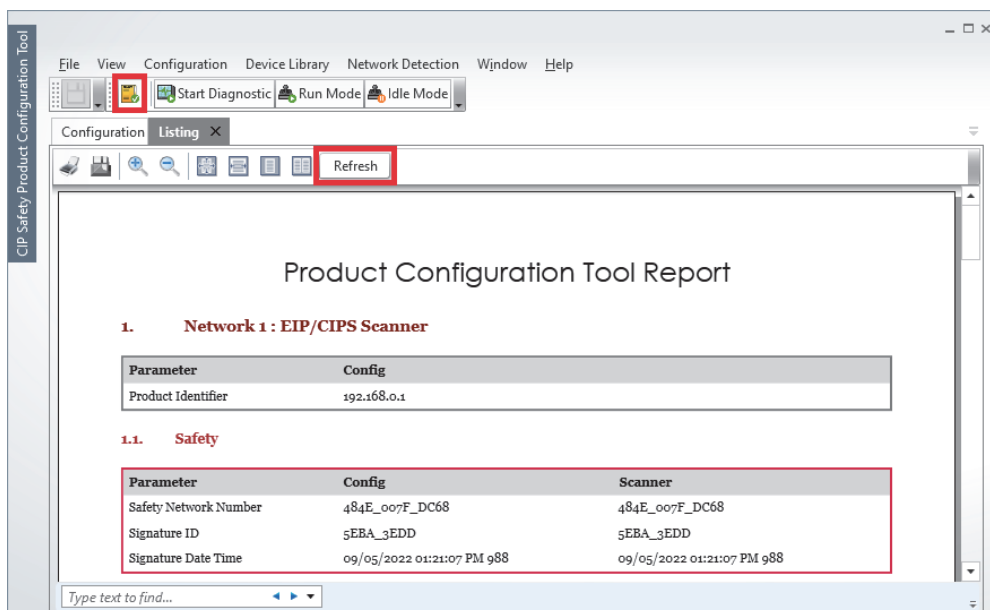
(4) Reset the CPU module or power off and on the system.

20. Check that the values in "Signature in SNCT" and those of "Signature in Scanner" are the same.

🖱️ "Network 1: EIP/CIPS Scanner" ⇒ [Safety] tab ⇒ [Refresh] button (same procedure for "Network 2: EIP/CIPS Scanner")



21. Click the [Display listing information on the current project] button and check that the parameters in the [Listing] tab is changed to the required settings. (Same procedure for "Network 2: EIP/CIPS Scanner")



Point

- Steps 21 and 22 must be performed for each port for which parameters have been set.
- To output a list, close the [Listing] tab being displayed, then output the list. (Or, click the [Refresh] button in the tab.)
- "Signature ID" and "Signature Date Time" in the [Config] column are displayed when "Enable Signature" is selected.

🖱️ Page 77 [Safety Settings] tab

22. Close CIP Safety Configuration Tool.

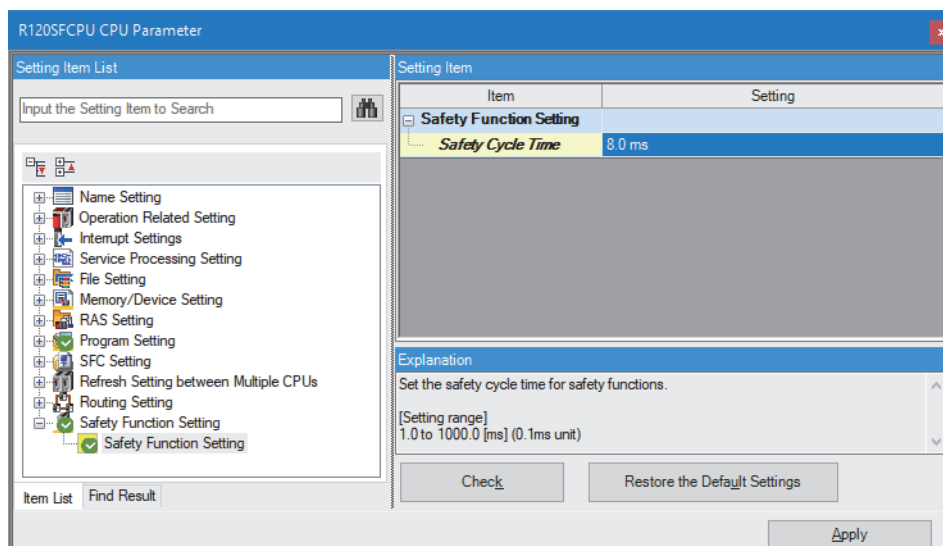
23. Reset the CPU module or power off and on the system.

Settings using the engineering tool

Set [Safety Cycle Time] of CIP Safety Configuration Tool to "Safety Function Setting" of the originator and the target. The value displayed in CIP Safety Configuration Tool is a recommended value. Therefore, adjust the time according to the safety program or other programs.

1. Set "Safety Function Setting" as follows.

 [Navigation window] ⇒ [Parameter] ⇒ [R08SFCPU] ⇒ [CPU Parameter] ⇒ [Safety Function Setting]

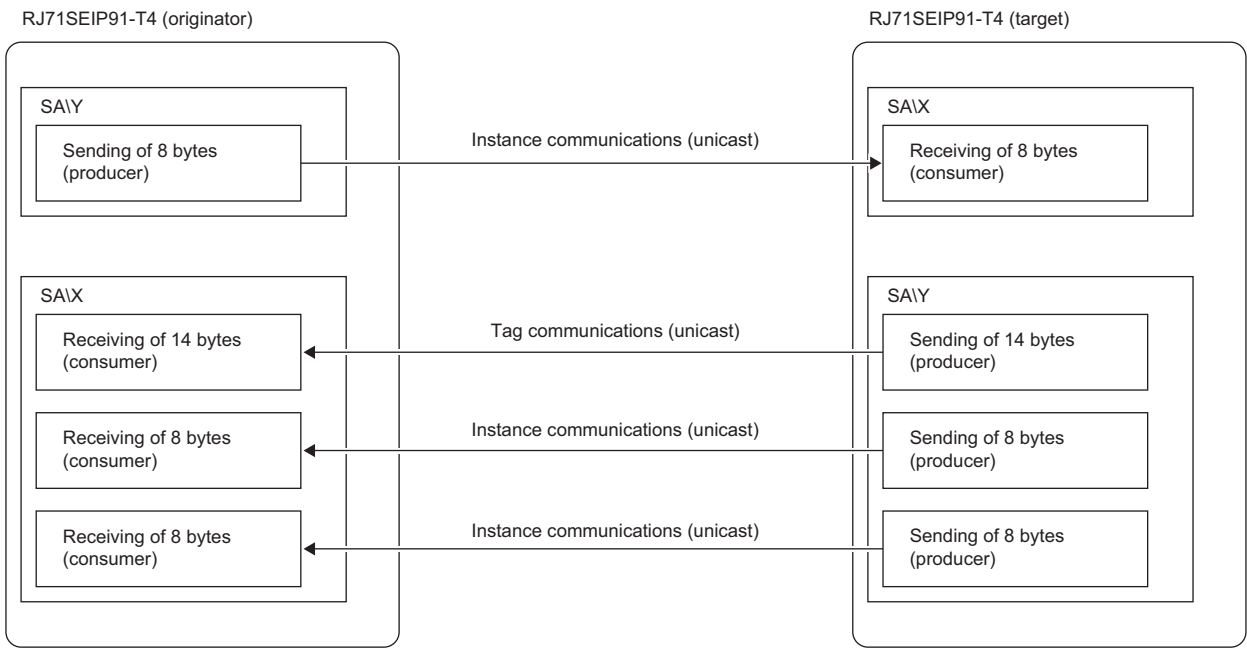


2. Write the set parameter to the CPU module and reset the CPU module or power off and on the system.

 [Online] ⇒ [Write to PLC]

Program example

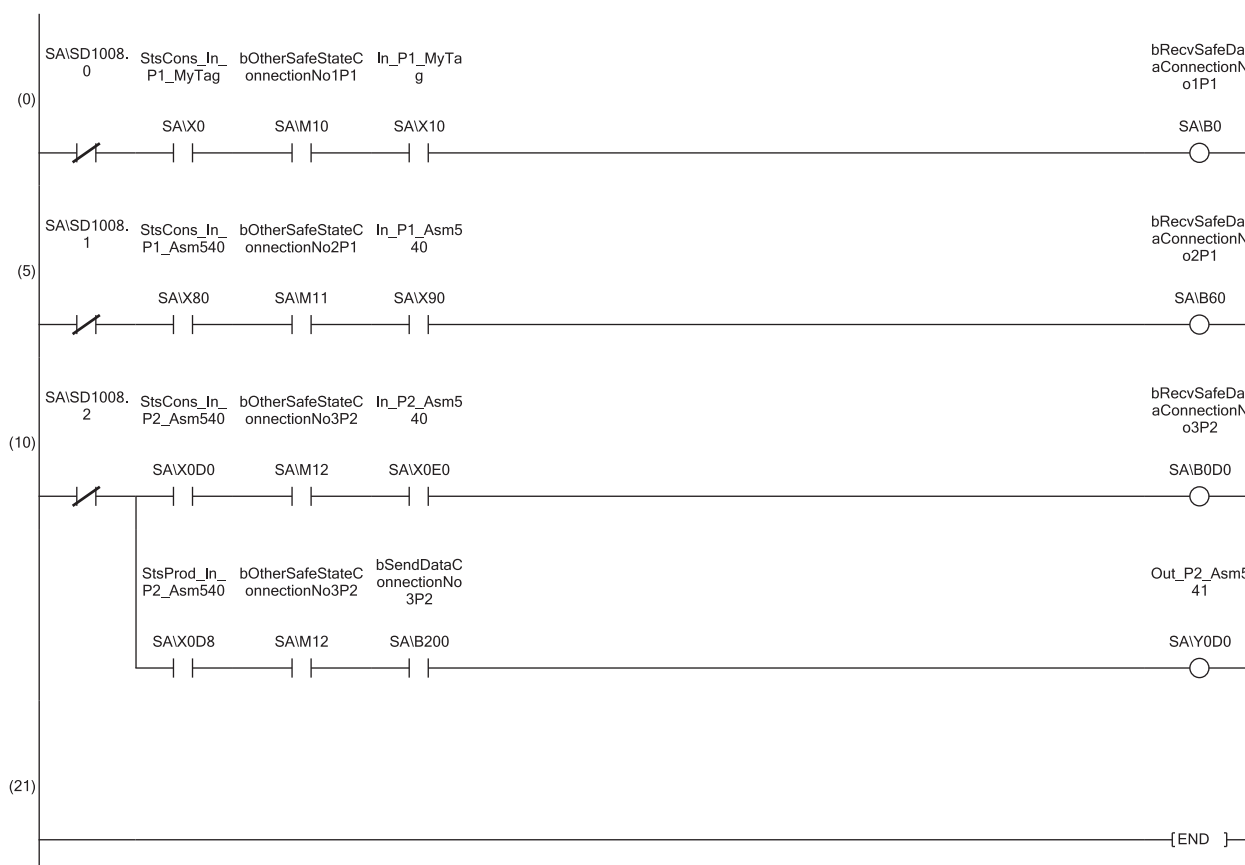
Create this program as a safety program.



Program for the CIP Safety module (originator)

Classification	Description	Device
Safety special register	Safety refresh communication status for each safety connection (1st module) (safety connection No.1)	SA\SD1008.0
	Safety refresh communication status for each safety connection (1st module) (safety connection No.2)	SA\SD1008.1
	Safety refresh communication status for each safety connection (1st module) (safety connection No.3)	SA\SD1008.2
Label to be defined	Define global labels as shown below.	

	Label Name	Data Type	Class	Assign (Device/Label)
1	In_P1_MyTag	Bit(0..111)	VAR_GLOBAL	SA\X10
2	StsCons_In_P1_MyTag	Bit	VAR_GLOBAL	SA\X0
3	StsProd_In_P1_MyTag	Bit	VAR_GLOBAL	SA\X8
4	In_P1_Asm540	Bit(0..63)	VAR_GLOBAL	SA\X90
5	StsCons_In_P1_Asm540	Bit	VAR_GLOBAL	SA\X80
6	StsProd_In_P1_Asm540	Bit	VAR_GLOBAL	SA\X88
7	In_P2_Asm540	Bit(0..63)	VAR_GLOBAL	SA\X0E0
8	StsCons_In_P2_Asm540	Bit	VAR_GLOBAL	SA\X0D0
9	StsProd_In_P2_Asm540	Bit	VAR_GLOBAL	SA\X0D8
10	Out_P2_Asm541	Bit(0..63)	VAR_GLOBAL	SA\Y0D0
11				
12	bOtherSafeStateConnectionNo1P1	Bit	VAR_GLOBAL	SA\M10
13	bOtherSafeStateConnectionNo2P1	Bit	VAR_GLOBAL	SA\M11
14	bOtherSafeStateConnectionNo3P2	Bit	VAR_GLOBAL	SA\M12
15	bRecvSafeDataConnectionNo1P1	Bit	VAR_GLOBAL	SA\B0
16	bRecvSafeDataConnectionNo2P1	Bit	VAR_GLOBAL	SA\B60
17	bRecvSafeDataConnectionNo3P2	Bit	VAR_GLOBAL	SA\B0D0
18	bSendDataConnectionNo3P2	Bit	VAR_GLOBAL	SA\B200



■Communication program for safety connection No.1

(0) When SA\SD1008.0 is normal and SA\X0 is on, safety input of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo1P1*1 is on in this state, if the safety input data is received, bRecvSafeDataConnectionNo1P1 turns on.

■Communication program for safety connection No.2

(5) When SA\SD1008.1 is normal and SA\X80 is on, safety input of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo2P1*1 is on in this state, if the safety input data is received, bRecvSafeDataConnectionNo2P1 turns on.

■Communication program for safety connection No.3

(10) When SA\SD1008.2 is normal and SA\X0D0 is on, safety input of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo3P2*1 is on in this state, if the safety input data is received, bRecvSafeDataConnectionNo3P2 turns on.

In addition, when SA\SD1008.2 is normal and SA\X0D8 is on, safety output of the CIP Safety module is enabled.

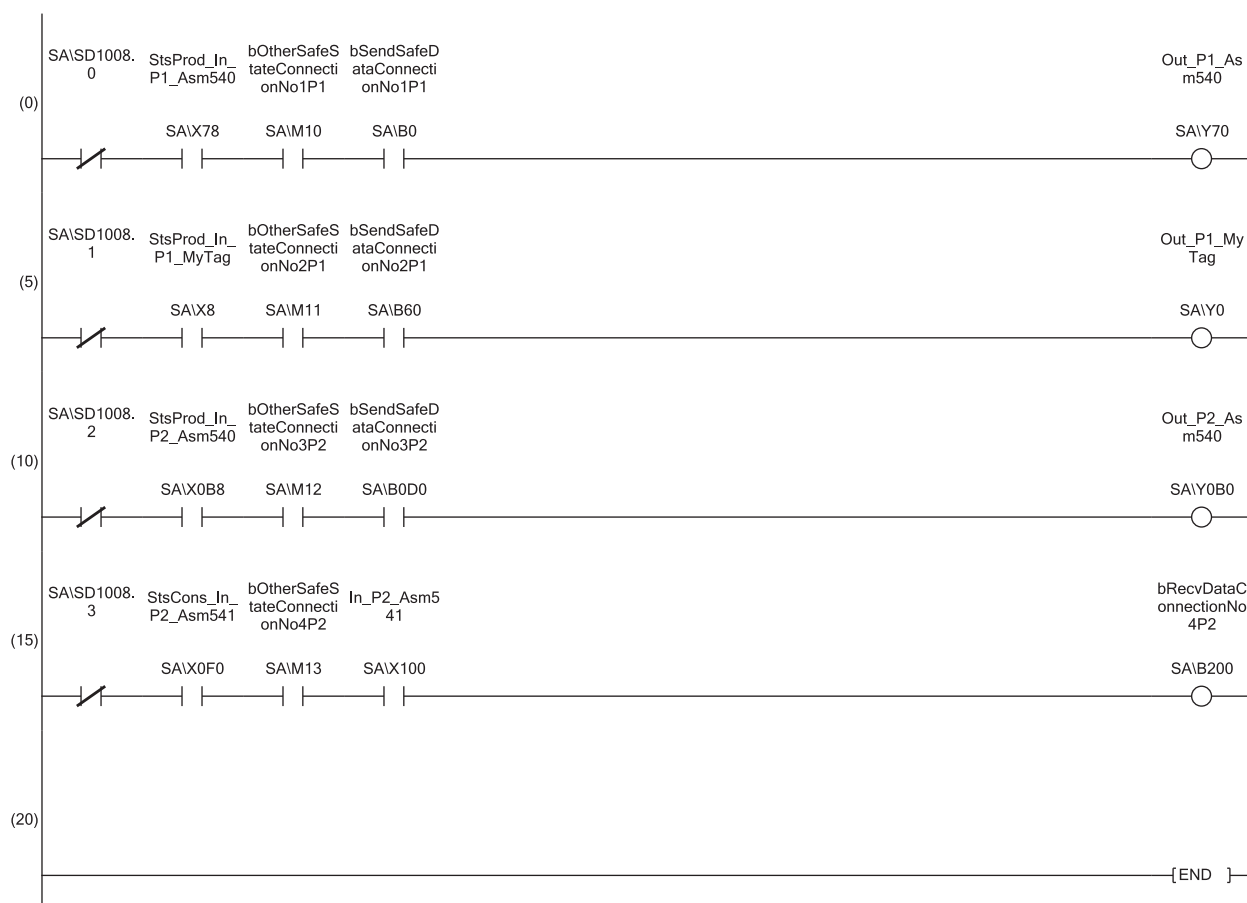
While bOtherSafeStateConnectionNo3P2*1 is on in this state, if bSendDataConnectionNo3P2 is turned on, the safety output data reflects it.

*1 bOtherSafeStateConnection□ is a state defined independently by the user.

Program for the CIP Safety module (target)

Classification	Description	Device
Safety special register	Safety refresh communication status for each safety connection (1st module) (safety connection No.1)	SA\SD1008.0
	Safety refresh communication status for each safety connection (1st module) (safety connection No.2)	SA\SD1008.1
	Safety refresh communication status for each safety connection (1st module) (safety connection No.3)	SA\SD1008.2
	Safety refresh communication status for each safety connection (1st module) (safety connection No.4)	SA\SD1008.3
Label to be defined	Define global labels as shown below.	

	Label Name	Data Type		Class	Assign
1	StsCons_In_P1_Asm540	Bit	VAR_GLOBAL	SA\X70	
2	StsProd_In_P1_Asm540	Bit	VAR_GLOBAL	SA\X78	
3	Out_P1_Asm540	Bit(0..63)	VAR_GLOBAL	SA\Y70	
4	StsCons_In_P1_MyTag	Bit	VAR_GLOBAL	SA\X0	
5	StsProd_In_P1_MyTag	Bit	VAR_GLOBAL	SA\X8	
6	Out_P1_MyTag	Bit(0..111)	VAR_GLOBAL	SA\Y0	
7	StsCons_In_P2_Asm540	Bit	VAR_GLOBAL	SA\X0B0	
8	StsProd_In_P2_Asm540	Bit	VAR_GLOBAL	SA\X0B8	
9	Out_P2_Asm540	Bit(0..63)	VAR_GLOBAL	SA\Y0B0	
10	In_P2_Asm541	Bit(0..63)	VAR_GLOBAL	SA\X100	
11	StsCons_In_P2_Asm541	Bit	VAR_GLOBAL	SA\X0F0	
12	StsProd_In_P2_Asm541	Bit	VAR_GLOBAL	SA\X0F8	
13					
14	bOtherSafeStateConnectionNo1P1	Bit	VAR_GLOBAL	SA\M10	
15	bOtherSafeStateConnectionNo2P1	Bit	VAR_GLOBAL	SA\M11	
16	bOtherSafeStateConnectionNo3P2	Bit	VAR_GLOBAL	SA\M12	
17	bOtherSafeStateConnectionNo4P2	Bit	VAR_GLOBAL	SA\M13	
18	bSendSafeDataConnectionNo1P1	Bit	VAR_GLOBAL	SA\B0	
19	bSendSafeDataConnectionNo2P1	Bit	VAR_GLOBAL	SA\B60	
20	bSendSafeDataConnectionNo3P2	Bit	VAR_GLOBAL	SA\B0D0	
21	bRecvDataConnectionNo4P2	Bit	VAR_GLOBAL	SA\B200	



■Communication program for safety connection No.1

(0) When SA\SD1008.0 is normal and SA\X78 is on, safety output of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo1P1*1 is on in this state, if bSendSafeDataConnectionNo1P1 is turned on, the safety output data reflects it.

