MITSUBISHI ELECTRIC

Programmable Controller

MELSEC iQ-R series

MELSEC iQ-R OPC UA Server Module User's Manual (Application)

-RD81OPC96
-SW1DND-ROPCUA-E (MX OPC UA Module Configurator-R)

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 for the programmable controller system, refer to MELSEC iQ-R Module Configuration Manual.

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.

[Design Precautions]

⚠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.
- For the operating status of each station after a communication failure, refer to manuals relevant to the network. 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.
- 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.

[Design Precautions]

⚠WARNING

- 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.
- 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.
- To maintain the safety of the programmable controller system against unauthorized access from external devices via the network, take appropriate measures. To maintain the safety against unauthorized access via the Internet, take measures such as installing a firewall.

[Design Precautions]

⚠CAUTION

- Do not install the control lines or communication cables together with the main circuit lines or power cables. Keep a distance of 100 mm or more between them. Failure to do so may result in malfunction due to noise.
- 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 do not reset the CPU module while the settings are being written. Doing so will make the data in the flash ROM or SD memory card undefined. The values need to be set in the buffer memory and written to the flash ROM or the SD memory card again. Doing so 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 in Program" for "Open Method Setting" of "Module Parameter". If "OPEN in 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.

[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 general specifications written in Safety Guidelines included in the base unit. 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, and make sure to fix the module with screws since this module has no module fixing hook. Incorrect interconnection may cause malfunction, failure, or drop of the module.
- Tighten the screws within the specified torque range. Undertightening can cause drop of the screw, short circuit, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, or malfunction.
- 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 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.
- 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 the included terminal cover to the module before turning it on for operation. Failure to do so may result in electric shock.

[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. Keep a distance of 100 mm or more between them. Failure to do so may result in malfunction due to noise.
- 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.
- A protective film is attached to the top of the module to prevent foreign matter, such as wire chips, from entering the module during wiring. Do not remove the film during wiring. Remove it for heat dissipation before system operation.

[Wiring Precautions]

⚠CAUTION

- 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 or 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.

[Startup and Maintenance Precautions]

⚠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) more than 25cm 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
- 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.

[Startup and Maintenance Precautions]

⚠CAUTION

- Before handling the module, touch a conducting object such as a grounded metal to discharge the static electricity from the human body. Failure to do so may cause the module to fail or malfunction.

[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 or SD memory card undefined. The values need to be set in the buffer memory and written to the flash ROM or 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.

CONDITIONS OF USE FOR THE PRODUCT

(1) Mitsubishi programmable controller ("the PRODUCT") shall be used in conditions;
i) where any problem, fault or failure occurring in the PRODUCT, if any, shall not lead to any major or serious accident; and
ii) where the backup and fail-safe function are systematically or automatically provided outside of the PRODUCT for the case of any problem, fault or failure occurring in the PRODUCT.

(2) The PRODUCT has been designed and manufactured for the purpose of being used in general industries.
MITSUBISHI SHALL HAVE NO RESPONSIBILITY OR LIABILITY (INCLUDING, BUT NOT LIMITED TO ANY AND ALL RESPONSIBILITY OR LIABILITY BASED ON CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY) FOR ANY INJURY OR DEATH TO PERSONS OR LOSS OR DAMAGE TO PROPERTY CAUSED BY the PRODUCT THAT ARE OPERATED OR USED IN APPLICATION NOT INTENDED OR EXCLUDED BY INSTRUCTIONS, PRECAUTIONS, OR WARNING CONTAINED IN MITSUBISHI'S USER, INSTRUCTION AND/OR SAFETY MANUALS, TECHNICAL BULLETINS AND GUIDELINES FOR the PRODUCT.
("Prohibited Application")
Prohibited Applications include, but not limited to, the use of the PRODUCT in;

- Nuclear Power Plants and any other power plants operated by Power companies, and/or any other cases in which the public could be affected if any problem or fault occurs in the PRODUCT.
- Railway companies or Public service purposes, and/or any other cases in which establishment of a special quality assurance system is required by the Purchaser or End User.
- Aircraft or Aerospace, Medical applications, Train equipment, transport equipment such as Elevator and Escalator, Incineration and Fuel devices, Vehicles, Manned transportation, Equipment for Recreation and Amusement, and Safety devices, handling of Nuclear or Hazardous Materials or Chemicals, Mining and Drilling, and/or other applications where there is a significant risk of injury to the public or property.