■Communication program for safety connection No.2

(5) When SA\SD1008.1 is normal and SA\X8 is on, safety output of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo2P1*1 is on in this state, if bSendSafeDataConnectionNo2P1 is turned on, the safety output data reflects it.

■Communication program for safety connection No.3

(10)When SA\SD1008.2 is normal and SA\X0B8 is on, safety output of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo3P2*1 is on in this state, if bSendSafeDataConnectionNo3P2 is turned on, the safety output data reflects it.

■Communication program for safety connection No.4

(15)When SA\SD1008.3 is normal and SA\X0F0 is on, safety input of the CIP Safety module is enabled.

While bOtherSafeStateConnectionNo4P2*1 is on in this state, if the safety input data is received, bRecvDataConnectionNo4P2 turns on.

*1 bOtherSafeStateConnection□ is a state defined independently by the user.

11 TROUBLESHOOTING

This chapter describes troubleshooting of the CIP Safety module.

11.1 Checking with LEDs

This section describes troubleshooting using the LEDs.

The error status can be determined by the status of the RUN LED and ERR LED.

RUN LED	ERR LED	Error status ^{*1}	Description
Off	Flashing	Major error	An error such as hardware failure or memory failure. The module stops operating.
On	Flashing	Moderate error	An error, such as parameter error, which affects module operation. The module stops operating.
On	On	Minor error	An error that does not effect module operation. The module continues operating.

^{*1} When multiple errors occur, the error status is displayed in the order of major, moderate, and minor.

When the RUN LED turns off

When the RUN LED turns off after the CIP Safety module is powered on, check the following.

Check item	Action
Check if the power of the CPU module is turned on.	Turn on the power.
Check if the CIP Safety module has been properly mounted.	If not, properly mount the module on the base unit.
Check if the system parameters of the CPU module match the configuration of the actual machine.	Write the correct parameters to the CPU module. Then turn the CPU module off and on.
Check if an error has occurred by performing the module diagnostics.	Take actions proposed by the module diagnostics. (Page 205 Checking the Module Status)
Check if an error has been detected in the CIP Safety module using the module diagnostics of the CPU module.	Take actions proposed by the module diagnostics of the CPU module.
Check if power-off or reset was performed while the parameters are being written.	Power off and on or reset the CPU module again to start the CIP Safety module. After that, rewrite the parameters.
Check if the module is powered off and on or reset after performing a firmware update. ^{*1}	Power off and on or reset the CPU module again to start the CIP Safety module.
Other than the above	Power off and on the system. If the problem persists, replace the module.

^{*1} After operation, the module diagnostics of the CPU module may detect a module major error (error code: 2450H) for the CIP Safety module.

When the ERR LED turns on or flashes

When the ERR LED turns on or is flashing, check the following.

Check item	Action
Check if an error has occurred by performing the module diagnostics.	Take actions proposed by the module diagnostics. (Page 205 Checking the Module Status)

When the MS LED turns on in red or is flashing in red

When the MS LED turns on in red or is flashing in red, check the following.

Check item	Action
Check if an error has occurred by performing the module diagnostics.	Take actions proposed by the module diagnostics. (☞ Page 205 Checking the Module Status)
Check if the TUNID between the CIP Safety module and the parameters is mismatched.	Check P1 and P2 of the CIP Safety module and the parameter values using CIP Safety Configuration Tool. If they mismatch, execute Safety Reset to clear the TUNID and re-set the TUNID. <ul style="list-style-type: none"> • How to check the TUNID of the CIP Safety module*1 (☞ Page 63 [Information] tab) • How to check the TUNID of the parameters*2 (☞ Page 60 [Safety] tab)

*1 Can be checked in the item "CIP Identifier, SNN".

*2 TUNID is a combination of "Scanner CIP Identifier" and "Safety Network Number".

When the NS LED turns off

If the NS LED turns off, check the following.

Check item	Action
Is the RUN LED off?	Check the power supply and mounting status. (☞ Page 201 When the RUN LED turns off)
Is the ERR LED on or flashing?	Identify the cause of the error. (☞ Page 201 When the ERR LED turns on or flashes)
Is the SPEED LED to which the Ethernet cable is connected on (link-up)?	<ul style="list-style-type: none"> • Check if the Ethernet cable is properly connected. • Check that the external device (switching hub or device) is connected to the end of the Ethernet cable and that communication is possible. • If the SPEED LED does not turn on (link-up) even after the above action, replace the Ethernet cable.

When the NS LED is flashing in green

When the NS LED is flashing in green, check the following.

Check item	Action
Is the connection set with the external device?	Use CIP Safety Configuration Tool to set the connection with the external device and write the parameters again.
Is the SPEED LED to which the Ethernet cable is connected on (link-up)?	<ul style="list-style-type: none"> • Check if the Ethernet cable is properly connected. • Check that the external device (switching hub or device) is connected to the end of the Ethernet cable and that communication is possible. • If the SPEED LED does not turn on (link-up) even after the above action, replace the Ethernet cable.
Has EtherNet/IP communication started?	Check if 0001H (Communication start) is set to 'EtherNet/IP Communication Start Request' (Un\G98048, Un\G1146624). If not, set the value and start EtherNet/IP communications.
Check the connection status with the following buffer memory. ■CIP Safety <ul style="list-style-type: none"> • 'Data link status' (Un\G16896 to Un\G16911, Un\G1065472 to Un\G1065487) • 'Error status' (Un\G16912 to Un\G16927, Un\G1065488 to Un\G1065503) • 'CIP Safety own station connection error status' (Un\G16928 to Un\G17407, Un\G1065504 to Un\G1065983) ■EtherNet/IP Class1 <ul style="list-style-type: none"> • 'Class1 communication status' (Un\G99408 to Un\G99447, Un\G1147984 to Un\G1148023) • 'Class1 Connection Behavior Error status' (Un\G99584 to Un\G100351, Un\G1148160 to Un\G1148927) ■EtherNet/IP UCMM <ul style="list-style-type: none"> • 'UCMM communication (No.1 to No.32) response area' (Un\G154624 to Un\G219135, Un\G1203200 to Un\G1267711) 	<ul style="list-style-type: none"> • Check the bit of the corresponding connection number in the data link status in each communication status. If the bit of each data link status is not on, check whether the connection with the external device is set from CIP Safety Configuration Tool. • In each communication status, check the bit of the connection number corresponding to the error status. If the error status bit is on, check the error code for each connection status, and take actions corresponding to the error code. (☞ Page 217 When the connection is abnormal)
Are the parameter settings correct?	Revise the following contents of CIP Safety Configuration Tool. <ul style="list-style-type: none"> • Model and name of the connected EtherNet/IP device • IP address of the connected EtherNet/IP device • Version of the registered EDS file
Is the ERR LED on or flashing?	Identify the cause of the error. (☞ Page 201 When the ERR LED turns on or flashes)

When the NS LED is flashing in red

When the NS LED is flashing in red, check the following.

Check item	Action
Is the SPEED LED to which the Ethernet cable is connected on (link-up)?	<ul style="list-style-type: none"> • Check if the Ethernet cable is properly connected. • Check that the external device (switching hub or device) is connected to the end of the Ethernet cable and that communication is possible. • If the SPEED LED does not turn on (link-up) even after the above action, replace the Ethernet cable.
Check the connection that has timed out with the following buffer memory. ■CIP Safety <ul style="list-style-type: none"> • 'Data link status' (Un\G16896 to Un\G16911, Un\G1065472 to Un\G1065487) • 'Error status' (Un\G16912 to Un\G16927, Un\G1065488 to Un\G1065503) ■EtherNet/IP Class1 <ul style="list-style-type: none"> • 'Class1 communication status' (Un\G99408 to Un\G99447, Un\G1147984 to Un\G1148023) ■EtherNet/IP UCMM <ul style="list-style-type: none"> • 'UCMM communication (No.1 to No.32) response area' (Un\G154624 to Un\G219135, Un\G1203200 to Un\G1267711) 	Identify the external device from the timeout connection and perform the subsequent checks.
Can the module communicate with the external device?	Check if the external device can perform EtherNet/IP connection communications (by examining the device status and settings). For details, refer to the manuals of the external device.
Use the software or hardware monitoring the line to check the load on the line and the effect of noise.	<ul style="list-style-type: none"> • Reduce the line load. (Such as by reducing and distributing communication) • Take measures to reduce noise. (Such as by removing the source of noise, using the noise-resistant cable, and changing the wiring)

When the NS LED is on in red

When the NS LED is on in red, check the following.

Check item	Action
Is the ERR LED on or flashing?	Identify the cause of the error. (🔍 Page 201 When the ERR LED turns on or flashes)
Check the error code of the following buffer memory. ■CIP Safety <ul style="list-style-type: none"> • 'Data link status' (Un\G16896 to Un\G16911, Un\G1065472 to Un\G1065487) • 'Error status' (Un\G16912 to Un\G16927, Un\G1065488 to Un\G1065503) • 'CIP Safety own station connection error status' (Un\G16928 to Un\G17407, Un\G1065504 to Un\G1065983) ■EtherNet/IP Class1 <ul style="list-style-type: none"> • 'Class1 communication status' (Un\G99408 to Un\G99447, Un\G1147984 to Un\G1148023) • 'Class1 Connection Behavior Error status' (Un\G99584 to Un\G100351, Un\G1148160 to Un\G1148927) ■EtherNet/IP UCMM <ul style="list-style-type: none"> • 'UCMM communication (No.1 to No.32) response area' (Un\G154624 to Un\G219135, Un\G1203200 to Un\G1267711) 	Take actions corresponding to the error code. (🔍 Page 217 When the connection is abnormal)

When the SAFETY COM RUN LED turns off

If the SAFETY COM RUN LED turns off, check the following items.

Check item	Action
Is the SAFETY FUNCTION LED off?	Use CIP Safety Configuration Tool to set the connection with the external device and write the parameters again.
Is the SPEED LED to which the Ethernet cable is connected on (link-up)?	<ul style="list-style-type: none"> • Check if the Ethernet cable is properly connected. • Check that the external device (switching hub or device) is connected to the end of the Ethernet cable and that communication is possible. • If the SPEED LED does not turn on (link-up) even after the above action, replace the Ethernet cable.
Check the connection status with the following buffer memory. ■CIP Safety <ul style="list-style-type: none"> • 'Data link status' (Un\G16896 to Un\G16911, Un\G1065472 to Un\G1065487) • 'Error status' (Un\G16912 to Un\G16927, Un\G1065488 to Un\G1065503) • 'CIP Safety own station connection error status' (Un\G16928 to Un\G17407, Un\G1065504 to Un\G1065983) 	<ul style="list-style-type: none"> • Check the bit of the corresponding connection number in the data link status in each communication status. If the bit of each data link status is not on, check whether the connection with the external device is set from CIP Safety Configuration Tool. • In each communication status, check the bit of the connection number corresponding to the error status. If the error status bit is on, check the error code for each connection status, and take actions corresponding to the error code. (☞ Page 217 When the connection is abnormal)
Are the parameter settings correct?	Revise the following contents of CIP Safety Configuration Tool. <ul style="list-style-type: none"> • Model and name of the connected CIP Safety device • IP address of the connected CIP Safety device • Version of the registered EDS file
Is the ERR LED on or flashing?	Identify the cause of the error. (☞ Page 201 When the ERR LED turns on or flashes)

When the SAFETY COM ERR LED turns on

When the SAFETY COM ERR LED turns on, check the following.

Check item	Action
Is the ERR LED on?	Identify the cause of the error. (☞ Page 201 When the ERR LED turns on or flashes)
Is the SPEED LED to which the Ethernet cable is connected on (link-up)?	<ul style="list-style-type: none"> • Check if the Ethernet cable is properly connected. • Check that the external device (switching hub or device) is connected to the end of the Ethernet cable and that communication is possible. • If the SPEED LED does not turn on (link-up) even after the above action, replace the Ethernet cable.
Check the connection that has timed out with the following buffer memory. ■CIP Safety <ul style="list-style-type: none"> • 'Data link status' (Un\G16896 to Un\G16911, Un\G1065472 to Un\G1065487) • 'Error status' (Un\G16912 to Un\G16927, Un\G1065488 to Un\G1065503) 	Identify the external device from the timeout connection and perform the subsequent checks.
Can the module communicate with the external device?	Check if the external device can communicate with CIP Safety (by examining the device status and settings). For details, refer to the manuals of the external device.
Are the parameter settings correct?	Revise the following contents of CIP Safety Configuration Tool. <ul style="list-style-type: none"> • Transmission interval monitoring time • Safety refresh monitoring time • Time out Multiplier
Use the software or hardware monitoring the line to check the load on the line and the effect of noise.	<ul style="list-style-type: none"> • Reduce the line load. (Such as by reducing and distributing communication) • Take measures to reduce noise. (Such as by removing the source of noise, using the noise-resistant cable, and changing the wiring)

11.2 Checking the Module Status

The following functions can be used in the "Module Diagnostics" window for the CIP Safety module.

Function	Application
Error Information	Displays the details of the errors currently occurring. Click the [Event History] button to check the history of errors that have occurred on the CIP Safety, errors detected for each module, and operations that have been executed.
Module Information List	Displays various status information of the CIP Safety module.

Error information

Check the details of the error currently occurring and action to eliminate the error.

Module Diagnostics(Start I/O No. 0020)

Module Name: RJ71SEIP91-T4

Supplementary Function: [Dropdown]

Display Format of Error Code: ☐ Decimal ☒ Hexadecimal

No.	Occurrence Date	Status	Error Code	Overview
1	2000/01/01 04:22:22.901	Major	H1F04	Safety communication timeout

Legend: Major (Red Triangle), Moderate (Yellow Triangle), Minor (Green Triangle)

Cause: A timeout error occurred during safety communication.

Corrective Action: -Check the safety communication settings. After check the settings, write the parameters to CIP Safety module and CPU module again, reset CPU module and then RUN.
-If the parameters are set correctly, noise on the bus or hardware failure may be the cause. If the same error occurs again even after noise suppression, the module may be faulty. Please consult your local Mitsubishi representative.

Buttons: Error Jump, Event History, Clear Error, Detail, Create File..., Close

Item	Description
Status	Major: An error such as hardware failure or memory failure. The module stops operating. Moderate: An error, such as parameter error, which affects module operation. The module stops operating. Minor: An error that does not effect module operation. The module continues operating.
Error Code	Page 212 List of Error Codes
[Error Jump] button	Cannot be used for the CIP Safety module.
[Event History] button	Click to display the errors that have occurred on the network and the history of the errors detected and the operations executed on each module. (Page 222 Event List)
[Error reset] button	Cannot be used for the CIP Safety module.
Detailed Information	Displays detailed information about each error (maximum of three pieces).
Cause	Displays the detailed error causes.
Action	Displays the actions to eliminate the error causes.

Module Information List

Switch to the [Module Information List] tab to display each status information of the CIP Safety module.

Module Name
RJ71SEIP91-T4

Production information

Supplementary Function

Execute

Monitoring

Stop Monitoring

Display Format of Error Code

☐ Decimal

☒ Hexadecimal

Error Information

Module Information List

Item	Content
LED Information(Module)	
RUN/ERR	On(Green)/Off: Normal operation
LED Information(Communication)	
MS	On(Red): Operation stop(Major error occurrence)
NS(P1)	On(Red): Offline(Port stop error occurred)
NS(P2)	On(Red): Offline(Port stop error occurred)
LED Information(Safety)	
SAFETY FUNCTION(P1)	513
SAFETY COM RUN(P1)	513
SAFETY COM ERR(P1)	Off: No timeout on safety connection
SAFETY FUNCTION(P2)	513
SAFETY COM RUN(P2)	513
SAFETY COM ERR(P2)	Off: No timeout on safety connection
Discrete Information	
P1 IP Address(1st Octet)	192
P1 IP Address(2nd Octet)	168
P1 IP Address(3rd Octet)	0
P1 IP Address(4th Octet)	10
P1 MAC Address(1st Octet)	0
P1 MAC Address(2nd Octet)	0
P1 MAC Address(3rd Octet)	0
P1 MAC Address(4th Octet)	0
P1 MAC Address(5th Octet)	0
P1 MAC Address(6th Octet)	0
P2 IP Address(1st Octet)	192
P2 IP Address(2nd Octet)	168

Create File...

Close

Item			Description
LED information (Module)			Displays the status of the RUN LED and ERR LED of the CIP Safety module.
LED information (Communication)			Displays the status of the MS LED and NS LED of the CIP Safety module.
LED information (Safety)			Displays the status of the SAFETY FUNCTION LED, SAFETY COM RUN LED, and SAFETY COM ERR LED of the CIP Safety module.
Setting information	P1/P2	IP Address (1st Octet)	Displays the IP address of the CIP Safety module.
		IP Address (2nd Octet)	
		IP Address (3rd Octet)	
		IP Address (4th Octet)	
		MAC Address (1st Octet)	Displays the MAC address of the CIP Safety module.
		MAC Address (2nd Octet)	
		MAC Address (3rd Octet)	
		MAC Address (4th Octet)	
		MAC Address (5th Octet)	
		MAC Address (6th Octet)	

11.3 Checking the Network Status

Use the following methods to check the EtherNet/IP network status.

- EtherNet/IP network diagnostics of CIP Safety Configuration Tool
- Checking with the buffer memory

EtherNet/IP network diagnostics of CIP Safety Configuration Tool

The EtherNet/IP network diagnostics of CIP Safety Configuration Tool can be used to check the connection information of EtherNet/IP devices.


For details on CIP Safety Configuration Tool, refer to the following.

 Page 66 [Diagnostics] tab

11



If the CIP Safety module cannot connect to CIP Safety Configuration Tool, refer to the following.


 Page 208 The CIP Safety module cannot connect to CIP Safety Configuration Tool

Checking with the buffer memory

The status of the Class1 communication connections and the error details can be checked with the following buffer memory areas.

- 'Class1 communication status' (Un\G99408 to Un\G99447, Un\G1147984 to Un\G1148023)
- 'Class1 Connection Behavior Error status' (Un\G99584 to Un\G100351, Un\G1148160 to Un\G1148927)

11.4 Troubleshooting by Symptom

This section describes troubleshooting by symptom. If an error has occurred in the CIP Safety module, identify the error cause using the engineering tool. ( Page 205 Checking the Module Status)

The CIP Safety module cannot connect to CIP Safety Configuration Tool

If the CIP Safety module cannot connect to CIP Safety Configuration Tool, check the following items.

Check item	Action
Is the Ethernet cable connected correctly?	Connect the Ethernet cable again.
Are the IP address settings for the CIP Safety module and the personal computer to be connected correct?	Set the IP addresses so that they have the same class and subnet address.
Has "CIP Safety Configuration Tool" been allowed in the firewall settings?	Check the firewall settings and allow "CIP Safety Configuration Tool".

Communications with EtherNet/IP devices cannot be performed

The following table lists the actions to be taken if communications with EtherNet/IP devices cannot be performed.

Check item	Action
Is the Ethernet cable connected correctly?	Connect the Ethernet cable again.
Is the EtherNet/IP device compatible with the CIP Safety module communication functions (Class1 communications and UCMM communications)?	Check the specifications of the EtherNet/IP device.
Is the power supply of the EtherNet/IP device on?	Turn on the power supply of the EtherNet/IP device.
Has an error occurred on the EtherNet/IP device, switching hub, or a similar device?	If an error has occurred on the EtherNet/IP device, switching hub, or a similar device, check the manual of each device.
Has the initial processing completed successfully?	Check whether communication is starting after 'Module READY' (X0) turns on.
Are 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) on.	Check if 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are on, and if they are on, eliminate the cause and start communication after 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) turn on.
Has EtherNet/IP communication started?	Check if 0001H (Communication start) is set to 'EtherNet/IP Communication Start Request' (Un\G98048, Un\G1146624). If not, set the value and start EtherNet/IP communications.
Has a timeout error occurred on the connection that performs communications normally?	Depending on the external device used, the connection that performs communications normally may be disconnected and a timeout error may occur after the time specified by Encapsulation Inactivity Timeout has elapsed. In that case, set the Encapsulation Inactivity Timeout setting to Disable (0H).

Class1 communication cannot be performed

The following table lists the actions to be taken if Class1 communication cannot be performed.

Check item	Action
Has the EtherNet/IP device to be connected been registered in CIP Safety Configuration Tool?	If the EtherNet/IP device to be connected is not displayed in the network configuration setting of CIP Safety Configuration Tool, add the device.
Is the corresponding connection a reservation station?	Check the parameters and see if the corresponding connection is a reserved station.
When the target is the CIP Safety module, has the multicast communication been performed with other originators?	<ul style="list-style-type: none"> Match the settings of the CIP Safety module (originator) with those of other originators that are being communicated with. Check the settings of other originators that are being communicated with the external device. Configure the system so that the external device performs communications only with the CIP Safety module (originator).
When the target is the CIP Safety module, is the number of connection consumed 64?	Check 'Number of connection consumed' (Un\G1777843, Un\G1777844) and revise the system configuration so that the number of used connections is less than 64.
Is the input data stored in the 'Class1 Input Area' (Un\G24576 to Un\G57343, Un\G1073152 to Un\G1105919)?	<ul style="list-style-type: none"> Check that the send data is set in the send area of the external device, and if not, set the data in the send area. For details, refer to the manual of each device. Check that the auto refresh setting is correct. (Page 38 Refresh)
Is the output data set in 'Class1 Output Area' (Un\G61440 to Un\G94207, Un\G1110016 to Un\G1142783)?	If auto refresh is used, check that the auto refresh setting is correct. Also, check that data is set for the set auto refresh device. (Page 38 Refresh)
Is an external device the NX-EIC202 manufactured by OMRON Corporation?	Set "Check Type" to "Compatible" in CIP Safety Configuration Tool. (Configuration view ⇒ Select communication destination device (target device) in "Network □: EIP/CIPS Scanner" ⇒ [Standard Settings] tab ⇒ [Keying] tab)

Class1 instance communications cannot be performed

The following table lists the actions to be taken if Class1 instance communications cannot be performed.

Check item	Action
Is the instance ID specified correctly?	Referring to the manual of the EtherNet/IP device connected, check the parameters of the CIP Safety module (originator) to see that the specified instance ID is available for receiving request. When the specified instance ID is not available for receiving request, change the instance ID and write the parameter again.

Class1 tag communications cannot be performed

The following table lists the actions to be taken if Class1 tag communications cannot be performed.

Check item	Action
Is the tag name specified correctly?	Check that the tag name of the external device on the CIP Safety module (originator) matches the tag name on the external device (target). If they are not matched, check the tag name and write the parameter again.

UCMM communications (message communications) cannot be performed

The following table lists the actions to be taken if UCMM communications (message communications) cannot be performed.

CIP Safety module type	Check item	Action
Client	Are the requested commands supported by the EtherNet/IP device (server)?	Check whether the supported commands being sent in the manual of the EtherNet/IP device (server).
Client	Are the settings of the commands to request correct?	Check the value set in the request area in 'UCMM data link (No.1 to No.32) area' (Un\G153600 to Un\G219135, Un\G1202176 to Un\G1267711).
Client	Is the response result correct?	Check the Result storage area stored in the response area in 'UCMM data link (No.1 to No.32) area' (Un\G153600 to Un\G219135, Un\G1202176 to Un\G1267711) and take the corrective action for the stored codes.
Client	Is 'UCMM data link execution completion (No.1 to No.32)' (Un\G151584 to Un\G151585, Un\G1200160 to Un\G1200161) on?	After 'UCMM data link execution request (No.1 to No.32)' (Un\G151552 to Un\G151553, Un\G1200128 to Un\G1200129) is turned on, if 'UCMM data link execution completion (No.1 to No.32)' (Un\G151584 to Un\G151585, Un\G1200160 to Un\G1200161) is not turned on within 3 minutes, turn off and on 'UCMM data link execution request (No.1 to No.32)' (Un\G151552 to Un\G151553, Un\G1200128 to Un\G1200129) again.
Client	Does the number of simultaneous executions per port exceed 16?	Reduce the number of client functions to be executed simultaneously.
Server	Are the settings of the commands to be requested from the EtherNet/IP device (client) correct?	Check the value of the command content to be requested by the EtherNet/IP device (client).
Server	Is the response result of the EtherNet/IP device (client) correct?	Check the response result of the EtherNet/IP device (client).



Communications cannot be properly performed using the DLR function

The following table lists the actions to be taken if communications cannot be properly performed using the DLR function.

Check item	Action
Is the IP address for the active ring supervisor set to 0?	No ring supervisor exists in the ring configuration. Review the setting of each device and set one or more ring supervisors. For CIP Safety module, check if the ring supervisor is set to be enabled in CIP Safety Configuration Tool. If not, set it and write the parameters again.
Is the line stable enough?	For each ring node, refer to the manual of each configuration device to check the following: <ul style="list-style-type: none"> • The number of ring nodes is less than 50. • The module is DLR-compliant. • The module is 100Mbps-compliant. • The communication method is full-duplex.
Is the DLR network status normal?	In CIP Safety Configuration Tool, check that the network status in the [DLR] tab and take an action according to the stored value. If "Rapid Fault/Restore Cycle" is stored, use the [Clear Rapid Fault] button in the window or instance service 4Ch (Clear_Rapid_Faults) for the Device Level Ring (DLR) object to perform clear operation.
Is the value of ring supervisor priority appropriate?	If the active ring supervisor has been changed to a backup ring supervisor without any failure, check the ring supervisor priority and change the priority as needed.

Safety communications cannot be performed


The following table lists the actions to be taken if safety communications cannot be performed.



Check item	Action
Is the connection with the external device set using CIP Safety Configuration Tool?	Use CIP Safety Configuration Tool to set the connection with the external device and write the parameters again.
Is the safety station interlock status interlocked?	Use the safety station interlock release request for each safety connection to release the interlock status. For details on the safety station interlock status, refer to the following.  Page 231 List of Safety Special Register Areas
Is a device that does not support CIP Safety set as the external device with CIP Safety Configuration Tool?	Set a device that supports CIP Safety in the connection settings of CIP Safety Configuration Tool, and write the parameters again.
Are the safety data transfer device settings for CIP Safety Configuration Tool correct?	Use CIP Safety Configuration Tool to revise the safety data transfer device settings, and write the parameters again.
Is the port used for communication with the external device and one that was set with CIP Safety Configuration Tool correct?	Revise the port settings used by CIP Safety Configuration Tool, and write the parameters again.
Are the originator and target settings set with CIP Safety Configuration Tool correct?	If the external device is the target, set the CIP Safety Configuration Tool settings to the originator. If the external device is the originator, set the CIP Safety Configuration Tool settings to the target and write the parameters again.
Are the target Device Name, Connection Name/Tag Name, and DataSize correctly set in CIP Safety Configuration Tool?	Use CIP Safety Configuration Tool to select the EDS file that matches the external device, review the settings for the target Device Name, Connection Name/Tag Name, and Data Size, and write the parameters again.
Is the target IP Address, SNN, RPI, Timeout Multiplier, and Safety Signature set according to the external device in CIP Safety Configuration Tool?	Use CIP Safety Configuration Tool to set the target IP Address, SNN, RPI, Timeout Multiplier, and Safety Signature according to the external device, and write the parameters again.
Is Connection Name set for the external device correct?	If the CIP Safety module is the target, set Connection Name set in CIP Safety Configuration Tool to the external device.
Does the number of external devices for safety communications exceed 15 in one producer (target) setting?	For the producer (target) setting of one CIP Safety module, the maximum number of external devices that can perform safety communications by multicast is 15. Therefore, if it exceeds 15, reduce the number of external devices.
Does the producer (target) connection exceed the maximum number of connections?	When the external device communicates with the producer (target) connection by multicast, one connection is used for each external device. Check the maximum number of connections that can be used for safety communications as a producer in the CIP Safety module. If exceeded, reduce the number of external devices. For the maximum number of connections, refer to the following.  Page 23 Performance Specifications
If the safety connection set in the CIP Safety module satisfies all the conditions below even when any error codes (1A40H to 1A80H) of the safety communications do not occur in the self-diagnostics code of the CPU module, take the action. <ul style="list-style-type: none"> No safety connection with the normal safety communications exists in the safety refresh communication status for each safety connection. No safety connection during an interlock exists in the safety station interlock status for each safety connection. No normal safety connection exists in the safety connection status in the safety device. 	Reset the CPU module and restart it.

11.5 List of Error Codes

This section lists the error codes, error details and causes, and actions for the errors that occur in the processing for data communications between the CIP Safety module and EtherNet/IP devices or that are caused by processing requests from the CPU module on the own station.

Error codes when a module error occurs

Error codes when a module error occurs are classified into major error, moderate error, and minor error, and can be checked in the [Error Information] tab of the "Module Diagnostics" window of the CIP Safety module. ( Page 205 Error information)

Error code	Error details and causes	Action	Detailed information
1080H	The number of writes to ROM exceeded 100000. (Number of writes > 100000)	Replace the module.	Frequency information • Frequency (setting value)
1A40H	Error information has been received from a safety communication destination station.	<ul style="list-style-type: none"> • Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. • For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For safety communications using the CIP Safety module, execute the system monitor and check the details of the error that has occurred in the CIP Safety module. • For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. ( MELSEC iQ-R CPU Module User's Manual (Application)) 	■System configuration information <ul style="list-style-type: none"> • (I/O No.) • (Base No.) • (Slot No.) • (CPU No.) • Network No. • Station No. ■Error information of other stations CC-Link IE TSN/ (CC-Link IE Field) <ul style="list-style-type: none"> • Error classification • Error code • Date (yyyymmdd) • Time (hhmmss) • Day of the week • Detailed error information
1A50H	<ul style="list-style-type: none"> • The safety approval codes written to the CPU module and to the safety communication destination station do not match. • The parameters written to the CPU module and to the safety communication destination station do not match. 	<ul style="list-style-type: none"> • Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. • For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For safety communications using the CIP Safety module, check the safety communication setting method and setting procedure, and write the parameters for the CPU module and the CIP Safety module. If the same error code is displayed again, the possible cause is a hardware failure of the data memory in the CPU module or the CIP Safety module. Please consult your local Mitsubishi representative. • For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. ( MELSEC iQ-R CPU Module User's Manual (Application)) 	System configuration information <ul style="list-style-type: none"> • (I/O No.) • (Base No.) • (Slot No.) • (CPU No.) • Network No. • Station No.

Error code	Error details and causes	Action	Detailed information
1A51H	The device actually connected to perform safety communications and the device set in the network configuration settings do not match.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For safety communications using the CIP Safety module, write the parameters to the CIP Safety module and the CPU module. If the same error code is displayed again, the possible cause is a hardware failure of the data memory in the CPU module or the CIP Safety module. Please consult your local Mitsubishi representative. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.
1A52H	The version of the device actually connected to perform safety communications and the version of the device set in the network configuration settings do not match.		
1A60H to 1A62H	A timeout error occurred during safety communications.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) Check that no online operation is being performed from a peripheral such as the engineering tool for the CPU module or CIP Safety module. Check the system configuration and parameters. (Page 28 SYSTEM CONFIGURATION, Page 36 PARAMETER SETTINGS) Check the details of the error that has occurred in the CIP Safety module. Take measures to reduce noise as the possible cause is malfunction due to bus noise. The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative. 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.
1A63H	A timeout error occurred during safety communications.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) When communicating with the CIP Safety module, execute the system monitor for the station and check the details of the error. Take measures to reduce noise as the possible cause is malfunction due to bus noise. Check that no online operation is being performed from a peripheral such as the engineering tool for the CPU module or CIP Safety module. Check the system configuration. (Page 28 SYSTEM CONFIGURATION) The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative. 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.

Error code	Error details and causes	Action	Detailed information
1A64H	A timeout error occurred during safety communications.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) Check that no online operation is being performed from a peripheral such as the engineering tool for the CPU module or CIP Safety module. Check the system configuration and parameters. (Page 28 SYSTEM CONFIGURATION, Page 36 PARAMETER SETTINGS) Check the details of the error that has occurred in the CIP Safety module. Take measures to reduce noise as the possible cause is malfunction due to bus noise. The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative. 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.
1A65H	A timeout error occurred during safety communications.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) When communicating with the CIP Safety module, execute the system monitor for the station and check the details of the error. Take measures to reduce noise as the possible cause is malfunction due to bus noise. Check that no online operation is being performed from a peripheral such as the engineering tool for the CPU module or CIP Safety module. Check the system configuration. (Page 28 SYSTEM CONFIGURATION) The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative. 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.

Error code	Error details and causes	Action	Detailed information
1A66H	A timeout error occurred during safety communications.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) Check that no online operation is being performed from a peripheral such as the engineering tool for the CPU module or CIP Safety module. Check the system configuration and parameters. (Page 28 SYSTEM CONFIGURATION, Page 36 PARAMETER SETTINGS) Check the details of the error that has occurred in the CIP Safety module. Take measures to reduce noise as the possible cause is malfunction due to bus noise. The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative. 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.
1A70H	The received data is abnormal.	<ul style="list-style-type: none"> Check the detailed information (system configuration information) of the error by executing module diagnostics using the engineering tool and check the displayed station number. For safety communications using the CIP Safety module, the network number and station number are displayed as FFFFH. Execute the system monitor and check the details of the error of the CIP Safety module. The possible cause is a hardware failure of the CIP Safety module. Please consult your local Mitsubishi representative. For communication types other than that of safety communications using the CIP Safety module, take actions as indicated in the manual for the CPU module. (MELSEC iQ-R CPU Module User's Manual (Application)) 	System configuration information <ul style="list-style-type: none"> (I/O No.) (Base No.) (Slot No.) (CPU No.) Network No. Station No.
1A71H			
1A72H			
1A73H			
1F00H	An error was detected in safety communications by the safety CPU.	<ul style="list-style-type: none"> Check and correct the safety communication setting. After that, write the parameters to the CIP Safety module and CPU module again. Then, reset the CPU module and restart it. If the parameter settings are normal, the possible cause is the effect of bus noise or a hardware failure. If the same error occurs again even after taking measures to reduce noise, the possible cause is a module failure. Please consult your local Mitsubishi representative. 	—
1F01H	A timeout error occurred during safety communications.	<ul style="list-style-type: none"> Check and correct the safety communication setting. After that, write the parameters to the CIP Safety module and CPU module again. Then, reset the CPU module and restart it. If the safety communication settings are normal, the possible cause is the effect of bus noise or a hardware failure. If the same error occurs again even after taking measures to reduce noise, the possible cause is a module failure. Please consult your local Mitsubishi representative. 	—
1F02H			
1F03H			
1F04H			

Error code	Error details and causes	Action	Detailed information
1F05H	The received data is abnormal.	<ul style="list-style-type: none"> Check and correct the safety communication setting. After that, write the parameters to the CIP Safety module and CPU module again. Then, reset the CPU module and restart it. If the safety communication settings are normal, the possible cause is the effect of bus noise or a hardware failure. If the same error occurs again even after taking measures to reduce noise, the possible cause is a module failure. Please consult your local Mitsubishi representative. 	—
1F06H			
2160H	Overlapping IP addresses have been detected.	Take one of the following actions so that the IP address is unique in the network. <ul style="list-style-type: none"> Change the IP address of the port. Change the IP address of the external device. Change the network wiring. After performing the above, write the parameters again. Then, reset the CPU module and restart it.	Cause port <ul style="list-style-type: none"> Network system number IP address
2264H	An inconsistency was detected between the parameters set in the engineering tool and the parameters set in CIP Safety Configuration Tool.	<ul style="list-style-type: none"> There is an inconsistency between the parameters set in the engineering tool and the parameters set in CIP Safety Configuration Tool. Write each parameter again. Correct and match between the parameters set in the engineering tool and the parameters set in CIP Safety Configuration Tool. 	—
3100H	A parameter error was detected.	<ul style="list-style-type: none"> Use the engineering tool to write the parameters to the CPU module again. If the error occurs again even after the above action is taken, the possible cause is a hardware failure of the module on which the error occurred. Please consult your local Mitsubishi representative. 	—
3110H	The parameters of this module are not set in the CPU.	<ul style="list-style-type: none"> Set the parameters for the CPU module. Check the mounting position of the module. 	System configuration information 2 <ul style="list-style-type: none"> I/O number
3120H	<ul style="list-style-type: none"> The safety module parameters set in the engineering tool are set, but the safety communication parameters are not set in CIP Safety Configuration Tool. The safety module parameters set in the engineering tool are not set, but the safety communication parameters are set in CIP Safety Configuration Tool. 	Take actions so that the safety module parameters set in the engineering tool and the safety communication parameters set in CIP Safety Configuration Tool match. Take action and rewrite each parameter.	—
3A30H	Standard communications/safety communications stopped due to module initialization.	After the module initialization is complete, restart the system.	—
3C00H	A hardware failure has been detected.	<ul style="list-style-type: none"> Take measures to reduce noise. Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative. 	—
3C01H			
3C02H			
3C03H			
3C0FH			
3C22H	An error was detected in the memory.	<ul style="list-style-type: none"> Take measures to reduce noise. Format the memory. After that, write all the files, reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative. 	—
3C2FH		<ul style="list-style-type: none"> Take measures to reduce noise. Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative. 	
3E16H	A hardware failure has been detected.	<ul style="list-style-type: none"> Take measures to reduce noise. Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative. 	—
3E17H			

Error codes when a communication error occurs

When the connection is abnormal

Error codes for connection errors can be checked with 'CIP Safety own station connection error status'. ( Page 241 CIP Safety own station connection error status)

This section describes how to store the error codes.

Buffer memory address ^{*1}		Connection destination	Storage method
P1: Un\G16928 P2: Un\G1065504	P1: Un\G16929 P2: Un\G1065505	Input Connection No. 1 Connection No. 2 : Connection No. 119 Connection No. 120	<div> <div>8 bits</div> <div>8 bits</div> <div>16 bits</div> </div> <div> <div>When used as the target</div> <div>(1) StatusIn (3) CIP Status^{*2} (4) CIP Extended^{*3}</div> </div> <div> <div>When used as the originator</div> <div>(1) StatusIn (5) CIP Status^{*2} (6) CIP Extended^{*3}</div> </div>
P1: Un\G16930 P2: Un\G1065506	P1: Un\G16931 P2: Un\G1065507		
:	:		
P1: Un\G17164 P2: Un\G1065740	P1: Un\G17165 P2: Un\G1065741		
P1: Un\G17166 P2: Un\G1065742	P1: Un\G17167 P2: Un\G1065743		
P1: Un\G17168 P2: Un\G1065744	P1: Un\G17169 P2: Un\G1065745	Output Connection No. 1 Connection No. 2 : Connection No. 119 Connection No. 120	<div> <div>8 bits</div> <div>8 bits</div> <div>16 bits</div> </div> <div> <div>When used as the target</div> <div>(2) StatusOut (3) CIP Status (4) CIP Extended</div> </div> <div> <div>When used as the originator</div> <div>(2) StatusOut (5) CIP Status (6) CIP Extended</div> </div>
P1: Un\G17170 P2: Un\G1065746	P1: Un\G17171 P2: Un\G1065747		
:	:		
P1: Un\G17404 P2: Un\G1065980	P1: Un\G17405 P2: Un\G1065981		
P1: Un\G17406 P2: Un\G1065982	P1: Un\G17407 P2: Un\G1065983		

*1 Error codes are stored in 32 bits.