Notwithstanding the above restrictions, Mitsubishi may in its sole discretion, authorize use of the PRODUCT in one or more of the Prohibited Applications, provided that the usage of the PRODUCT is limited only for the specific applications agreed to by Mitsubishi and provided further that no special quality assurance or fail-safe, redundant or other safety features which exceed the general specifications of the PRODUCTs are required. For details, please contact the Mitsubishi representative in your region.

INTRODUCTION

Thank you for purchasing the Mitsubishi Electric MELSEC iQ-R series programmable controllers.
This manual describes the functions, configuration tool, and troubleshooting to use the modules 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.
Please make sure that the end users read this manual.

Point

The program examples shown in this manual are the examples in which OPC UA server module (RD81OPC96) is assigned to the input/output No. X/Y0 to X/Y1F unless otherwise specified. To use the program examples shown in this manual, the input/output number assignment is required. For details on the assignment of input/output number, refer to the following manual.
MELSEC iQ-R Module Configuration Manual

Relevant product

RD81OPC96

CONTENTS

RELEVANT MANUALS

Manual name [manual number]	Description	Available form
MELSEC iQ-R OPC UA Server Module User's Manual (Application) [SH-081694ENG] (this manual)	Explains the functions, configuration tool, parameter setting, troubleshooting, I/O signal, and buffer memory of an OPC UA server module.	Print book
		e-Manual PDF
MELSEC iQ-R OPC UA Server Module User's Manual (Startup) [SH-081693ENG]	Explains the specifications, procedure before operation, wiring, and operation examples of an OPC UA server module.	Print book
		e-Manual PDF

Point

e-Manual refers to the Mitsubishi Electric FA electronic book manuals that can be browsed using a dedicated tool.

e-Manual has the following features:

- Required information can be cross-searched in multiple manuals.
- Other manuals can be accessed from the links in the manual.
- Hardware specifications of each part can be found from the product figures.
- Pages that users often browse can be bookmarked.
- Sample programs can be copied to an engineering tool.

TERMS

Unless otherwise specified, this manual uses the following terms.

Term	Description
Address space	Data that contains information of an access target device, a group, and a tag.
Anonymous	A user who do not use both an account name and a password.
Application certificate	A client certificate used for application authentication in OPC UA communication. It can be uploaded to the trust list in the "Manage Application Certificate" screen of the configuration tool.
Certificate authority	An authority that registers, issues, and revokes electronic certificates.
Certificate revocation list	A certificate revocation list managed by a certificate authority.
Clamping	Controlling values in the range of set upper and lower limit values.
Client certificate	The certificate of an OPC UA client used for OPC UA communication. A generic term for user certificates and application certificates.
Configuration tool	An abbreviation for MX OPC UA Module Configurator-R.
Discovery server	A server that manages endpoints of each OPC UA server on a network.
Endpoint	A server or client connected at the end of network. It physically refers to a personal computer or OPC UA server module at the end.
Engineering tool	A tool used for setting up programmable controllers, programming, debugging, and maintenance. For the supported tools, refer to the following: MELSEC iQ-R Module Configuration Manual
Issuers authentication	An authentication method using an electronic certificate issued by a certificate authority. Communication with higher security than a normal authentication method is available.
MX OPC UA Module Configurator-R	A product name for SW1DND-ROPCUA-E.
OPC	An abbreviation for OLE for Process Control. An interoperability standard for the secure and reliable exchange of data in an industrial automation field and in other industries.
OPC UA	An abbreviation for OPC Unified Architecture. Platform independent service-oriented architecture that integrates all the functionality of each OPC Classic specification into an extensible framework.
OPC UA server module	An abbreviation for RD81OPC96 OPC UA server modules.
Server certificate	The certificate of an OPC UA server used for application authentication in OPC UA communication.
Tag	Information to access device data of the CPU module of the own station or a CPU module on a network from an OPC UA client.
User certificate	A client certificate used for user authentication in OPC UA communication. A certificate can be uploaded to the trust list in the "Manage User Certificate" screen of the configuration tool.