*2 When StatusIn is 41H, the General Status Code received from the external device is stored.

*3 When StatusIn is 41H, the Extended Status Code received from the external device is stored.

Buffer memory storage value			Error details and causes	Action
Stored value (1) or (2)	Stored value (3) or (5)	Stored value (4) or (6)		
0H	Other than 0H	—	A connection error has occurred.	<ul style="list-style-type: none"> Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. When safety communications are performed, check whether the SAFETY COM ERR LED is on. When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. Check that the IP address of the external device is correct. Check whether the operating status of the external device is normal. Check that the correct port is used for communications with the external device. Check for errors in the line status. The line may be busy, so retry at a later time. The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. Take measures to reduce noise. Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
20H	—	—	An error was detected in the memory.	<ul style="list-style-type: none"> Take measures to reduce noise. Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.

Buffer memory storage value			Error details and causes	Action
Stored value (1) or (2)	Stored value (3) or (5)	Stored value (4) or (6)		
21H	—	—	A timeout error has occurred.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
34H	—	—	An error was detected in the memory.	<ul style="list-style-type: none"> • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
35H	—	—	The connection is in the IDLE status.	<ul style="list-style-type: none"> • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device.
36H	—	—	The connections have been disconnected.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.

Buffer memory storage value			Error details and causes	Action
Stored value (1) or (2)	Stored value (3) or (5)	Stored value (4) or (6)		
3AH	—	—	An error has occurred in TCP communications.	<ul style="list-style-type: none"> • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
41H	01H	—	An error notification has been received from the external device.	<ul style="list-style-type: none"> • Perform diagnostics using CIP Safety Configuration Tool to check whether a connection error has occurred. • Refer to documentation such as the manuals of the external device and CIP specifications to check the causes of which a notification is made for this error and the action to take.
	FBH	—	A timeout error has occurred.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check that the value of 'Number of connection consumed' (UnG1777843, UnG1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
	Except for shown above	—	An error notification has been received from the external device.	Refer to documentation such as the manuals of the external device and CIP specifications to check the causes of which a notification is made for this error and the action to take.
42H	—	—	The available resources are insufficient.	<ul style="list-style-type: none"> • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.

Buffer memory storage value			Error details and causes	Action
Stored value (1) or (2)	Stored value (3) or (5)	Stored value (4) or (6)		
44H	—	—	A timeout error has occurred.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
45H	—	—	An error has occurred when setting up a connection.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check if 0001H (Communication start) is set to 'EtherNet/IP Communication Start Request' (Un\G98048, Un\G1146624). • Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
46H	—	—	An error has occurred in EtherNet/IP communications.	<ul style="list-style-type: none"> • Check whether the operating status of the external device is normal. • Check for errors in the line status. • The line may be busy, so retry at a later time.
4DH	—	—	Communications have been disconnected.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check for errors in the line status.

Buffer memory storage value			Error details and causes	Action
Stored value (1) or (2)	Stored value (3) or (5)	Stored value (4) or (6)		
E0H	—	—	A connection error has occurred.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
FFH	—	—	The connections have been disconnected.	<ul style="list-style-type: none"> • Check whether 'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) are on. • Check that 'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) are not on. • Check that the value of 'Number of connection consumed' (Un\G1777843, Un\G1777844) is less than the maximum number of connections. • When safety communications are performed, check whether the SAFETY COM ERR LED is on. • When UCMM communications are performed, check whether the setting details of the UCMM request area are correct. • Check that the IP address of the external device is correct. • Check whether the operating status of the external device is normal. • Check that the correct port is used for communications with the external device. • Check for errors in the line status. • The line may be busy, so retry at a later time. • The external device may not be able to transmit data at the specified RPI due to a high communication load, so specify a larger RPI and connect again. • Take measures to reduce noise. • Reset the CPU module and restart it. If the same error code is displayed again, the possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.

11.6 Event List

This section lists the events that occur in the CIP Safety module.

There are two types of events: system and operation.

System

Event code	Overview	Cause
00100	Link-up	The CPU module has entered into the link-up state as a result of an operation such as connecting a network cable between the CPU module and an external device.
00400	Communication stop	EtherNet/IP communications (including safety communications) have stopped.
00401	Communication start	EtherNet/IP communications (including safety communication) have started.
00440	Selected as an active ring supervisor	The system itself is selected as an active ring supervisor. ^{*1}
00441	Selected as a backup ring supervisor	The system itself is selected as a backup ring supervisor. ^{*1}
00442	Ring fault clear	The ring fault was cleared when the ring was connected. ^{*1}
00800	Link-down	The CPU module has entered into the link-down state as a result of an operation such as disconnecting a network cable between the CPU module and an external device.

^{*1} This event can be registered twice.

Operation

Event code	Overview	Cause
24000	Module initialization completed successfully.	Module initialization completed successfully.
24001	Module initialization completed with an error.	Module initialization failed.

APPENDICES

Appendix 1 Module Label

Module labels can be used to set the I/O signals and buffer memory of the CIP Safety module.

Module label structure

Module label names are defined with the following structure.

"instance name"_"module number"."label name"

"instance name"_"module number"."label name"_D

Ex.

RJ71SEIP91_1. bSts_ModuleReady

■Instance name

The instance name of the CIP Safety module is as shown below.

Module name	Instance name
RJ71SEIP91	RJ71SEIP91

■Module number

Module numbers start from 1 and are added to identify modules that have the same instance name.

■Label name

A label name unique to the module.

■_D

This symbol indicates that the module label is for direct access. If this symbol is not present, the label is for refreshing.

Refreshing and direct access differ as shown below.

Type	Description	Access timing
Refresh	The values written to and read from the module label are reflected on the module as a batch during refreshing. This function makes it possible to reduce the program execution time.	Refreshing
Direct access	The values written to and read from the module label are immediately reflected on the module. The program execution time is longer than the refresh time, but the responsiveness increases.	Writing to/reading from module labels

A

Appendix 2 I/O Signals

This section describes the I/O signals transmitted to or received from the CPU module. The I/O signal assignment for when the start I/O number of the CIP Safety module is "0" is listed below.

List of I/O signals

The following tables list I/O signals. Device X input signals are input signals from the CIP Safety module to the CPU module. Device Y output signals are output signals from the CPU module to the CIP Safety module.

Input signals

Device No.	Signal name
X0	Module READY
X1	Port start status (P1)
X2	Port stop error status (P1)
X3 to X10	Use prohibited
X11	Port start status (P2)
X12	Port stop error status (P2)
X13 to X1F	Use prohibited

Output signals

Device No.	Signal name
Y0 to Y1F	Use prohibited



Do not use (turn on) any "use prohibited" signals as an input or output signal to the CPU module. Doing so may cause malfunction of the programmable controller system.

Details of input signals

Module READY (X0)

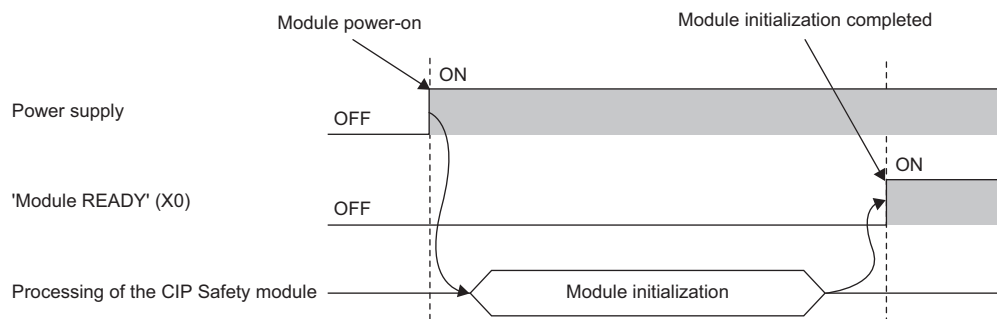
This input signal notifies that the CIP Safety module can be operated (access to I/O signals and buffer memory is possible).

Status of 'Module READY' (X0)	Operations for the CIP Safety module (○: Yes, ×: No)				
	Input signal		Output signals	Buffer memory ^{*1}	
	Read 'Module READY' (X0)	Read an input signal other than 'Module READY' (X0)	Write	Read	Write
Off	○	×	×	×	×
On	○	○	○	○	○

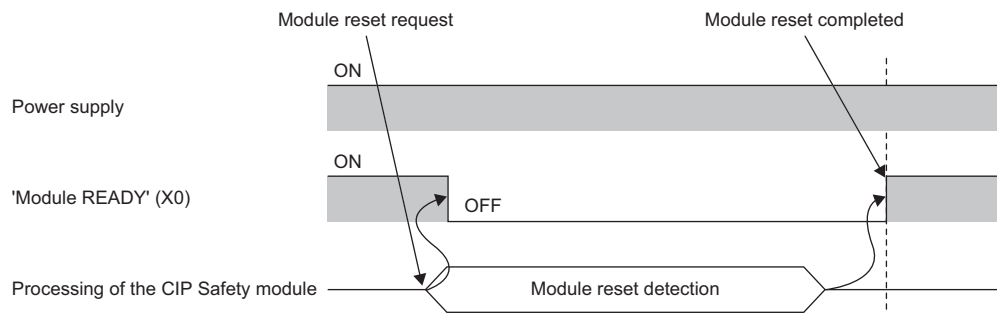
*1 If the refresh setting is enabled, the labels and devices of the refresh target are also refreshed.

After the CPU module is powered off and on or is reset, this signal turns on at the completion of the preparation for the CIP Safety module.

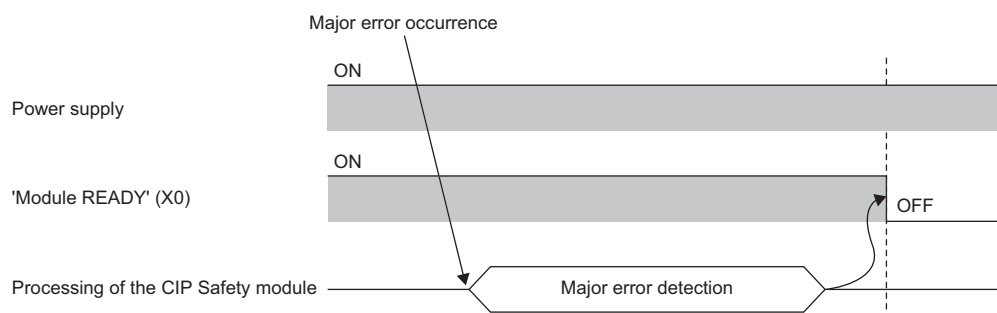
■At power-on



■When the module is reset



■When a major error has occurred



Port start status (P1) (X1), port start status (P2) (X11)

'Port start status (P1)' (X1) and 'Port start status (P2)' (X11) notify the start status of each port (P1/P2) of the CIP Safety module.

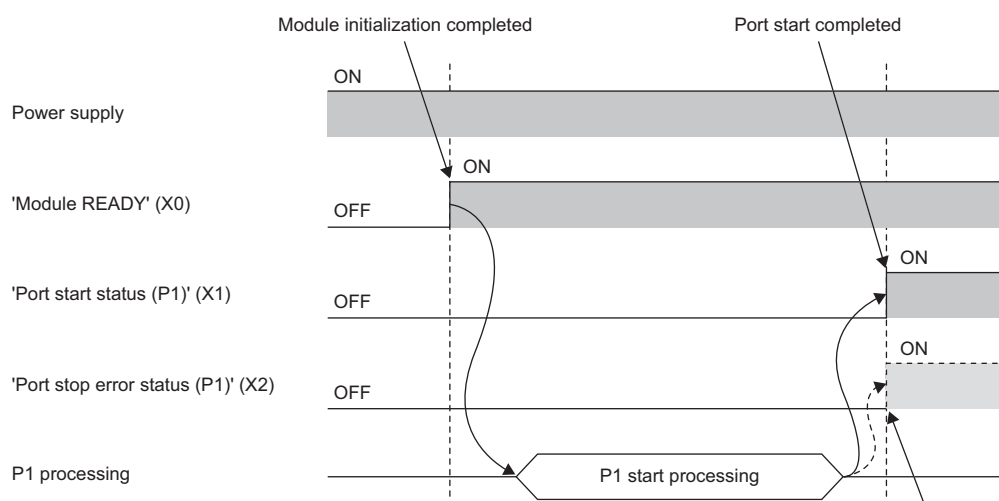
By combining with 'Module READY' (X0), communication availability can be checked for each port. The following table shows the signal combinations and port communication availability. (The operation is the same on P2.)

Signal status			Port status	
'Module READY' (X0)	'Port start status (P1)' (X1)	'Port stop error status (P1)' (X2)	Communication availability	Description
Off	—	—	No	Communication is not possible because the port is stopped.
On	Off	—	Yes	Communication is possible.
	On	Off		
		On	No	An error has occurred in the port and communication is not possible.

The following table shows the conditions for turning each signal on/off. (The operation is the same on P2.)

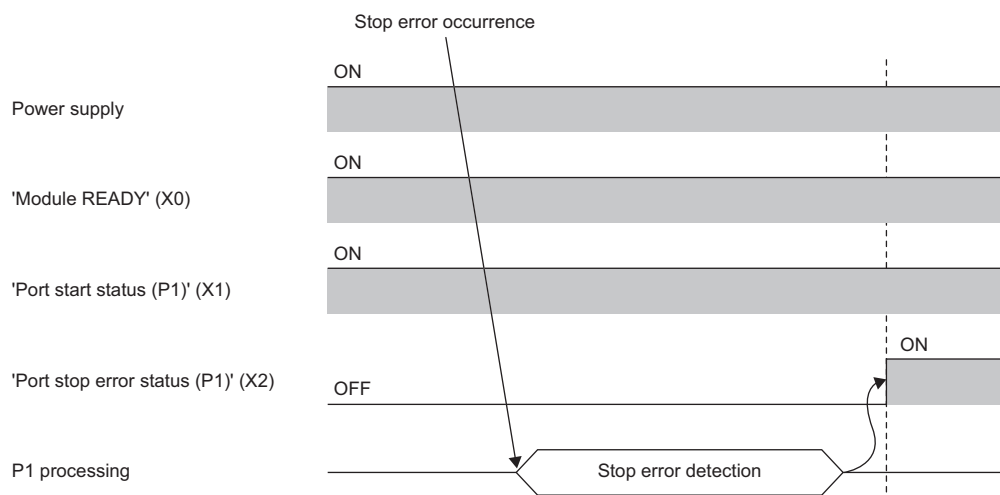
Signal	Signal operation	Condition	Description
'Port start status (P1)' (X1)	Off → On	The port has started up.	At power-on, at reset clear (Page 226 At power-on, at reset clear)
	On → Off	The port has stopped.	When the module is reset (Page 227 When the module is reset)
'Port stop error status (P1)' (X2)	Off → On	A stop error has occurred on the port.	<ul style="list-style-type: none"> At power-on, at reset clear (Page 226 At power-on, at reset clear) At the occurrence of a stop error after the port is started (Page 227 At the occurrence of a stop error after the port is started)
	On → Off	The port has stopped.	When the module is reset (Page 227 When the module is reset)

■At power-on, at reset clear

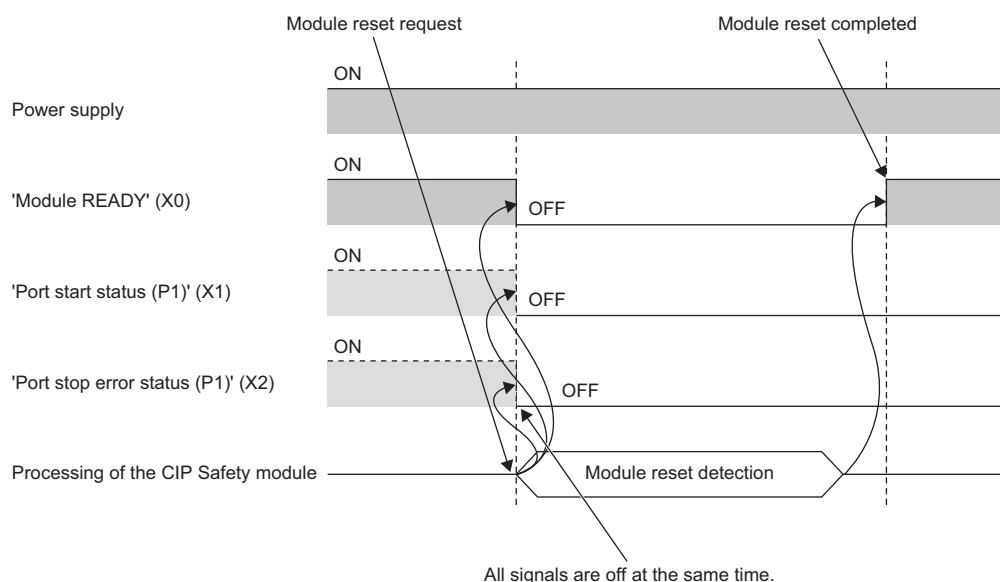


'Port stop error status (P1)' (X2) is on simultaneously when an error occurs.

■At the occurrence of a stop error after the port is started



■When the module is reset



Port stop error status (P1) (X2), Port stop error status (P2) (X12)

'Port stop error status (P1)' (X2) and 'Port stop error status (P2)' (X12) notify the stop error occurrence status of each port of the CIP Safety module.

For details, refer to the following.

📖 Page 226 Port start status (P1) (X1), port start status (P2) (X11)

Appendix 3 List of Special Relay Areas

The following table lists items in the list.

Item	Description
No.	Special relay number
Name	Special relay name
Description	Data stored in the special relay and its meaning
Details	Detailed description of the data stored

Point

When counting the number of modules mounted on the base unit, the following modules are included: CIP Safety modules that use safety communications, CC-Link IE TSN master/local modules, Motion modules, and CC-Link IE Field Network-equipped master/local modules.

Also, the type of safety communications consists of the following: safety communications using CC-Link IE TSN, safety communications using CC-Link IE Field Network, and safety communications using CIP Safety.

Safety information

The following is a list of special relay areas relating to safety information.

No.	Name	Description	Details
SM1904	Safety communication setting (1st module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1904.
SM1905	Safety communication setting (2nd module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1905.
SM1906	Safety communication setting (3rd module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1906.
SM1907	Safety communication setting (4th module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1907.
SM1908	Safety communication setting (5th module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1908.
SM1909	Safety communication setting (6th module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1909.
SM1910	Safety communication setting (7th module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1910.
SM1911	Safety communication setting (8th module)	Off: Not set On: Set	<ul style="list-style-type: none">This relay stores the safety communication setting status.When safety communications are available (the relay is on), the start I/O number of the target module is stored in SD1911.

Appendix 4 List of Special Register Areas

The following table lists items in the list.

Item	Description
No.	Special register number
Name	Special register name
Description	Data stored in the special register
Details	Detailed description of the data stored



When counting the number of modules mounted on the base unit, the following modules are included: CIP Safety modules that use safety communications, CC-Link IE TSN master/local modules, Motion modules, and CC-Link IE Field Network-equipped master/local modules.

Also, the type of safety communications consists of the following: safety communications using CC-Link IE TSN, safety communications using CC-Link IE Field Network, and safety communications using CIP Safety.

Safety information

The following is the list of special register areas relating to the safety information.

No.	Name	Description	Details
SD1904	Start I/O number of Safety communication target station (1st module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1905	Start I/O number of Safety communication target station (2nd module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1906	Start I/O number of Safety communication target station (3rd module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1907	Start I/O number of Safety communication target station (4th module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1908	Start I/O number of Safety communication target station (5th module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1909	Start I/O number of Safety communication target station (6th module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1910	Start I/O number of Safety communication target station (7th module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.
SD1911	Start I/O number of Safety communication target station (8th module)	0 to FFH: Start I/O number FFFFH: Not set	<ul style="list-style-type: none"> The value obtained by dividing the start I/O number of the station targeted for safety communications by 16 is stored. When the safety communication function is not used, FFFFFH is stored.

A

Appendix 5 List of Safety Special Relay Areas

The following table lists items in the list.

Item	Description
No.	Safety special relay number
Name	Safety special relay name
Description	Data stored in the safety special relay and its meaning
Details	Detailed description of the data stored

Point

When counting the number of modules mounted on the base unit, the following modules are included: CIP Safety modules that use safety communications, CC-Link IE TSN master/local modules, Motion modules, and CC-Link IE Field Network-equipped master/local modules.

Also, the type of safety communications consists of the following: safety communications using CC-Link IE TSN, safety communications using CC-Link IE Field Network, and safety communications using CIP Safety.

Safety information

The following is the list of safety special relay areas relating to safety information.

No.	Name	Description	Details
SA\SM1008	Safety refresh communication status of each module (1st module)	Off: Normal On: Communication error	The safety refresh communication status of the first CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1904) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1008 to SA\SD1015.)
SA\SM1016	Safety refresh communication status of each module (2nd module)	Off: Normal On: Communication error	The safety refresh communication status of the second CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1905) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1016 to SA\SD1023.)
SA\SM1024	Safety refresh communication status of each module (3rd module)	Off: Normal On: Communication error	The safety refresh communication status of the third CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1906) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1024 to SA\SD1031.)
SA\SM1032	Safety refresh communication status of each module (4th module)	Off: Normal On: Communication error	The safety refresh communication status of the fourth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1907) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1032 to SA\SD1039.)
SA\SM1040	Safety refresh communication status of each module (5th module)	Off: Normal On: Communication error	The safety refresh communication status of the fifth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1908) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1040 to SA\SD1047.)
SA\SM1048	Safety refresh communication status of each module (6th module)	Off: Normal On: Communication error	The safety refresh communication status of the sixth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1909) is stored. (The safety refresh communication status of each safety connection is stored in SA\SDSD1048 to SA\SD1055.)
SA\SM1056	Safety refresh communication status of each module (7th module)	Off: Normal On: Communication error	The safety refresh communication status of the seventh CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1910) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1056 to SA\SD1063.)
SA\SM1064	Safety refresh communication status of each module (8th module)	Off: Normal On: Communication error	The safety refresh communication status of the eighth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1911) is stored. (The safety refresh communication status of each safety connection is stored in SA\SD1064 to SA\SD1071.)
SA\SM1088	Module switch request for safety communication information	Off: Module specification completed On: Module specification requested	The SA\SD1088 content is updated when this relay changes from off to on. This relay turns off when SA\SD1090 to 1097 and SA\SD1104 to 1223 data update is complete.

Appendix 6 List of Safety Special Register Areas

The following table lists items in the list.

Item	Description
No.	Safety special register number
Name	Safety special register name
Description	Data stored in the safety special register
Details	Detailed description of the data stored

Point

When counting the number of modules mounted on the base unit, the following modules are included: CIP Safety modules that use safety communications, CC-Link IE TSN master/local modules, Motion modules, and CC-Link IE Field Network-equipped master/local modules.

Also, the type of safety communications consists of the following: safety communications using CC-Link IE TSN, safety communications using CC-Link IE Field Network, and safety communications using CIP Safety.

Safety information

The following is the list of safety special register areas relating to safety information.

No.	Name	Description	Details
SA\SD1008 to SA\SD1015	Safety refresh communication status of each safety connection (1st module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the first CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1904) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.
SA\SD1016 to SA\SD1023	Safety refresh communication status of each safety connection (2nd module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the second CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1905) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.
SA\SD1024 to SA\SD1031	Safety refresh communication status of each safety connection (3rd module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the third CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1906) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.
SA\SD1032 to SA\SD1039	Safety refresh communication status of each safety connection (4th module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the fourth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1907) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.
SA\SD1040 to SA\SD1047	Safety refresh communication status of each safety connection (5th module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the fifth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1908) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.
SA\SD1048 to SA\SD1055	Safety refresh communication status of each safety connection (6th module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the sixth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1909) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.
SA\SD1056 to SA\SD1063	Safety refresh communication status of each safety connection (7th module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none"> The communication status of safety stations connected to the seventh CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1910) is stored. A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.

A

No.	Name	Description	Details																																																																																																																																																									
SA\SD1064 to SA\SD1071	Safety refresh communication status of each safety connection (8th module)	0: Safety communications normal, safety connection not set, own station 1: Communication error	<ul style="list-style-type: none">The communication status of safety stations connected to the eighth CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module (the one whose start I/O number is stored in SD1911) is stored.A communication error means that the safety station is not in any of the communication states stored in SA\SD1104 to SA\SD1223.																																																																																																																																																									
SA\SD1088	Module setting for safety communication information (1st to 8th module)	1 to 8: Target module	<ul style="list-style-type: none">The CIP Safety module, CC-Link IE Field Network master/local module or CC-Link IE TSN master/local module targeted for safety communication status check is specified.To reflect the value set in this register, turn on SA\SM1088.If an unmounted module is specified, 0 is stored in SA\SD1090 to SA\SD1097 and SA\SD1104 to SA\SD1223.																																																																																																																																																									
SA\SD1089	Target module for safety communication information (1st to 8th module)	1 to 8: Target module	<ul style="list-style-type: none">The module number specified in SA\SD1088 is stored.Data for the module displayed in this register is stored in SA\SD1090 to SA\SD1097 and SA\SD1104 to SA\SD1223.																																																																																																																																																									
SA\SD1090 to SA\SD1097	Safety communication setting of each safety connection (1st to 8th module)	0: Not set 1: Set	The communication setting status of safety connections of the module stored in SA\SD1089 is stored.																																																																																																																																																									
SA\SD1104 to SA\SD1223	Safety communication status of each safety connection (1st to 8th module) Safety Connection No: 1 to 120	Safety communication status of safety connection numbers 1 to 120	<ul style="list-style-type: none">The safety communication status of safety connections of the module stored in SA\SD1089 is stored.0 is stored if not used in SA\SD1104 to SA\SD1223, or if own station.																																																																																																																																																									
SA\SD1232 to SA\SD1239	Interlock status of each safety connection (1st module)	0: Not interlocked 1: Interlocked	<p>After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on.</p> <table><tr><th></th><th>b15</th><th>b14</th><th>b13</th><th>b12</th><th>b11</th><th>b10</th><th>b9</th><th>b8</th><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th></tr><tr><td>SA\SD1232</td><td>16</td><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr><tr><td>SA\SD1233</td><td>32</td><td>31</td><td>30</td><td>29</td><td>28</td><td>27</td><td>26</td><td>25</td><td>24</td><td>23</td><td>22</td><td>21</td><td>20</td><td>19</td><td>18</td><td>17</td></tr><tr><td>SA\SD1234</td><td>48</td><td>47</td><td>46</td><td>45</td><td>44</td><td>43</td><td>42</td><td>41</td><td>40</td><td>39</td><td>38</td><td>37</td><td>36</td><td>35</td><td>34</td><td>33</td></tr><tr><td>SA\SD1235</td><td>64</td><td>63</td><td>62</td><td>61</td><td>60</td><td>59</td><td>58</td><td>57</td><td>56</td><td>55</td><td>54</td><td>53</td><td>52</td><td>51</td><td>50</td><td>49</td></tr><tr><td>SA\SD1236</td><td>80</td><td>79</td><td>78</td><td>77</td><td>76</td><td>75</td><td>74</td><td>73</td><td>72</td><td>71</td><td>70</td><td>69</td><td>68</td><td>67</td><td>66</td><td>65</td></tr><tr><td>SA\SD1237</td><td>96</td><td>95</td><td>94</td><td>93</td><td>92</td><td>91</td><td>90</td><td>89</td><td>88</td><td>87</td><td>86</td><td>85</td><td>84</td><td>83</td><td>82</td><td>81</td></tr><tr><td>SA\SD1238</td><td>112</td><td>111</td><td>110</td><td>109</td><td>108</td><td>107</td><td>106</td><td>105</td><td>104</td><td>103</td><td>102</td><td>101</td><td>100</td><td>99</td><td>98</td><td>97</td></tr><tr><td>SA\SD1239</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>120</td><td>119</td><td>118</td><td>117</td><td>116</td><td>115</td><td>114</td><td>113</td></tr></table> <p>1 to 120: Safety connection number —: Fixed to 0</p>		b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0	SA\SD1232	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	SA\SD1233	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	SA\SD1234	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	SA\SD1235	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	SA\SD1236	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	SA\SD1237	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	SA\SD1238	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	SA\SD1239	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113
	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0																																																																																																																																												
SA\SD1232	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1																																																																																																																																												
SA\SD1233	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17																																																																																																																																												
SA\SD1234	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33																																																																																																																																												
SA\SD1235	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49																																																																																																																																												
SA\SD1236	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65																																																																																																																																												
SA\SD1237	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81																																																																																																																																												
SA\SD1238	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97																																																																																																																																												
SA\SD1239	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113																																																																																																																																												
SA\SD1240 to SA\SD1247	Interlock release request for each safety connection (1st module)	0: Do not release the interlock. 1: Release the interlock.	<p>Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.)</p> <table><tr><th></th><th>b15</th><th>b14</th><th>b13</th><th>b12</th><th>b11</th><th>b10</th><th>b9</th><th>b8</th><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th></tr><tr><td>SA\SD1240</td><td>16</td><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr><tr><td>SA\SD1241</td><td>32</td><td>31</td><td>30</td><td>29</td><td>28</td><td>27</td><td>26</td><td>25</td><td>24</td><td>23</td><td>22</td><td>21</td><td>20</td><td>19</td><td>18</td><td>17</td></tr><tr><td>SA\SD1242</td><td>48</td><td>47</td><td>46</td><td>45</td><td>44</td><td>43</td><td>42</td><td>41</td><td>40</td><td>39</td><td>38</td><td>37</td><td>36</td><td>35</td><td>34</td><td>33</td></tr><tr><td>SA\SD1243</td><td>64</td><td>63</td><td>62</td><td>61</td><td>60</td><td>59</td><td>58</td><td>57</td><td>56</td><td>55</td><td>54</td><td>53</td><td>52</td><td>51</td><td>50</td><td>49</td></tr><tr><td>SA\SD1244</td><td>80</td><td>79</td><td>78</td><td>77</td><td>76</td><td>75</td><td>74</td><td>73</td><td>72</td><td>71</td><td>70</td><td>69</td><td>68</td><td>67</td><td>66</td><td>65</td></tr><tr><td>SA\SD1245</td><td>96</td><td>95</td><td>94</td><td>93</td><td>92</td><td>91</td><td>90</td><td>89</td><td>88</td><td>87</td><td>86</td><td>85</td><td>84</td><td>83</td><td>82</td><td>81</td></tr><tr><td>SA\SD1246</td><td>112</td><td>111</td><td>110</td><td>109</td><td>108</td><td>107</td><td>106</td><td>105</td><td>104</td><td>103</td><td>102</td><td>101</td><td>100</td><td>99</td><td>98</td><td>97</td></tr><tr><td>SA\SD1247</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>—</td><td>120</td><td>119</td><td>118</td><td>117</td><td>116</td><td>115</td><td>114</td><td>113</td></tr></table> <p>1 to 120: Safety connection number —: Fixed to 0</p>		b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0	SA\SD1240	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	SA\SD1241	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	SA\SD1242	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	SA\SD1243	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	SA\SD1244	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	SA\SD1245	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	SA\SD1246	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	SA\SD1247	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113
	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0																																																																																																																																												
SA\SD1240	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1																																																																																																																																												
SA\SD1241	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17																																																																																																																																												
SA\SD1242	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33																																																																																																																																												
SA\SD1243	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49																																																																																																																																												
SA\SD1244	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65																																																																																																																																												
SA\SD1245	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81																																																																																																																																												
SA\SD1246	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97																																																																																																																																												
SA\SD1247	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113																																																																																																																																												
SA\SD1248 to SA\SD1255	Interlock status of each safety connection (2nd module)	0: Not interlocked 1: Interlocked	<p>After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on.</p> <p>The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)</p>																																																																																																																																																									
SA\SD1256 to SA\SD1263	Interlock release request for each safety connection (2nd module)	0: Do not release the interlock. 1: Release the interlock.	<p>Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.)</p> <p>The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)</p>																																																																																																																																																									
SA\SD1264 to SA\SD1271	Interlock status of each safety connection (3rd module)	0: Not interlocked 1: Interlocked	<p>After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on.</p> <p>The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)</p>																																																																																																																																																									

No.	Name	Description	Details
SA\SD1272 to SA\SD1279	Interlock release request for each safety connection (3rd module)	0: Do not release the interlock. 1: Release the interlock.	Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.) The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1280 to SA\SD1287	Interlock status of each safety connection (4th module)	0: Not interlocked 1: Interlocked	After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on. The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1288 to SA\SD1295	Interlock release request for each safety connection (4th module)	0: Do not release the interlock. 1: Release the interlock.	Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.) The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1296 to SA\SD1303	Interlock status of each safety connection (5th module)	0: Not interlocked 1: Interlocked	After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on. The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1304 to SA\SD1311	Interlock release request for each safety connection (5th module)	0: Do not release the interlock. 1: Release the interlock.	Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.) The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1312 to SA\SD1319	Interlock status of each safety connection (6th module)	0: Not interlocked 1: Interlocked	After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on. The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1320 to SA\SD1327	Interlock release request for each safety connection (6th module)	0: Do not release the interlock. 1: Release the interlock.	Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.) The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1328 to SA\SD1335	Interlock status of each safety connection (7th module)	0: Not interlocked 1: Interlocked	After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on. The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1336 to SA\SD1343	Interlock release request for each safety connection (7th module)	0: Do not release the interlock. 1: Release the interlock.	Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.) The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1344 to SA\SD1351	Interlock status of each safety connection (8th module)	0: Not interlocked 1: Interlocked	After safety communication error is detected and the safety connection is interlocked, the bit corresponding to the safety connection turns on. The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)
SA\SD1352 to SA\SD1359	Interlock release request for each safety connection (8th module)	0: Do not release the interlock. 1: Release the interlock.	Turn off and on the bit corresponding to the safety connection to release the interlock. (The bit does not automatically turn off after execution is complete.) The bit arrangement of the safety connection number is the same as that of the 1st module. (Note that the SA\SD numbers differ.)

Appendix 7 Buffer Memory

The buffer memory is used to exchange data between the CIP Safety module and the CPU module or EtherNet/IP devices. Buffer memory values are set to their defaults (initial values) when the CPU module is reset or the system is powered off and on.

List of buffer memory addresses

P1		P2		Name			Initial value	Read, write
Address (decimal)	Address (hexadecimal)	Address (decimal)	Address (hexadecimal)					
0 to 16436	0H to 4034H	0 to 1065012	0H to 104034H	System area				
16437 to 16439	4035H to 4037H	1065013 to 1065015	104035H to 104037H	Setting status	Own Station Ethernet Address (MAC address)		Setting value	Read
16440 to 16639	4038H to 40FFH	1065016 to 1065215	104038H to 1040FFH	System area				
16640 to 16759	4100H to 4177H	1065216 to 1065335	104100H to 104177H	CIP Safety Input Data Size			0	Read
16760 to 16767	4178H to 417FH	1065336 to 1065343	104178H to 10417FH	System area				
16768 to 16887	4180H to 41F7H	1065344 to 1065463	104180H to 1041F7H	CIP Safety Output Data Size			0	Read
16888 to 16895	41F8H to 41FFH	1065464 to 1065471	1041F8H to 1041FFH	System area				
16896 to 16903	4200H to 4207H	1065472 to 1065479	104200H to 104207H	Data link status	Input		0	Read
16904 to 16911	4208H to 420FH	1065480 to 1065487	104208H to 10420FH		Output		0	Read
16912 to 16919	4210H to 4217H	1065488 to 1065495	104210H to 104217H	Error status	Input		0	Read
16920 to 16927	4218H to 421FH	1065496 to 1065503	104218H to 10421FH		Output		0	Read
16928, 16929	4220H, 4421H	1065504, 1065505	104220H, 104221H	CIP Safety own station connection error status	Input	Connection 1	0	Read
16930 to 17167	4222H to 430FH	1065506 to 1065743	104222H to 10430FH			Connection2 to 120	0	Read
17168, 17169	4310H, 4311H	1065744, 1065745	104310H, 104311H		Output	Connection 1	0	Read
17170 to 17407	4312H to 43FFH	1065746 to 1065983	104312H to 1043FFH			Connection2 to 120	0	Read
17408 to 18431	4400H to 47FFH	1065984 to 1067007	104400H to 1047FFH	System area				
18432 to 18451	4800H to 4813H	1067008 to 1067027	104800H to 104813H	Connection information area	Input	Connection 1	0	Read
18452 to 20831	4814H to 515FH	1067028 to 1069407	104814H to 10515FH			Connection2 to 120	0	Read
20832 to 20851	5160H to 5173H	1069408 to 1069427	105160H to 105173H		Output	Connection 1	0	Read
20852 to 23231	5174H to 5ABFH	1069428 to 1071807	105174H to 105ABFH			Connection2 to 120	0	Read
23232 to 24575	5AC0H to 5FFFH	1071808 to 1073151	105AC0H to 105FFFH	System area				
24576 to 57343	6000H to DFFFH	1073152 to 1105919	106000H to 10DFFFH	Class1 Input Area			0	Read
57344 to 61439	E000H to EFFFH	1105920 to 1110015	10E000H to 10EFFFH	System area				
61440 to 94207	F000H to 16FFFH	1110016 to 1142783	10F000H to 116FFFH	Class1 Output Area			0	Read, write
94208 to 98047	17000H to 17EFFH	1142784 to 1146623	117000H to 117EFFH	System area				

P1		P2		Name			Initial value	Read, write	
Address (decimal)	Address (hexadecimal)	Address (decimal)	Address (hexadecimal)						
98048	17F00H	1146624	117F00H	EtherNet/IP communication start request			0	Read, write	
98049 to 98303	17F01H to 17FFFH	1146625 to 1146879	117F01H to 117FFFH	System area					
98304 to 98431	18000H to 1807FH	1146880 to 1147007	118000H to 11807FH	Class1 Input data size			0	Read	
98432 to 98559	18080H to 180FFH	1147008 to 1147135	118080H to 1180FFH	System area					
98560 to 98687	18100H to 1817FH	1147136 to 1147263	118100H to 11817FH	Class1 Output data size			0	Read	
98688 to 98815	18180H to 181FFH	1147264 to 1147391	118180H to 1181FFH	System area					
98816 to 98943	18200H to 1827FH	1147392 to 1147519	118200H to 11827FH	Class1 Start offset address to the input data			FFFFH	Read	
98944 to 99071	18280H to 182FFH	1147520 to 1147647	118280H to 1182FFH	System area					
99072 to 99199	18300H to 1837FH	1147648 to 1147775	118300H to 11837FH	Class1 Start offset address to the output data			FFFFH	Read	
99200 to 99407	18380H to 1844FH	1147776 to 1147983	118380H to 11844FH	System area					
99408 to 99415	18450H to 18457H	1147984 to 1147991	118450H to 118457H	Class1 communication status	Data link status (Class1)		0	Read	
99416 to 99423	18458H to 1845FH	1147992 to 1147999	118458H to 11845FH		System area				
99424 to 99431	18460H to 18467H	1148000 to 1148007	118460H to 118467H		Error status (Class1)		0	Read	
99432 to 99439	18468H to 1846FH	1148008 to 1148015	118468H to 11846FH		System area				
99440 to 99447	18470H to 18477H	1148016 to 1148023	118470H to 118477H		Reserved station (Class1)		0	Read	
99448 to 99583	18478H to 184FFH	1148024 to 1148159	118478H to 1184FFH	System area					
99584 to 99585	18500H to 18501H	1148160 to 1148161	118500H to 118501H	Class1 Connection Behavior Error status	Input	Connection 1	0	Read	
99586 to 99839	18502H to 185FFH	1148162 to 1148415	118502H to 1185FFH			Connection 2 to 128		0	Read
99840 to 100095	18600H to 186FFH	1148416 to 1148671	118600H to 1186FFH			System area			
100096 to 100097	18700H to 18701H	1148672 to 1148673	118700H to 118701H		Output	Connection 1	0	Read	
100098 to 100351	18702H to 187FFH	1148674 to 1148927	118702H to 1187FFH			Connection 2 to 128		0	Read
100352 to 139263	18800H to 21FFFH	1148928 to 1187839	118800H to 121FFFH	System area					
139264 to 139283	22000H to 22013H	1187840 to 1187859	122000H to 122013H	Connection information area		Connection 1	0	Read	
139284 to 141823	22014H to 229FFH	1187860 to 1190399	122014H to 1229FFH			Connection 2 to 128		0	Read
141824 to 151551	22A00H to 24FFFH	1190400 to 1200127	122A00H to 124FFFH	System area					
151552 to 151553	25000H to 25001H	1200128 to 1200129	125000H to 125001H	UCMM data link execution request (No.1 to No.32)			0	Read, write	
151554 to 151567	25002H to 2500FH	1200130 to 1200143	125002H to 12500FH	System area					
151568 to 151569	25010H to 25011H	1200144 to 1200145	125010H to 125011H	UCMM data link execution request acceptance (No.1 to No.32)			0	Read	
151570 to 151583	25012H to 2501FH	1200146 to 1200159	125012H to 12501FH	System area					