For definitions of terms for safety CPUs, refer to the following:

MELSEC iQ-R CPU Module User's Manual (Application)

1 FUNCTIONS

This chapter explains the details of the OPC UA server module functions.

1.1 OPC UA Server Functions

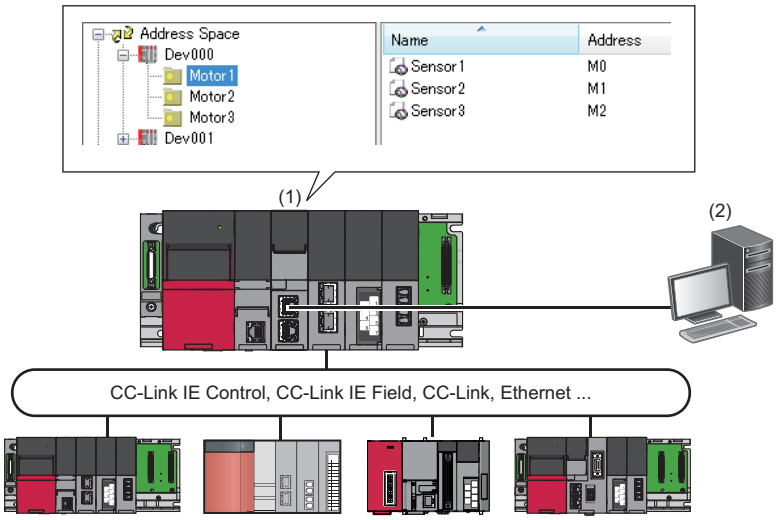
Data Access function

This function is to access tags registered in the address space set in the configuration tool (devices of the CPU module of the own station or a CPU module on a network) and structure labels*1 from an OPC UA client.

*1 Members of a structure are used as tags.

A tag value registered in the address space is updated based on a set polling cycle.

A function related to Data Access supports 'Standard DataChange Subscription Server Facet' of the OPC UA specifications.



(1) OPC UA server module
(2) OPC UA client

Setting method

For the setting method of the address space, refer to the following:

☞ Page 23 Address Space Setting

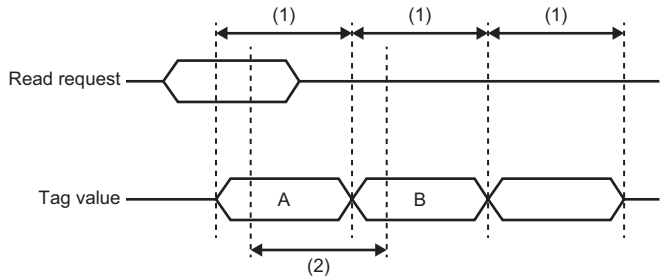
Data type

For accessible data types, refer to the following:

MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

Timing to read data in an OPC UA client (Read)

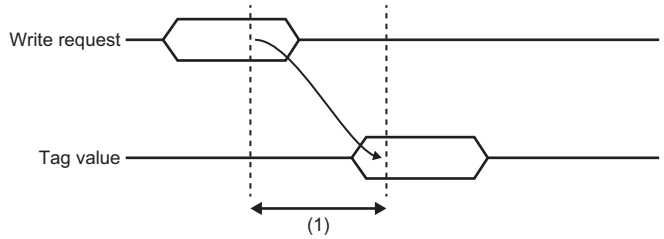
When an OPC UA client requests to read a tag value in the address space, a tag value at the time when the communication time and the OPC UA processing time elapse from the request timing is read.



A: Tag value at the request timing of an OPC UA client
B: Tag value to notify an OPC UA client
(1) Polling cycle
(2) Communication time + OPC UA processing

Timing to write data from an OPC UA client (Write)

When an OPC UA client requests to write a tag value in the address space, the tag value is written when the communication time and the OPC UA processing time elapse from the request timing.



(1) Communication time + OPC UA processing

Security function

This function prevents an OPC UA server module from being stolen, falsified, operated incorrectly, and executed improperly due to unauthorized access from a third party.

For the security setting for an OPC UA server which runs on an OPC UA server module, refer to the following:

☞ Page 48 OPC UA Server Setting

User authentication function

This function controls access to an OPC UA server module to prevent unauthorized access by users other than specific users.

■Authentication with a user name and password

Authentication with a user name and password is performed when accessing an OPC UA server module from the configuration tool or an OPC UA client.