P1		P2		Name		Initial value	Read, write
Address (decimal)	Address (hexadecimal)	Address (decimal)	Address (hexadecimal)				
151584 to 151585	25020H to 25021H	1200160 to 1200161	125020H to 125021H	UCMM data link execution completion (No.1 to No.32)		0	Read
151586 to 153599	25022H to 257FFH	1200162 to 1202175	125022H to 1257FFH	System area			
153600	25800H	1202176	125800H	UCMM data link (No.1) request area	Communication method specification	0	Read, write
153601	25801H	1202177	125801H		Communication method specification	0	Read, write
153602 to 153604	25802H to 25804H	1202178 to 1202180	125802H to 125804H		System area		
153605	25805H	1202181	125805H		Service	0	Read, write
153606 to 153607	25806H to 25807H	1202182 to 1202183	125806H to 125807H		Target IP Address	0	Read, write
153608 to 153627	25808H to 2581BH	1202184 to 1202203	125808H to 12581BH		System area		
153628	2581CH	1202204	12581CH		Data Size	0	Read, write
153629	2581DH	1202205	12581DH		System area		
153630	2581EH	1202206	12581EH		Class	0	Read, write
153631	2581FH	1202207	12581FH		Instance	0	Read, write
153632	25820H	1202208	125820H		Attribute	0	Read, write
153633 to 153765	25821H to 258A5H	1202209 to 1202341	125821H to 1258A5H		System area		
153766 to 154472	258A6H to 25B68H	1202342 to 1203048	1258A6H to 125B68H		Request data	0	Read, write
154473 to 154623	25B69H to 25BFFH	1203049 to 1203199	125B69H to 125BFFH		System area		
154624	25C00H	1203200	125C00H	UCMM data link (No.1) response area	Communication method specification	0	Read
154625	25C01H	1203201	125C01H		Communication method specification	0	Read
154626	25C02H	1203202	125C02H		System area		
154627 to 154628	25C03H to 25C04H	1203203 to 1203204	125C03H to 125C04H		Result storage area	0	Read
154629	25C05H	1203205	125C05H		Service	0	Read
154630 to 154631	25C06H to 25C07H	1203206 to 1203207	125C06H to 125C07H		Target IP Address	0	Read
154632 to 154651	25C08H to 25C1BH	1203208 to 1203227	125C08H to 125C1BH		System area		
154652	25C1CH	1203228	125C1CH		Data Size	0	Read
154653	25C1DH	1203229	125C1DH		System area		
154654	25C1EH	1203230	125C1EH		Class	0	Read
154655	25C1FH	1203231	125C1FH		Instance	0	Read
154656	25C20H	1203232	125C20H		Attribute	0	Read
154657 to 154787	25C21H to 25CA3H	1203233 to 1203363	125C21H to 125CA3H		System area		
154788 to 154789	25CA4H to 25CA5H	1203364 to 1203365	125CA4H to 125CA5H		Execution completion count	0	Read
154790 to 155496	25CA6H to 25F68H	1203366 to 1204072	125CA6H to 125F68H		Receive data	0	Read
155497 to 155647	25F69H to 25FFFH	1204073 to 1204223	125F69H to 125FFFH		System area		
155648 to 219135	26000H to 357FFH	1204224 to 1267711	126000H to 1357FFH	The same as UCMM data link (No.2 to No.32) request area and UCMM data link (No.1) response area			

P1		P2		Name		Initial value	Read, write
Address (decimal)	Address (hexadecimal)	Address (decimal)	Address (hexadecimal)				
219136 to 1777842	35800H to 1B20B2H	1267712 to 1777663	135800H to 1B1FFFH	System area			
1777843	1B20B3H	—	—	Number of connection consumed	For P1	0	Read
1777844	1B20B4H	—	—		For P2	0	Read
1777845 to 2097151	1B20B5H to 1FFFFFFH	—	—	System area			



Do not write data to "System area". Doing so may cause malfunction of the programmable controller system.

Details of buffer memory addresses

The following describes the buffer memory addresses of the CIP Safety module.

Setting status

■'Own Station Ethernet Address (MAC address)' (Un\G16437 to Un\G16439, Un\G1065013 to Un\G1065015)

The Ethernet address (MAC address) set in the CIP Safety module is stored.

- First word lower byte: 6th octet
- First word upper byte: 5th octet
- Second word lower byte: 4th octet
- Second word upper byte: 3rd octet
- Third word lower byte: 2nd octet
- Third word upper byte: 1st octet

CIP Safety input data size

■'CIP Safety Input Data Size' (Un\G16640 to Un\G16759, Un\G1065216 to Un\G1065335)

In safety communications, the size of the data received by the CIP Safety module from the external device is stored in units of words and in the order of connection numbers 1 to 120 whose CIP Safety module is a consumer.

CIP Safety output data size

■'CIP Safety Output Data Size' (Un\G16768 to Un\G16887, Un\G1065344 to Un\G1065463)

In safety communications, the size of the data transmitted from the CIP Safety module to the external device is stored in units of words in the order of connection numbers 1 to 120 whose CIP Safety module is a producer.

Data link status

■'Data link status Input' (Un\G16896 to Un\G16903, Un\G1065472 to Un\G1065479)

The data link status of connection numbers 1 to 120 whose CIP Safety module is a consumer is stored.

It automatically turns on when communication recovers from an error.

However, this status is not data communicated by safety communications, so do not use it in a safety program.

- Corresponding bit on: Connection established
- Corresponding bit off: No connection setting, connection being established, connection timeout, error due to setting mismatch

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
16896	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
16897	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
16898	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
16899	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
16900	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
16901	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81
16902	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97
16903	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113

*1 When using P2, add the offset value (1048576).

■'Data link status Output' (Un\G16904 to Un\G16911, Un\G1065480 to Un\G1065487)

The data link status of connection numbers 1 to 120 whose CIP Safety module is a producer is stored.

It automatically turns on when communication recovers from an error.

However, this status is not data communicated by safety communications, so do not use it in a safety program.

When sending data by safety communication multicast, the data link status turns on when even one connection is established.

The data link status turns off when all connections are not communicating or have a communication error.

- Corresponding bit on: Connection established
- Corresponding bit off: No connection setting, connection being established, connection timeout, error due to setting mismatch

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
16904	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
16905	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
16906	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
16907	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
16908	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
16909	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81
16910	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97
16911	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113

*1 When using P2, add the offset value (1048576).

Error status

■'Error status Input' (Un\G16912 to Un\G16919, Un\G1065488 to Un\G1065495)

The error status of connection numbers 1 to 120 whose CIP Safety module is a consumer is stored.

It automatically turns off when communication recovers from an error.

- Corresponding bit on: Connection timeout, setting mismatch error, connection error, external device error
- Corresponding bit off: No connection setting, connection established

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
16912	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
16913	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
16914	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
16915	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
16916	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
16917	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81
16918	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97
16919	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113

*1 When using P2, add the offset value (1048576).

■'Error status Output' (Un\G16920 to Un\G16927, Un\G1065496 to Un\G1065503)

The error status of connection numbers 1 to 120 whose CIP Safety module is a producer is stored.

It automatically turns off when communication recovers from an error.

When sending data by safety communication multicast, the error status turns off when even one connection is established.

When all connected connections have a communication error, the communication error turns on.

- Corresponding bit on: Connection timeout, setting mismatch error, connection error, external device error
- Corresponding bit off: No connection setting, connection established

The following table shows the assignment of the connection number to each bit.


Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
16920	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
16921	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
16922	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
16923	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
16924	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
16925	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81
16926	112	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97
16927	—	—	—	—	—	—	—	—	120	119	118	117	116	115	114	113

*1 When using P2, add the offset value (1048576).

CIP Safety own station connection error status

■'CIP Safety own station connection error status input (Connection 1)' (Un\G16928, Un\G16929, Un\G1065504, Un\G1065505)

The error code of the error that occurred in connection number 1 whose CIP Safety module is a consumer is stored in double-word units.


Setting value	Description
0	Normal
Other than 0	Error code ( Page 217 When the connection is abnormal)

■'CIP Safety own station connection error status input (Connection 2 to 120)' (Un\G16930 to Un\G17167, Un\G1065506 to Un\G1065743)

The information of connection numbers 2 to 120 is stored in the same way as 'CIP Safety own station connection error status input (Connection 1)' (Un\G16928, Un\G16929, Un\G1065504, Un\G1065505).

■'CIP Safety own station connection error status output (Connection 1)' (Un\G17168, Un\G17169, Un\G1065744, Un\G1065745)

The error code of the error that occurred in connection number 1 whose CIP Safety module is a producer is stored in double-word units.

Setting value	Description
0	Normal
Other than 0	Error code ( Page 217 When the connection is abnormal)

■'CIP Safety own station connection error status output (Connection 2 to 120)' (Un\G17170 to Un\G17407, Un\G1065746 to Un\G1065983)

The information of connection numbers 2 to 120 is stored in the same way as 'CIP Safety own station connection error status output (Connection 1)' (Un\G17168, Un\G17169, Un\G1065744, Un\G1065745).

Connection information area

To prevent the data from becoming inconsistent, read an even-numbered word size when reading a two-word size area.
(Specify an even-numbered size with the BMOV/FROM instruction, or use the DMOV/DFROM instruction.)
Also, specify an even-numbered address for the start address to be read.

■'Connection information area input (Connection 1)' (Un\G18432 to Un\G18451, Un\G1067008 to Un\G1067027)

The connection information of connection number 1 whose CIP Safety module is a consumer is stored.

The following table shows the stored data.

Number of words	Name		Description
1st to 2nd words	Diagnostic	Production Connection ID	Stores the transmission connection ID for the target of the requested connection.
3rd to 4th words		Consumption Connection ID	Stores the receive connection ID for the target of the requested connection.
5th to 6th words		O->T API (μs)	Stores the originator to target API (μs) for the target of the requested connection.
7th to 8th word		T->O API (μs)	Stores the target to originator API (μs) for the target of the requested connection.
9th to 10th words		O->T RPI (μs)	Stores the originator to target RPI (μs) for the target of the requested connection.
11th to 12th words		T->O RPI (μs)	Stores the target to originator RPI (μs) for the target of the requested connection.
13th to 14th words		O->T Net Parameters	Stores the originator to target network parameters for the target of the requested connection.
15th to 16th words		T->O Net Parameters	Stores the target to originator network parameters for the target of the requested connection.
17th word		Originator Connection Serial Number	Stores the originator connection serial number.
18th word		Originator Vendor Id	Stores the originator vendor ID.
19th to 20th words		Originator Serial Number	Stores the originator serial number.

■'Connection information area input (Connection 2 to 120)' (Un\G18452 to Un\G20831, Un\G1067028 to Un\G1069407)

The information of connection numbers 2 to 120 is stored in the same way as Connection 1.

■'Connection information area output (Connection 1)' (Un\G20832 to Un\G20851, Un\G1069408 to Un\G1069427)

The connection information of connection number 1 whose CIP Safety module is a producer is stored.

Stored data is the same as 'Connection information area input (Connection 1)' (Un\G18432 to Un\G18451, Un\G1067008 to Un\G1067027).

■'Connection information area output (Connection 2 to 120)' (Un\G20852 to Un\G23231, Un\G1069428 to Un\G1071807)

The information of connection numbers 2 to 120 is stored in the same way as 'Connection information area output (Connection 1)' (Un\G20832 to Un\G20851, Un\G1069408 to Un\G1069427).

Class1 Input Area

■'Class1 Input Area' (Un\G24576 to Un\G57343, Un\G1073152 to Un\G1105919)

The data received by the CIP Safety module from the EtherNet/IP device during Class1 communications is stored.

The storage area is secured in ascending order from connection number 1 at the start address of this area.

Class1 Output Area

■'Class1 Output Area' (Un\G61440 to Un\G94207, Un\G1110016 to Un\G1142783)

The data to transmit to the EtherNet/IP device from the CIP Safety module during Class1 communications is stored.

The storage area is secured in ascending order from connection number 1 at the start address of this area.

EtherNet/IP Communication Start Request

■'EtherNet/IP Communication Start Request' (Un\G98048, Un\G1146624)

Set the value to bit 0 when the EtherNet/IP communications start is requested. (Use of bit 1 to 15 is prohibited.)

- Off: Not requested
- On: Requested

Class1 input data size

■'Class1 input data size' (Un\G98304 to Un\G98431, Un\G1146880 to Un\G1147007)

The size of the data received by the CIP Safety module from the EtherNet/IP device during Class1 communications is stored in units of words and in ascending order from connection number 1.

Class1 output data size

■'Class1 output data size' (Un\G98560 to Un\G98687, Un\G1147136 to Un\G1147263)

The size of the data to send to the EtherNet/IP device from the CIP Safety module during Class1 communications is stored in units of words and in ascending order from connection number 1.

Class1 Start offset address to the input data

■'Class1 Start offset address to the input data' (Un\G98816 to Un\G98943, Un\G1147392 to Un\G1147519)

The offset address of the data storage location ('Class1 Input Area' (Un\G24576, Un\G1073152)) received by the CIP Safety module from the EtherNet/IP device during Class1 communications is stored in ascending order from connection number 1.

The offset address of each connection is aligned to start in two-word units.

Setting value	Description
0 to 32767 (0H to 7FFFH)	Offset address
65535 (FFFFH)	No assignment

Class1 Start offset address to the output data

■'Class1 Start offset address to the output data' (Un\G99072 to Un\G99199, Un\G1147648 to Un\G1147775)

The offset address of the data storage location ('Class1 Output Area' (Un\G61440, Un\G1110016)) to send to the EtherNet/IP device from the CIP Safety module during Class1 communications is stored in ascending order from connection number 1.

The offset address of each connection is aligned to start in two-word units.

Setting value	Description
0 to 32767 (0H to 7FFFH)	Offset address
65535 (FFFFH)	No assignment

Class1 communication status

■'Data link status (Class1)' (Un\G99408 to Un\G99415, Un\G1147984 to Un\G1147991)

The data link status of each connection during Class1 communications is stored.

It automatically turns on when communication recovers from an error.

- Corresponding bit on: Connection established
- Corresponding bit off: No connection setting, connection being established, connection timeout, error due to setting mismatch

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
99408	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
99409	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
99410	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
99411	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49

*1 When using P2, add the offset value (1048576).

Precautions

During tag communications, if one producer tag is connected to multiple consumer tags through multicast communications, it turns on if even one communication operation is normal.

The connection with all consumer tags turns off when there is no communication or a communication error occurs.

■'Error status (Class1)' (Un\G99424 to Un\G99431, Un\G1148000 to Un\G1148007)

The error status of each connection during Class1 communications is stored.

It automatically turns off when communication recovers from an error.

- Corresponding bit on*1: Connection timeout, setting mismatch error, connection error, external device error
- Corresponding bit off: No connection setting, connection established

*1 For a producer tag during tag communications, it turns on only when communications with all the connected consumer tags are stopped.

The following table shows the assignment of the connection number to each bit.

Buffer memory address*2	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
99424	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
99425	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
99426	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
99427	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49

*2 When using P2, add the offset value (1048576).

■'Reserved station (Class1)' (Un\G99440 to Un\G99447, Un\G1148016 to Un\G1148023)

The setting status of the reserved station of each connection during Class1 communications is stored.

The setting details set by CIP Safety Configuration Tool are reflected for the reserved station.

- Corresponding bit on: Reserved station
- Corresponding bit off: Not set as reserved station

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
99440	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
99441	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
99442	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
99443	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49

*1 When using P2, add the offset value (1048576).


Class1 Connection Behavior Error status

To prevent the data from becoming inconsistent, read an even-numbered word size when reading. (Specify an even-numbered size with the BMOV/FROM instruction, or use the DMOV/DFROM instruction.)

Also, specify an even-numbered address for the start address to be read.

■'Class1 Connection Behavior Error status input (Connection 1)' (Un\G99584 to Un\G99585, Un\G1148160 to Un\G1148161)

The error code on the input side (at the time of reception) that occurred at each connection during Class1 communications is stored in double-word units.


Setting value	Description
0	Normal
Other than 0	Error code ( Page 217 When the connection is abnormal)

■'Class1 Connection Behavior Error status input (connection 2 or higher)' (Un\G99586 to Un\G99839, Un\G1148162 to Un\G1148415)

The same information as 'Class1 Connection Behavior Error status input (Connection 1)' (Un\G99584 to Un\G99585, Un\G1148160 to Un\G1148161) is stored.

■'Class1 Connection Behavior Error status output (Connection 1)' (Un\G100096 to Un\G100097, Un\G1148672 to Un\G1148673)

The error code on the output side (during transmission) that occurred at each connection during Class1 communications is stored in double-word units.

Setting value	Description
0	Normal
Other than 0	Error code ( Page 217 When the connection is abnormal)

■'Class1 Connection Behavior Error status output (Connection 2 or higher)' (Un\G100098 to Un\G100351, Un\G1148674 to Un\G1148927)

The same information as 'Class1 Connection Behavior Error status output (Connection 1)' (Un\G100096 to Un\G100097, Un\G1148672 to Un\G1148673) is stored.

A

Connection information area

To prevent the data from becoming inconsistent, read an even-numbered word size when reading a two-word size area.
(Specify an even-numbered size with the BMOV/FROM instruction, or use the DMOV/DFROM instruction.)
Also, specify an even-numbered address for the start address to be read.

■'Connection information area (Connection1)' (Un\G139264 to Un\G139283, Un\G1187840 to Un\G1187859)

The connection information of each connection of Class1 is stored.

The following table shows the stored data.

Number of words	Name		Description
1st to 2nd words	Diagnostic	Production Connection ID	Stores the transmission connection ID for the target of the requested connection.
3rd to 4th words		Consumption Connection ID	Stores the receive connection ID for the target of the requested connection.
5th to 6th words		O->T API (μs)	Stores the originator to target API (μs) for the target of the requested connection.
7th to 8th word		T->O API (μs)	Stores the target to originator API (μs) for the target of the requested connection.
9th to 10th words		O->T RPI (μs)	Stores the originator to target RPI (μs) for the target of the requested connection.
11th to 12th words		T->O RPI (μs)	Stores the target to originator RPI (μs) for the target of the requested connection.
13th to 14th words		O->T Net Parameters	Stores the originator to target network parameters for the target of the requested connection.
15th to 16th words		T->O Net Parameters	Stores the target to originator network parameters for the target of the requested connection.
17th word		Originator Connection Serial Number	Stores the originator connection serial number.
18th word		Originator Vendor Id	Stores the originator vendor ID.
19th to 20th words		Originator Serial Number	Stores the originator serial number.