Item	Specification	Setting method
Number of users	Up to 16 users	☞ Page 44 Security Setting
User Name	Length: Up to 32 characters	
Password	Length: Up to 32 characters	
Default user	User name: RD81OPC96 Password: MITSUBISHI	

■Authentication with a certificate

Authentication with a certificate is performed when accessing an OPC UA server module from an OPC UA client.

For details on the setting method, refer to the following:

☞ Page 44 Security Setting

Conversion function

The conversion function converts device values and values in the engineering unit.

Device values and values in the engineering unit are converted by specifying their ranges.

Conversion type

The following table shows the available conversion for an OPC UA server module.

Conversion type	Description	Setting method
None (Double type)	To convert values to Double type. (Values themselves are not converted.) The engineering unit (EU) and a device value (IR) cannot be set.	☞ Page 39 Conversion Definition Setting
Linear	To convert values by using a linear function.	
Square root	To convert values by using a quadratic function.	

Linear function conversion

The following formula is used for linear function conversion (linear conversion).

■When reading a value from a device

$$y = E_{Min} + \frac{(E_{Max} - E_{Min}) \times (x - R_{Min})}{(R_{Max} - R_{Min})}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

■When writing a value to a device

$$x = R_{Min} + \frac{(y - E_{Min}) \times (R_{Max} - R_{Min})}{(E_{Max} - E_{Min})}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

Quadratic function conversion

The following formula is used for quadratic function conversion (square-root conversion).

■When reading a value from a device

$$y = E_{Min} + \frac{(E_{Max} - E_{Min}) \times \sqrt{(x - R_{Min})}}{\sqrt{(R_{Max} - R_{Min})}}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

■When writing a value to a device

$$x = R_{Min} + \frac{(y - E_{Min})^2 \times (R_{Max} - R_{Min})}{(E_{Max} - E_{Min})^2}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

Clamping

When "Linear" or "Square Root" is selected for "Conversion Type", values in the engineering unit exceeding the setting range after conversion can be rounded to a specified range by clamping. Note that clamping is not performed for writing.

The following table shows the clamping types that can be specified for an OPC UA server module.

Clamping type	Description
None	No clamping.
Engineering Unit	The minimum value and the maximum value of the engineering unit are set as the clamp values.
Details	A specified minimum value and maximum value are set as clamp values.

1.2 Other Functions

Self-diagnostic function

This function performs the self-diagnostic test to check the hardware of an OPC UA server module.

The following tests are included in the self-diagnostics.

- ☞ Page 80 Automatic hardware test
- ☞ Page 81 Hardware test for LED check

SD memory card format function

This function formats an SD memory card.

After formatting an SD memory card, the volume label will be 'RD81OPC96'.

The operating status of an OPC UA server module will be in "STOP" state after formatting.

For the formatting method, refer to the following:

☞ Page 68 SD memory card diagnostic

2 MX OPC UA Module Configurator-R

This chapter explains MX OPC UA Module Configurator-R.

2.1 MX OPC UA Module Configurator-R

MX OPC UA Module Configurator-R is a tool to set the OPC UA server setting of an OPC UA server module.
For the startup method and screen configuration for MX OPC UA Module Configurator-R, refer to the following:
MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

2.2 Project File Handling

This section explains how to handle a project file.

Creating a new project

Create a new project.
The project being edited is discarded.

Operating procedure

1. Select [File] ⇨ [New].

Opening a project

Read a saved project.

Operating procedure

1. Select [File] ⇨ [Open Project].
2. Select a target file in the "Open" screen, then click the [Open] button.

Saving a project

Save a setting being edited to a project file.

Saving a project

Operating procedure

1. Select [File] ⇨ [Save].

Naming and saving a project

Operating procedure

1. Select [File] ⇨ [Save as].
2. Specify a save location and file name in the "Save as" screen, then click the [Save] button.

Opening a recently opened project file

Select a recently opened project file to open.

Operating procedure

1. Select [File] ⇨ [(recently opened project)].

2.3 Address Space Setting

Address space (access target device) setting

The following shows the screen to set an access target device accessed by an OPC UA server module.

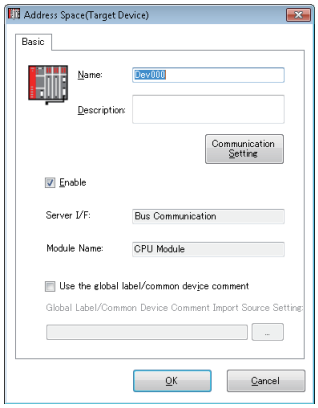
Window

■When newly adding

1. Select "Address Space" in the tree view.
2. Select [Edit] ⇨ [New Target Device].

■When editing

1. Double-click an item ( ) under "Address Space" in the tree view.



Displayed items

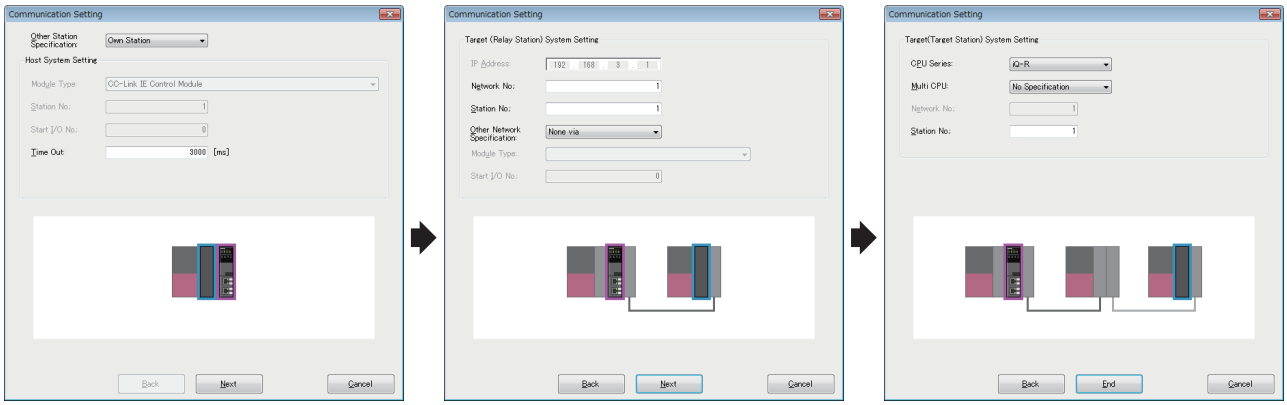
Item	Description
Name	Set the name of an access target device (up to 50 characters).
Description	Set the description of an access target device (up to 128 characters).
[Communication Setting] button	Click this to open the "Communication Setting" screen. ☞ Page 24 Communication setting
Enable	Select the checkbox to enable the connection to an access target device.
Server I/F	The setting content of a communication route is displayed.
Module Name	The setting content of the module type of an access source system is displayed.
Use the global label/common device comment	Select the checkbox to use the global label and common device comment import function. ☞ Page 50 Global Label and Common Device Comment Import Function
Global Label/Common Device Comment Import Source Setting	The path of a project created in an engineering tool specified as an import source is displayed. Specify an import source project in the "Select the Global Label/Common Device Comment Import Source Project" screen displayed by clicking the [...] button.

Communication setting

The following shows the screen to set a connection route to access a device from an OPC UA server module.

Window

Click the [Communication Setting] button in the "Address Space(Target Device)" screen.



Displayed items

Item		Description
Other Station Specification		Select "Own Station" when accessing a device on the system on which an OPC UA server module is mounted. Select "Other Station" when accessing a device connected via a network.
Host System Setting	Module Type	Select the type of a module on the access source system side.
	Station No.	Set the station number of a module on the access source system side.
	Start I/O No.	Set the start I/O number of a module on the access source system side.
	Time Out	Set a communication timeout time.
Target (Relay Station) System Setting	IP Address*1	Set the IP address of a module on the access target (relay station) system side.
	Network No.*2	Set the network number of a module on the access target (relay station) system side.
	Station No.*3	Set the station number of a module on the access target (relay station) system side.
	Other Network Specification	Select "Via Other System" when accessing another network via a system set in the access target (relay station) system side setting.
	Module Type*4,*5	Select the type of a module on the routed system side.
	Start I/O No.*6	Set the start I/O number of a module on the routed system side.
Target (Target Station) System Setting	CPU Series	Select the series of an access target CPU module.
	Multi CPU	Select the CPU number when an access target CPU is in a multiple CPU system.
	Network No.*7	Set the network number of a module on the access target (target station) system side.
	Station No.	Set the station number of a module on the access target (target station) system side.