■'Connection information area (Connection 2 or higher)' (Un\G139284 to Un\G141823, Un\G1187860 to Un\G1190399)

The same information as 'Connection information area (Connection 1)' (Un\G139264 to Un\G139283, Un\G1187840 to Un\G1187859) is stored.

UCMM data link execution request (No.1 to No.32)

■'UCMM data link execution request (No.1 to No.32)' (Un\G151552 to Un\G151553, Un\G1200128 to Un\G1200129)

Sending a request command by the communication specified in the request area in 'UCMM data link (No.1 to No.32) area' (Un\G153600 to Un\G219135, Un\G1202176 to G1267711) is requested.

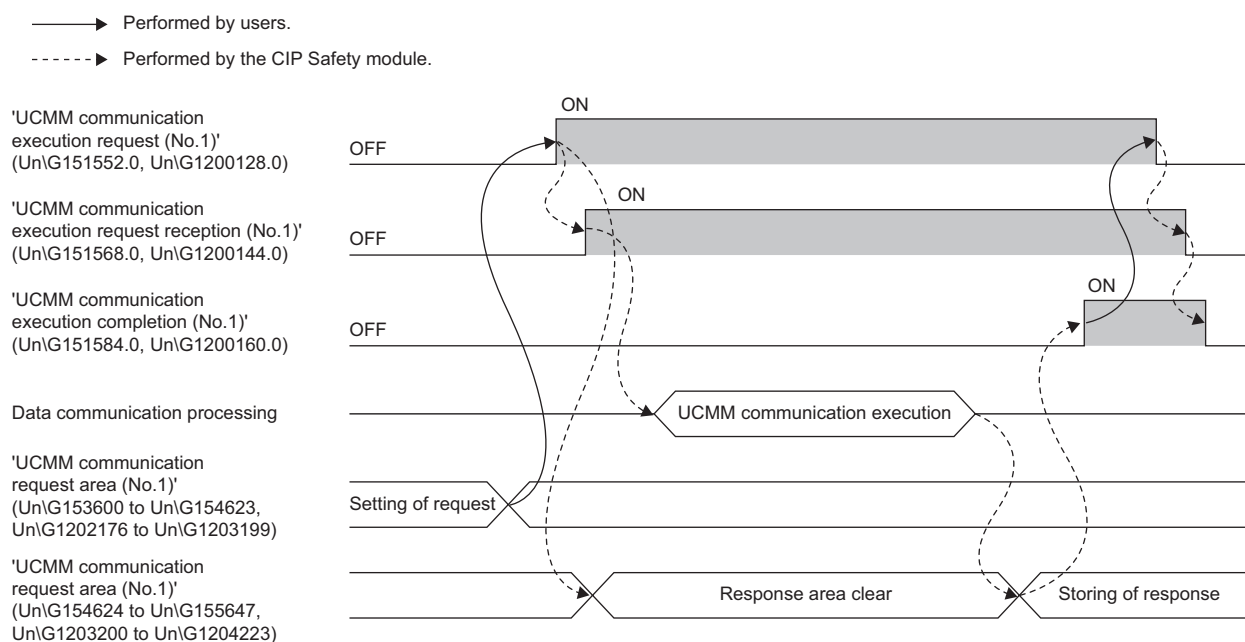
- Corresponding bit on: Request present
- Corresponding bit off: Request not present

The following table shows the assignment of the connection number to each bit.

Buffer memory address ^{*1}	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
151552	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
151553	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17

*1 When using P2, add the offset value (1048576).

The following is a timing chart that uses each area.



UCMM data link execution request acceptance (No.1 to No.32)

■'UCMM data link execution request acceptance (No.1 to No.32)' (Un\G151568 to Un\G151569, Un\G1200144 to Un\G1200145)

The acceptance status of the request by 'UCMM data link execution request (No.1 to No.32)' (Un\G151552 to Un\G151553, Un\G1200128 to Un\G1200129) is stored.

- Corresponding bit on: Accepted
- Corresponding bit off: Not accepted

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
151568	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
151569	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17

*1 When using P2, add the offset value (1048576).

For the timing chart that uses each area, refer to the following.

 Page 247 UCMM data link execution request (No.1 to No.32)

UCMM data link execution completion (No.1 to No.32)

■UCMM data link execution completion (No.1 to No.32) (Un\G151584 to Un\G151585, Un\G1200160 to Un\G1200161)

The execution status of the requested communications is stored.


- Corresponding bit on: Completed
- Corresponding bit off: Not completed or unexecuted

The following table shows the assignment of the connection number to each bit.

Buffer memory address*1	Assignment of connection number to bit															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
151584	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
151585	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17

*1 When using P2, add the offset value (1048576).

For the timing chart that uses each area, refer to the following.

 Page 247 UCMM data link execution request (No.1 to No.32)

UCMM data link (No.1) request area

■'UCMM data link (No.1) request area (communication method specification)' (Un\G153600, Un\G1202176)

The communication method is specified.

Setting value	Description
1H	UCMM communications

■'UCMM data link (No.1) request area (communication method specification)' (Un\G153601, Un\G1202177)

The communication method is specified.

Setting value	Description
1H	Message communications

■'UCMM data link (No.1) request area (Service)' (Un\G153605, Un\G1202181)

The service code of EtherNet/IP message communication is specified.

The following table shows some of the commonly used service codes. For other service codes, refer to the manuals of the external device.

Service code	Service name	Description
EH	Get_Attribute_Single	Obtains the setting value of the specified Attribute.
10H	Set_Attribute_Single	Sets the value to the specified Attribute.

■'UCMM data link (No.1) request area (target IP address)' (Un\G153606 to Un\G153607, Un\G1202182 to Un\G1202183)

The IP address of the EtherNet/IP device to which the request data is sent by UCMM communications is specified. (0.0.0.1 to 223.255.255.254)

- First word lower byte: 4th octet
- First word upper byte: 3rd octet
- Second word lower byte: 2nd octet
- Second word upper byte: 1st octet

■UCMM data link (No.1) request area (Data Size)' (Un\G153628, Un\G1202204)

The request data size is set. (0 to 504 bytes)

■'UCMM data link (No.1) request area (Class)' (Un\G153630, Un\G1202206)

The class of the transmit destination EtherNet/IP device is set. For details, refer to the manuals of the transmit destination EtherNet/IP device.

■'UCMM data link (No.1) request area (Instance)' (Un\G153631, Un\G1202207)

The instance of the transmit destination EtherNet/IP device is set. For details, refer to the manuals of the transmit destination EtherNet/IP device.

■'UCMM data link (No.1) request area (Attribute)' (Un\G153632, Un\G1202208)

The attribute of the transmit destination EtherNet/IP device is set. For details, refer to the manuals of the transmit destination EtherNet/IP device.

■'UCMM data link (No.1) request area (request data)' (Un\G153766 to Un\G154472, Un\G1202342 to Un\G1203048)

The required value for each service code is set.

However, this area is not used for services that acquire values from the transmit destination device.

For details, refer to the manuals of the transmit destination EtherNet/IP device.

The following table shows the examples of setting value for commonly used service codes.

Service name	Setting value
Get_Attribute_Single	Not set
Set_Attribute_Single	Value to be set for the specified Attribute

UCMM data link (No.1) response area

■'UCMM data link (No.1) response area (communication method specification)' (Un\G154624, Un\G1203200)

The value of the request area is stored.

■'UCMM data link (No.1) response area (communication method specification)' (Un\G154625, Un\G1203201)

The value of the request area is stored.

■'UCMM data link (No.1) response area (result storage area)' (Un\G154627 to Un\G154628, Un\G1203203 to Un\G1203204)

The processing result is stored.

- 0: Completed successfully
- Other than 0: Completed with an error (error code)

For details on the error codes, refer to the following.

☞ Page 217 When the connection is abnormal

■'UCMM data link (No.1) response area (Service)' (Un\G154629, Un\G1203205)

The value of the request area is stored.

■'UCMM data link (No.1) response area (target IP address)' (Un\G154630 to Un\G154631, Un\G1203206 to Un\G1203207)

The value of the request area is stored.

■'UCMM data link (No.1) response area (Data Size)' (Un\G154652, Un\G1203228)

Refer to the following.

📖 Manuals of the EtherNet/IP device from which the response command was transmitted

📖 CIP specifications

■'UCMM data link (No.1) response area (Class)' (Un\G154654, Un\G1203230)

Refer to the following.

📖 Manuals of the EtherNet/IP device from which the response command was transmitted

📖 CIP specifications

■'UCMM data link (No.1) response area (Instance)' (Un\G154655, Un\G1203231)

Refer to the following.

📖 Manuals of the EtherNet/IP device from which the response command was transmitted

📖 CIP specifications

■'UCMM data link (No.1) response area (Attribute)' (Un\G154656, Un\G1203232)

Refer to the following.

📖 Manuals of the EtherNet/IP device from which the response command was transmitted

📖 CIP specifications

■'UCMM data link (No.1) response area (number of executions completed)' (Un\G154788 to Un\G154789, Un\G1203364 to Un\G1203365)

The number of execution completions of UCMM communication is stored.

If the following request is completed when the current value is FFFFH, the value returns to 0H. (Only used for lower-order words and the value is fixed to 0H for higher-order words.)

■'UCMM data link (No.1) response area (response data)' (Un\G154790 to Un\G155496, Un\G1203366 to Un\G1204072)

The response data from the EtherNet/IP device from which the response command was transmitted is stored.

For details, refer to the manuals of the transmit destination EtherNet/IP device.

UCMM data link (No.2 to No.32) request area/response area

■'UCMM data link (No.2 to No.32) request area/response area' (Un\G155648 to Un\G219135, Un\G1204224 to Un\G1267711)

The information of No.2 to No.32 is set and stored in the same order as UCMM data link (No.1) request area and UCMM data link (No.1) response area.

Number of connection consumed

■'Number of connection consumed (P1)' (Un\G1777843)

The number of currently consumed connections is displayed. (0 to 64)

It counts up each time connection is made to the originator and target during Class1 communications.

If the count exceeds 64, connection will not be possible.

If the connected device cannot communicate due to a cable disconnection or communication error, it counts down.

■'Number of connection consumed (P2)' (Un\G1777844)

The same information as for P1 is stored.

Appendix 8 Processing Time

Refresh processing time

The refresh processing time is the time in which data is exchanged between the CIP Safety module and the CPU module. It is the processing time of when auto refresh is set.


This section describes the calculation method of the refresh processing time.

Calculation formula for refresh processing time

Refresh processing time [μ s] = refresh read time (transfer time from the CIP Safety module to the CPU module) + refresh write time (transfer time from the CPU module to the CIP Safety module)



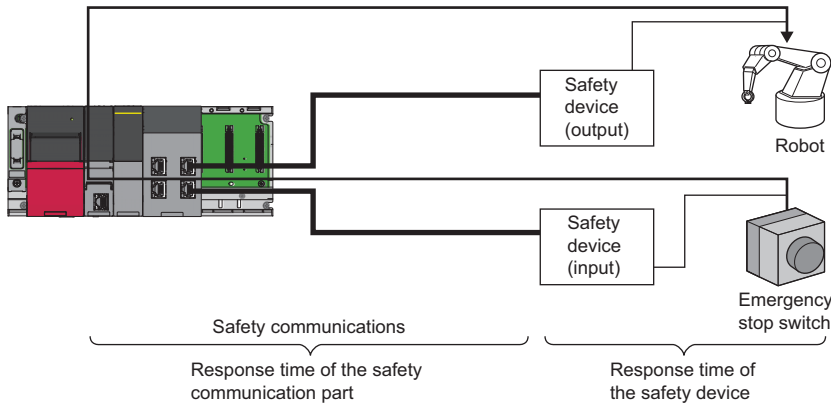
For the refresh read time and refresh write time, refer to the refresh processing time of the intelligent function module in the following manual.

 MELSEC iQ-R CPU Module User's Manual (Application)

Safety response time

The safety response time is the total response time (maximum value) from the input device (such as a sensor and switch) to the output device (such as an actuator).

If the following system configuration is used as an example, the safety response time is the time from when the emergency stop switch is pressed until the robot stops.



Calculation formula for safety response time

The total safety response time is the sum of the response time of the safety communication part and the response time of the safety device.

Item	Calculation formula
Response time of the safety communication part (ms)	$RPI_1 \times (Timeout_Multiplier_1 + 3) + RPI_2 \times (Timeout_Multiplier_2 + 3) + SC_{gw} \times 6 + SC_{CPU} \times 3 + RM_{CPU} \times 2$
Response time of the safety device (ms)	Maximum response time of the safety device

- RPI_1 : RPI value on the producer connection side
- $Timeout_Multiplier_1$: Timeout_Multiplier value on the producer connection side
- RPI_2 : RPI value on the consumer connection side
- $Timeout_Multiplier_2$: Timeout_Multiplier value on the consumer connection side
- SC_{CPU} : Safety CPU safety cycle time set with the engineering tool
- RM_{CPU} : Safety CPU safety refresh monitoring time
- SC_{gw} : CIP Safety module safety cycle time ($0.8 + 0.13 \times \text{total number of CIP Safety connections}$)

A

Communication performance

The following elements are factored into EtherNet/IP network communication performance.

- PPS (Packets Per Second): Number of send/receive packets per second
- RPI (Requested Packet Interval): A packet transmission interval of Class1 communications
- EPI (Expected Packet Interval): A packet transmission interval of CIP Safety communications

Generally, the PPS is used as an index of the communication performance of EtherNet/IP devices.

The PPS indicates the number of send/receive packets per second. Therefore, by calculating the PPS from the RPI (EPI), which represents the communication cycle of each connection, and then summing these values, the PPS of the device can be estimated.

☞ Page 254 PPS calculation method for Class1 communications

☞ Page 256 PPS calculation method for CIP Safety communications

When setting the RPI (EPI) of the CIP Safety module, calculate the PPS of each connection and configure the setting so that the following performance specifications are satisfied.

- Maximum PPS of the CIP Safety module
- Minimum RPI (EPI) of the CIP Safety module

☞ Page 23 Performance Specifications

PPS calculation method for Class1 communications

In Class1 communications, data is sent in two directions, the T->O side and the O->T side, in one connection. Therefore, the PPS can be calculated by the following formulas.

- $PPS = PPS_{TO} + PPS_{OT}$

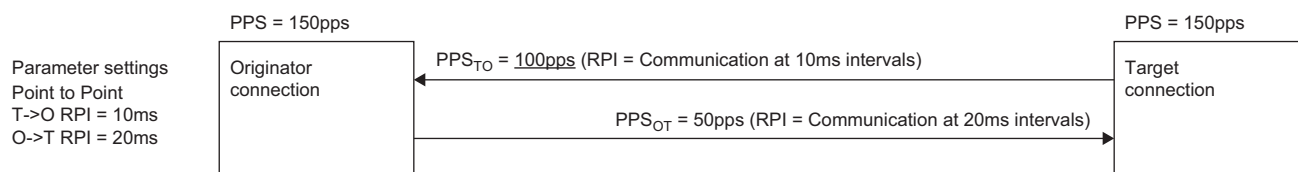
$$PPS_{TO} = 1000 / RPI_{TO}$$

$$PPS_{OT} = 1000 / RPI_{OT}$$

Item	Description
PPS_{TO}	PPS on the T->O side
RPI_{TO}	RPI setting value [ms] on the T->O side
PPS_{OT}	PPS on the O->T side
RPI_{OT}	RPI setting value [ms] on the O->T side

Ex.

Calculation example for Point to Point (1:1 connection)



Connection	PPS	Breakdown
Originator	150pps	100pps + 50pps
Target	150pps	(Same as above)

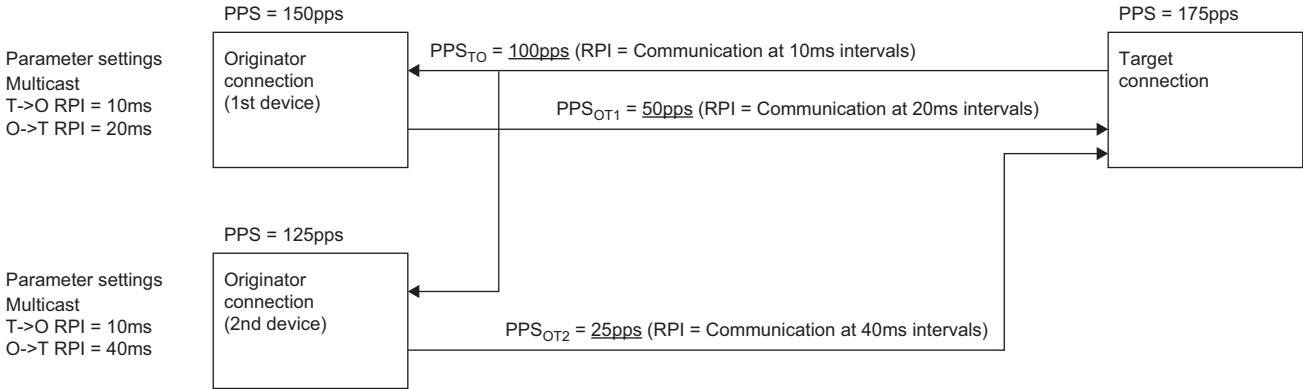
■When multiple devices are connected via multicast connection

When multiple devices are connected via multicast connection, add the PPS_{OT} for the additional connections.
When three devices are connected, calculate the PPS using the following formula.

- $PPS = PPS_{TO} + PPS_{OT1} + PPS_{OT2} + PPS_{OT3}$
PPS_{OT1}: PPS for the 1st device
PPS_{OT2}: PPS for the 2nd device (additional connection)
PPS_{OT3}: PPS for the 3rd device (additional connection)

Ex.

Calculation example for multicast connection (1:2 connection)



Connection	PPS	Breakdown
Originator (1st device)	150pps	100pps + 50pps
Originator (2nd device)	125pps	100pps + 25pps
Target	175pps	100pps + 50pps + 25pps

PPS calculation method for CIP Safety communications

In CIP Safety communications, the connections on the T->O side and the O->T side are independent of each other. In addition, transmission occurs in both directions for each connection: CIP Safety data and CIP Safety TCM (Time Coordination Message)^{*1}.

Therefore, in CIP Safety communications, calculate the PPS using the following formulas.

$$\bullet \text{ PPS} = (\text{PPS}_{\text{TO}} + \text{PPS}_{\text{TO_TCM}}) + (\text{PPS}_{\text{OT}} + \text{PPS}_{\text{OT_TCM}})$$

$$\text{PPS}_{\text{TO}} = 1000 / \text{EPI}_{\text{TO}}$$

$$\text{PPS}_{\text{TO_TCM}} = 1000 / (\text{EPI}_{\text{TO}} \times \text{Coefficient}^{*2})$$

$$\text{PPS}_{\text{OT}} = 1000 / \text{EPI}_{\text{OT}}$$

$$\text{PPS}_{\text{OT_TCM}} = 1000 / (\text{EPI}_{\text{OT}} \times 19^{*3})$$

Item	Description
PPS _{TO}	PPS for CIP Safety data on the T->O side
PPS _{TO_TCM}	PPS for CIP Safety TCM on the T->O side
EPI _{TO}	EPI setting value [ms] on the T->O side
PPS _{OT}	PPS for CIP Safety data on the O->T side
PPS _{OT_TCM}	PPS for CIP Safety TCM on the O->T side
EPI _{OT}	EPI setting value [ms] on the O->T side

*1 Data used to control CIP Safety communications. It needs to be included in the PPS calculation for CIP Safety communications.