*1 Can be set when any of the following items is selected for "Module Type" in "Host System Setting".
Built-in Ethernet Port [CH2](Connect to the Ethernet module)
Built-in Ethernet Port [CH2] (Connect to the CPU module (Ethernet port))

*2 Can be set when any of the following items is selected for "Module Type" in "Host System Setting".
Built-in Ethernet Port [CH2](Connect to the Ethernet module)
Ethernet Module
CC-Link IE Control Module
CC-Link IE Field Module

*3 Can be set when any of the following items is selected for "Module Type" in "Host System Setting".
Built-in Ethernet Port [CH2](Connect to the Ethernet module)
Ethernet Module
CC-Link IE Control Module
CC-Link IE Field Module
CC-Link Module

*4 Can be set when "Via Other System" is selected for "Other Network Specification".

*5 Any of the following items can be selected depending on an item selected for "Module Type" in "Host System Setting".
"Built-in Ethernet Port [CH2](Connect to the Ethernet module)" is selected: Ethernet/CC-Link IE Control/CC-Link IE Field
"Built-in Ethernet Port [CH2](Connect to the CPU module (Ethernet port))" or "CC-Link Module" is selected: Ethernet Module, CC-Link IE Control Module, or CC-Link IE Field Module
"Ethernet Module", "CC-Link IE Control Module", or "CC-Link IE Field Module" is selected: CC-Link Module

*6 Can be set when any of the following items is selected for "Module Type" in "Host System Setting" and "Via Other System" is selected for "Other Network Specification".
Ethernet Module
CC-Link IE Control Module
CC-Link IE Field Module

*7 Can be set when any of the following items is selected for "Module Type" in "Target (Relay Station) System Setting".
Ethernet/CC-Link IE Control/CC-Link IE Field
Ethernet Module
CC-Link IE Control Module
CC-Link IE Field Module

Address space (tag) setting

The following shows the screen to set a tag accessed by an OPC UA server module.

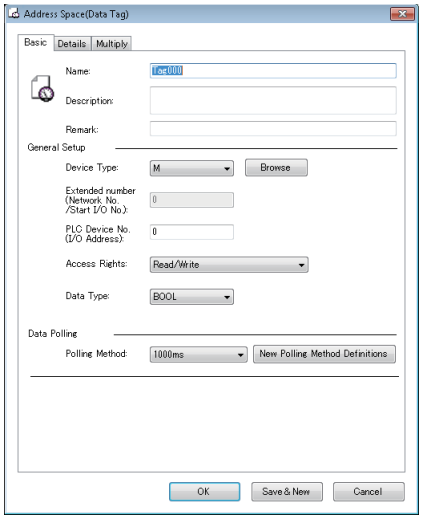
Window

■When newly adding

1. Select an item (or) under "Address Space" in the tree view.
2. Select [Edit] ⇨ [New Data Tag].

■When editing

1. Select an item (or) under "Address Space" in the tree view.
2. Double-click an item ( ) in the list view.



Displayed items

■[Basic] tab

Item		Description
Name		Set the name of a tag (up to 50 characters).
Description		Set the description of a tag (up to 128 characters).
Remark		Set a remark of a tag (up to 128 characters).
General Setup	Device Type	Select a device type. It can also be selected in the "Support Devices" screen displayed by clicking the [Browse] button.
	Extended number (Network No./Start I/O No.)	Set the extended number (n) of the following devices: • Link direct device (Jn\X, Jn\Y, Jn\B, Jn\SB, Jn\W, Jn\SW)*1 • Module access device (Un\G, U3En\G)*2 • CPU buffer memory (U3En\G, U3En\HG)*2
	PLC Device No. (IO Address)	Set the I/O address of an access target.
	Access Rights	Select an access right.
	Data Type	Select a data type. When an extended data type is set in the [Details] tab, the data type corresponding to the setting is displayed.
Data Polling	Polling Method	Select a polling method.
	[New Polling Method Definitions] button	Click this to open the "Polling Method Definitions" screen. ☞ Page 41 Polling Definition Setting
[Save & New] button		Click this to save the setting and display a new tag. • A sequential number is added to the name of a new tag. (Tag→Tag1→Tag2)*3 • When the last character of a tag name is a number, it is incremented. (Tag000→Tag001→Tag002)*3 • The number displayed in the field for "PLC Device No. (IO Address)" is incremented. (M0→M1→M2)

*1 'n' indicates the network number.
*2 'n' indicates the start I/O number.
*3 When a number to be added already exists, the number is skipped and the next available number is added.

■[Details] tab

Item		Description
General Setup	Enable Tag	Select the checkbox to enable the tag.
Data Conversion	Swap Word/Byte Order	Select the checkbox to swap the order of bytes in data. The data type of a device is WORD type: B1/B2 ↔ B2/B1 The data type of a device is LONGWORD type: B1/B2 B3/B4 ↔ B4/B3 B2/B1
	Convert to word*1	Select the checkbox to convert a tag value to the word size or double-word size when reading data from or writing data to an OPC UA client is requested. ■INT type tag • Reading: Data is converted to the double-word size and read from an OPC UA client. (A sign is considered.) • Writing: Data is converted to the word size and written to a tag. ■DINT type tag • Reading: Data is converted to the word size and read from an OPC UA client. • Writing: Data is converted to the double-word size and written to a tag. (A sign is considered.)
	Use Conversion	Select the checkbox to use a conversion definition.
	Conversion	Select a conversion definition.
	[New Conversion Definitions] button	Click this to open the "Conversion Definitions" screen. ☞ Page 39 Conversion Definition Setting
Extended Data Type	Use Advanced Type	Select the checkbox to use an extended type (array, character string).
	Extended Data Type	Select an extended data type.
	Number of elements*2	Set the number of elements of an array.
	Data Length (character number)	Set the number of characters of a character string.
[Save & New] button		Click this to save the setting and display the screen to set a new tag. • A sequential number is added to the name of a new tag. (Tag→Tag1→Tag2)*3 • When the last character of a tag name is a number, it is incremented. (Tag000→Tag001→Tag002)*3 • The number displayed in the field for "PLC Device No. (IO Address)" is incremented. (M0→M1→M2)

*1 Can be set when the data type of a member of the selected structure is any of the following:
INT
UINT
DINT
UDINT

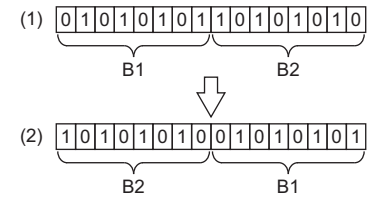
*2 Up to 128 elements can be set for an array.
[Number of elements in the first dimension] × [Number of elements in the second dimension] × [Number of elements in the third dimension] ≤ 128

*3 When a number to be added already exists, the number is skipped and the next available number is added.

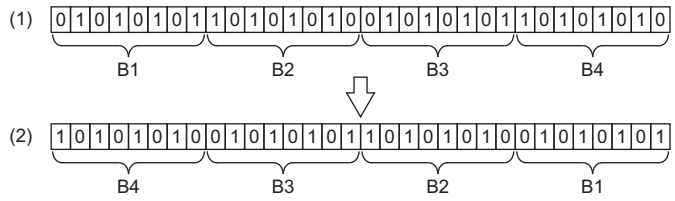
Ex.

The following shows examples for swapping the order of bytes.

<WORD>



<LONGWORD>



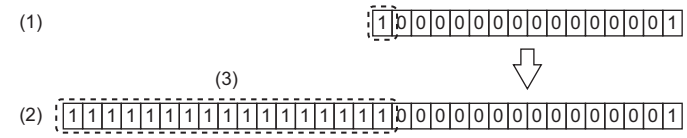
(1) Tag value

(2) Value in an OPC UA client

Ex.

The following shows examples of converting an INT type tag into the word size.