*2 The coefficients used for the CIP Safety module are as follows:

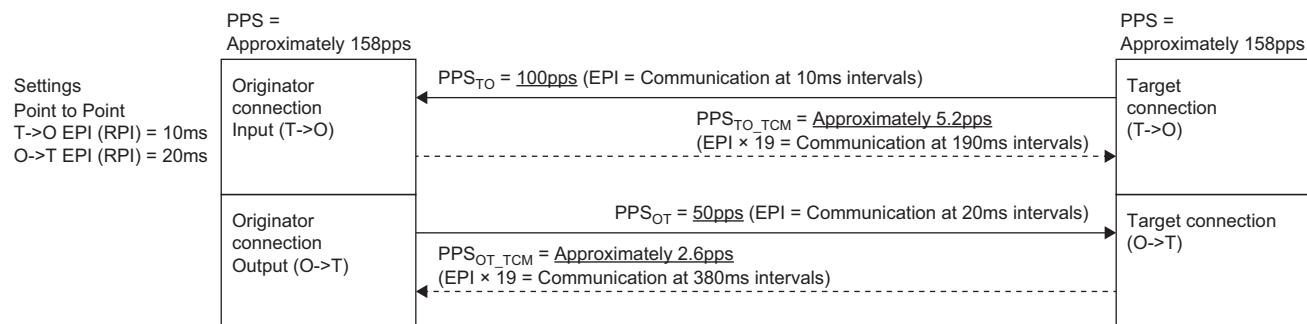
- Point to Point communication: 19
- Multicast communication: 100

*3 Because the O->T-side connection is always Point to Point communication, the coefficient is 19.

Ex.

Calculation example for Point to Point (1:1 connection)

[Legends] ———▶: CIP Safety data communication - - - -▶: CIP Safety TCM communication



Connection	PPS	Breakdown
Originator input (T->O)	105.2pps	100pps + 5.2pps
Originator output (O->T)	52.6pps	50pps + 2.6pps
Target (T->O)	105.2pps	100pps + 5.2pps
Target (O->T)	52.6pps	50pps + 2.6pps

Time required for detecting and recovering from ring configuration error

The following table shows the time defined in the CIP specification for detecting and recovering from ring configuration errors when the DLR function is used. Note that these values are approximate because times vary depending on the DLR parameter settings and the configuration devices.

Precondition

As preconditions, all connected devices support DLRs and operate at 100Mbps/full-duplex.

In addition, the details of two types of ring nodes are described below. If an Announce Frame Based Node exists in the ring configuration, the time required to detect and recover from an error will be longer than the case when the ring configuration consists only of Beacon Frame Based Nodes.

- Beacon Frame Based Nodes: Ring nodes that operate based on beacon frames from the DLR function
- Announce Frame Based Nodes: Ring nodes that operate based on announcement frames from the DLR function

Variable	Description
BcnFrmDly	Delay time due to beacon frames during storing and forward switching: 7μs
AvgEipFrmDly	Delay time due to average EtherNet/IP frames: 12μs
MaxFrmDly	Delay time due to Ethernet frames of maximum size: 124μs
MaxDlyNodePrct	Percentage of the number of nodes in the ring whose beacons are delayed due to Ethernet frames of maximum size: 10%
IntSwchDly	Internal switching delay time for each node: 5μs
WirePrpgtDly	Signal propagation delay time for 100m copper media: 1μs
NodeProcDly	Node processing delay time for responding to ring frames and events: 25μs
BcnIntrvl	Beacon interval: 400μs

Theoretical value

The following table shows theoretical values of the time required to detect and recover from an error under the above precondition.

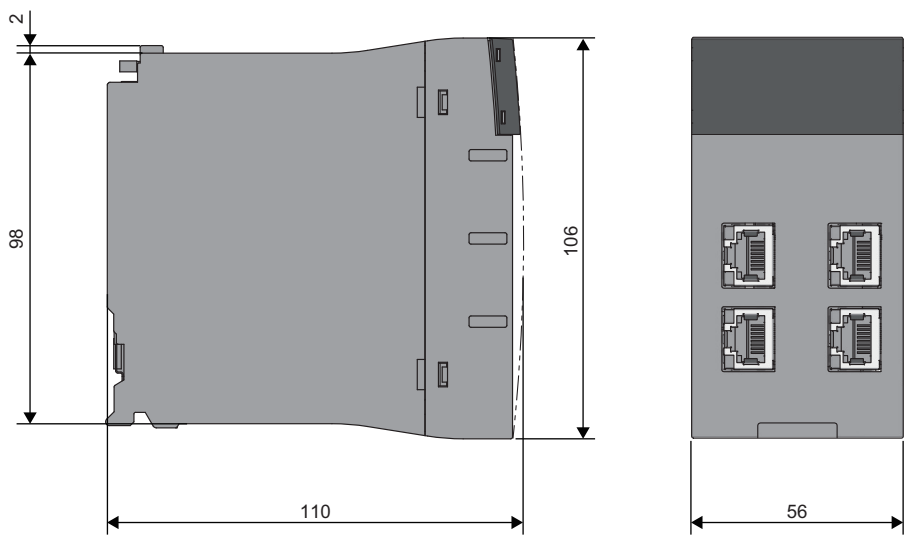
For detailed calculation method for the time required to detect and recover from an error, refer to the CIP specification.

Number of ring nodes	Parameter settings		Error detection time			Recovery time	
	Beacon sending interval	Beacon timeout	When physical failure is detected (for example, cable disconnection)	When physical failure is not detected (for example, packet loss)		Without Announce Frame Based Nodes in ring configuration	With Announce Frame Based Nodes in ring configuration
				Without Announce Frame Based Nodes in ring configuration	With Announce Frame Based Nodes in ring configuration		
25	400μs	1380μs	980μs	1858μs	2335μs	1808μs	2260μs
50	400μs	1960μs	1885μs	2890μs	3820μs	3165μs	4070μs

A

Appendix 9 External Dimensions

This section describes the external dimensions of the CIP Safety module.



(Unit: mm)

Appendix 10 Instance Number (Connection Point) for Class1 Instance Communications

This section describes the specifications of the instance number (connection point) used in a target connection for Class1 instance communications of the CIP Safety module. The required information on the connection settings for the device on the originator side is summarized when the CIP Safety module uses the target connection for Class1 instance communications. When the connection settings cannot be configured by using the EDS file because an originator device manufactured by other companies is used, the settings can be configured by using this information.



This information has been defined in the EDS file of the CIP Safety module, so setting is not necessary when the connection settings are available by using the EDS file.

Keying information (device identification) of the CIP Safety module

Item	Description
Vendor ID (vendor code)	161
Product type	140
Product code	11
Major version	1
Minor version	1

Instance list used in the CIP Safety module

The following instances are used as the instance numbers (connection points) for the CIP Safety module.

T: target, O: originator

Instance item	Instance number	Size	Format	Remarks
Configuration	1	0 bytes	—	Used for Exclusive Owner, Input Only
Input (T->O)	768 to 831	1 to 1444 bytes ^{*1}	Modeless	Used for Exclusive Owner, Input Only
Output (O->T)	1024 to 1087	1 to 1444 bytes ^{*1}	32bits, Run/Idle header	Used for Exclusive Owner
Heartbeat (O->T)	238	0 bytes	Heartbeat	Used for Input Only

^{*1} The size of the target connection set for the CIP Safety module.

Connection numbers and instance numbers

The instance numbers of the CIP Safety module are assigned as follows related to the set connection numbers on the target side.

Connection type	Connection number	Instance number			Configuration
		Input (T->O)	Output (O->T)	Heartbeat (O->T)	
Exclusive Owner	1	768	1024	—	1
	2	769	1025	—	1
	3	770	1026	—	1
	⋮	⋮	⋮	⋮	⋮
	62	829	1085	—	1
	63	830	1086	—	1
	64	831	1087	—	1
Input Only	1	768	—	238	1
	2	769	—	238	1
	3	770	—	238	1
	⋮	⋮	⋮	⋮	⋮
	62	829	—	238	1
	63	830	—	238	1
	64	831	—	238	1

Appendix 11 Added and Enhanced Functions

The functions added to or changed in the CIP Safety module are shown.

Added and enhanced functions	Firmware version of the CIP Safety module	CIP Safety Configuration Tool	Engineering tool (GX Works3)
<ul style="list-style-type: none">• The number of CIP Safety connections is extended from 60 to 120.• DLR is supported.• Reading configuration is supported.• Firmware update is supported.	"02"	■Model SW1DNN-SEIPCT-MD ■Software version Version 1.3.0.28 or later	Version 1.100E or later

INDEX

A

Adapter 28

C

Class1 communications 25

S

Safety communications 25
Scanner 28

U

UCMM communications 25



MEMO

REVISIONS

*The manual number is given on the bottom left of the back cover.

Revision date	*Manual number	Description
January 2023	SH(NA)-082444ENG-A	First edition
February 2024	SH(NA)-082444ENG-B	■Added functions Extension of the number of connections for CIP Safety from 60 to 120, DLR, reading of the configuration, firmware update ■Added or modified parts Chapter 1, Section 2.1, 2.2, 4.2, 4.4, 6.1, 6.5, 7.2, 8.2, 9.4, 9.6, 10.1, 10.2, 10.3, 10.4, 11.1, 11.4, 11.5, 11.6, Appendix 7, 8, 10, 11
December 2024	SH(NA)-082444ENG-C	■Added or modified parts Section 4.4, 11.4, Appendix 8

Japanese manual number: SH-082443-D

This manual confers no industrial property rights or any rights of any other kind, nor does it confer any patent licenses. Mitsubishi Electric Corporation cannot be held responsible for any problems involving industrial property rights which may occur as a result of using the contents noted in this manual.

© 2023 MITSUBISHI ELECTRIC CORPORATION

WARRANTY

Please confirm the following product warranty details before using this product.

1. Limited Warranty and Product Support.

- a. Mitsubishi Electric Company ("MELCO") warrants that for a period of eighteen (18) months after date of delivery from the point of manufacture or one year from date of Customer's purchase, whichever is less, Mitsubishi MELSEC Safety programmable logic controllers (the "Products") will be free from defects in material and workmanship.
- b. At MELCO's option, for those Products MELCO determines are not as warranted, MELCO shall either repair or replace them or issue a credit or return the purchase price paid for them.
- c. For this warranty to apply:
 - (1) Customer shall give MELCO (i) notice of a warranty claim to MELCO and the authorized dealer or distributor from whom the Products were purchased, (ii) the notice shall describe in reasonable details the warranty problem, (iii) the notice shall be provided promptly and in no event later than thirty (30) days after the Customer knows or has reason to believe that Products are not as warranted, and (iv) in any event, the notice must be given within the warranty period;
 - (2) Customer shall cooperate with MELCO and MELCO's representatives in MELCO's investigation of the warranty claim, including preserving evidence of the claim and its causes, meaningfully responding to MELCO's questions and investigation of the problem, grant MELCO access to witnesses, personnel, documents, physical evidence and records concerning the warranty problem, and allow MELCO to examine and test the Products in question offsite or at the premises where they are installed or used; and
 - (3) If MELCO requests, Customer shall remove Products it claims are defective and ship them to MELCO or MELCO's authorized representative for examination and, if found defective, for repair or replacement. The costs of removal, shipment to and from MELCO's designated examination point, and reinstallation of repaired or replaced Products shall be at Customer's expense.
 - (4) If Customer requests and MELCO agrees to effect repairs onsite at any domestic or overseas location, the Customer will pay for the costs of sending repair personnel and shipping parts. MELCO is not responsible for any re-commissioning, maintenance, or testing on-site that involves repairs or replacing of the Products.
- d. Repairs of Products located outside of Japan are accepted by MELCO's local authorized service facility centers ("FA Centers"). Terms and conditions on which each FA Center offers repair services for Products that are out of warranty or not covered by MELCO's limited warranty may vary.
- e. Subject to availability of spare parts, MELCO will offer Product repair services for (7) years after each Product model or line is discontinued, at MELCO's or its FA Centers' rates and charges and standard terms in effect at the time of repair. MELCO usually produces and retains sufficient spare parts for repairs of its Products for a period of seven (7) years after production is discontinued.
- f. MELCO generally announces discontinuation of Products through MELCO's Technical Bulletins. Products discontinued and repair parts for them may not be available after their production is discontinued.

2. Limits of Warranties.

- a. MELCO does not warrant or guarantee the design, specify, manufacture, construction or installation of the materials, construction criteria, functionality, use, properties or other characteristics of the equipment, systems, or production lines into which the Products may be incorporated, including any safety, fail-safe and shut down systems using the Products.
- b. MELCO is not responsible for determining the suitability of the Products for their intended purpose and use, including determining if the Products provide appropriate safety margins and redundancies for the applications, equipment or systems into which they are incorporated.
- c. Customer acknowledges that qualified and experienced personnel are required to determine the suitability, application, design, construction and proper installation and integration of the Products. MELCO does not supply such personnel.
- d. MELCO is not responsible for designing and conducting tests to determine that the Product functions appropriately and meets application standards and requirements as installed or incorporated into the end-user's equipment, production lines or systems.
- e. MELCO does not warrant any Product:
 - (1) repaired or altered by persons other than MELCO or its authorized engineers or FA Centers;
 - (2) subjected to negligence, carelessness, accident, misuse, or damage;
 - (3) improperly stored, handled, installed or maintained;
 - (4) integrated or used in connection with improperly designed, incompatible or defective hardware or software;
 - (5) that fails because consumable parts such as batteries, backlights, or fuses were not tested, serviced or replaced;
 - (6) operated or used with equipment, production lines or systems that do not meet applicable and commensurate legal, safety and industry-accepted standards;
 - (7) operated or used in abnormal applications;
 - (8) installed, operated or used in contravention of instructions, precautions or warnings contained in MELCO's user, instruction and/or safety manuals, technical bulletins and guidelines for the Products;
 - (9) used with obsolete technologies or technologies not fully tested and widely accepted and in use at the time of the Product's manufacture;
 - (10) subjected to excessive heat or moisture, abnormal voltages, shock, excessive vibration, physical damage or other improper environment; or
 - (11) damaged or malfunctioning due to Acts of God, fires, acts of vandals, criminals or terrorists, communication or power failures, or any other cause or failure that results from circumstances beyond MELCO's control.
- f. All Product information and specifications contained on MELCO's website and in catalogs, manuals, or technical information materials provided by MELCO are subject to change without prior notice.

3. Limits on Damages.

- a. MELCO'S MAXIMUM CUMULATIVE LIABILITY BASED ON ANY CLAIMS FOR BREACH OF WARRANTY OR CONTRACT, NEGLIGENCE, STRICT TORT LIABILITY OR OTHER THEORIES OF RECOVERY REGARDING THE SALE, REPLACEMENT, DELIVERY, PERFORMANCE, CONDITION, SUITABILITY, COMPLIANCE, OR OTHER ASPECTS OF THE PRODUCTS OR THEIR SALE, INSTALLATION OR USE SHALL BE LIMITED TO THE PRICE PAID FOR PRODUCTS NOT AS WARRANTED.
- b. Although MELCO has obtained the certification for Product's compliance to the international safety standards IEC61508 and EN954-1/ISO13849-1 from TUV Rheinland, this fact does not guarantee that Product will be free from any malfunction or failure. The user of this Product shall comply with any and all applicable safety standard, regulation or law and take appropriate safety measures for the system in which the Product is installed or used and shall take the second or third safety measures other than the Product. MELCO is not liable for damages that could have been prevented by compliance with any applicable safety standard, regulation or law.
- c. MELCO prohibits the use of Products with or in any application involving power plants, trains, railway systems, airplanes, airline operations, other transportation systems, amusement equipments, hospitals, medical care, dialysis and life support facilities or equipment, incineration and fuel devices, handling of nuclear or hazardous materials or chemicals, mining and drilling, and other applications where the level of risk to human life, health or property are elevated.
- d. MELCO SHALL NOT BE LIABLE FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT OR PUNITIVE DAMAGES, FOR LOSS OF PROFITS, SALES, OR REVENUE, FOR INCREASED LABOR OR OVERHEAD COSTS, FOR DOWNTIME OR LOSS OF PRODUCTION, FOR COST OVERRUNS, OR FOR ENVIRONMENTAL OR POLLUTION DAMAGES OR CLEAN-UP COSTS, WHETHER THE LOSS IS BASED ON CLAIMS FOR BREACH OF CONTRACT OR WARRANTY, VIOLATION OF STATUTE, NEGLIGENCE OR OTHER TORT, STRICT LIABILITY OR OTHERWISE.
- e. In the event that any damages which are asserted against MELCO arising out of or relating to the Products or defects in them, consist of personal injury, wrongful death and/or physical property damages as well as damages of a pecuniary nature, the disclaimers and limitations contained in these terms shall apply to all three types of damages to the fullest extent permitted by law. If, however, the personal injury, wrongful death and/or physical property damages cannot be disclaimed or limited by law or public policy to the extent provided by these terms, then in any such event the disclaimer of and limitations on pecuniary or economic consequential and incidental damages shall nevertheless be enforceable to the fullest extent allowed by law.
- f. In no event shall any cause of action arising out of breach of warranty or otherwise concerning the Products be brought by Customer more than one year after the cause of action accrues.
- g. Each of the limitations on remedies and damages set forth in these terms is separate and independently enforceable, notwithstanding the unenforceability or failure of essential purpose of any warranty, undertaking, damage limitation, other provision of these terms or other terms comprising the contract of sale between Customer and MELCO.

4. Repair

Please note that this product cannot be repaired.

5. Discontinuation of Production

- a. Discontinuation of production shall be notified with Mitsubishi Technical Bulletins, etc.
- b. Product supply (including repair parts) is not available after production is discontinued.

6. Overseas Service

Overseas, please contact Mitsubishi's local overseas FA Center.

7. Delivery/Force Majeure.

- a. Any delivery date for the Products acknowledged by MELCO is an estimated and not a promised date. MELCO will make all reasonable efforts to meet the delivery schedule set forth in Customer's order or the purchase contract but shall not be liable for failure to do so.
- b. Products stored at the request of Customer or because Customer refuses or delays shipment shall be at the risk and expense of Customer.
- c. MELCO shall not be liable for any damage to or loss of the Products or any delay in or failure to deliver, service, or replace the Products arising from shortage of raw materials, failure of suppliers to make timely delivery, labor difficulties of any kind, earthquake, fire, windstorm, flood, theft, criminal or terrorist acts, war, embargoes, governmental acts or rulings, loss or damage or delays in carriage, acts of God, vandals or any other circumstances reasonably beyond MELCO's control.

8. Choice of Law/Jurisdiction.

These terms and any agreement or contract between Customer and MELCO shall be governed by the laws of the State of New York without regard to conflicts of laws. To the extent any action or dispute is not arbitrated, the parties consent to the exclusive jurisdiction and venue of the federal and state courts located in the Southern District of the State of New York. Any judgment there obtained may be enforced in any court of competent jurisdiction.

9. Arbitration.

Any controversy or claim arising out of, or relating to or in connection with the Products, their sale or use or these terms, shall be settled by arbitration conducted in accordance with the Center for Public Resources (CPR) Rules for Non-Administered Arbitration of International Disputes, by a sole arbitrator chosen from the CPR's panels of distinguished neutrals. Judgment upon the award rendered by the Arbitrator shall be final and binding and may be entered by any court having jurisdiction thereof. The place of the arbitration shall be New York City, New York. The language of the arbitration shall be English. The neutral organization designated to perform the functions specified in Rule 6 and Rules 7.7(b), 7.8 and 7.9 shall be the CPR.

INFORMATION AND SERVICES

For further information and services, please contact your local Mitsubishi Electric sales office or representative.
Visit our website to find our locations worldwide.

mitsubishi electric Factory Automation Global Website

Locations Worldwide

www.MitsubishiElectric.com/fa/about-us/overseas/

TRADEMARKS

The company names, system names and product names mentioned in this manual are either registered trademarks or trademarks of their respective companies.

In some cases, trademark symbols such as '™' or '®' are not specified in this manual.

molex Molex, LLC www.molex.com

SH(NA)-082444ENG-C(2412)MEE

MODEL: RJ71SEIP91-U-E

MITSUBISHI ELECTRIC CORPORATION

HEAD OFFICE: TOKYO BLDG., 2-7-3, MARUNOUCHI, CHIYODA-KU, TOKYO 100-8310, JAPAN
NAGOYA WORKS: 1-14, YADA-MINAMI 5-CHOME, HIGASHI-KU, NAGOYA 461-8670, JAPAN

When exported from Japan, this manual does not require application to the
Ministry of Economy, Trade and Industry for service transaction permission.

Specifications subject to change without notice.