Reading

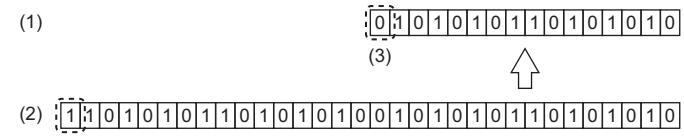


(1) Tag value

(2) Value in an OPC UA client

(3) Sign (considered)

Writing



(1) Tag value

(2) Value in an OPC UA client

(3) Sign (not considered)

■[Multiply] tab

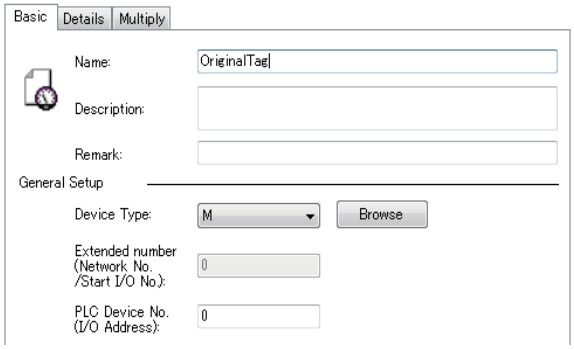
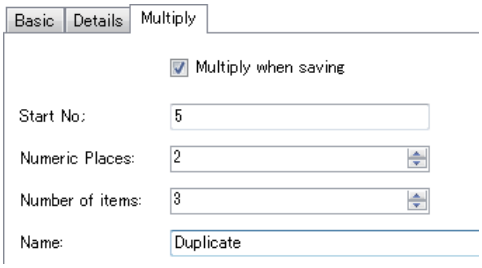
Item	Description
Multiply when saving	Select the checkbox to duplicate a tag when saving.
Start No.	Set the start number of a number added to a tag name when duplicating.
Numeric Places	Set the number of digits in the numeric part of a tag name.
Number of items	Set the number of tags to duplicate.
Name	Enter the base of a tag name.
[Multiply] button	Click this to duplicate a tag while keeping the set contents.
[Save & New] button	Click this to save the setting and display the screen to set a new tag. • A sequential number is added to the name of a new tag. (Tag→Tag1→Tag2)*1 • When the last character of a tag name is a number, it is incremented. (Tag000→Tag001→Tag002)*1 • The number displayed in the field for "PLC Device No. (IO Address)" is incremented. (M0→M1→M2)

*1 When a number to be added already exists, the number is skipped and the next available number is added.

Ex.

The following shows a setting example and tags duplicated based on the setting.

• Tag setting

[Basic] tab	[Multiply] tab
	

• Duplicated tags

Name	Notes	Remark	Enable	Device	Device Data Type
Duplicate05			True	M1	BIT
Duplicate06			True	M2	BIT
Duplicate07			True	M3	BIT
OriginalTag			True	M0	BIT

Structure label setting

The following shows the procedure and screen for setting a structure label in the address space.
The data structure of a structure set in the following section can be created in the address space.
☞ Page 42 Structure Definition Setting

Operating procedure

■When newly adding

1. Select an item (or) under "Address Space" in the tree view.
2. Select [Edit] ⇨ [New Structure Type Declarations].
3. Set each item in the "Structure Label Definitions" screen. (☞ Page 32 Label, Page 33 Address, Page 36 Tag)

■When editing

1. Select an item (or) under "Address Space" in the tree view.
2. Select an item ( ) in the list view, then select [Edit] ⇨ [Properties].
3. Set each item in the "Structure Label Definitions" screen. (☞ Page 32 Label, Page 33 Address, Page 36 Tag)

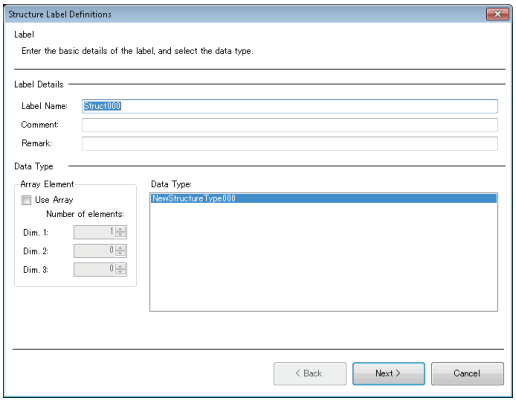
Point

A structure array is displayed with the following icon.

Label

The following shows the screen to set the name and data type of a structure label.

Window



Displayed items

Item			Description
Label Details	Label Name		Set the name of a structure label (1 to 50 characters).
	Comment		Set a comment (up to 128 characters).
	Remark		Set a remark (up to 128 characters).
Data Type	Array Element	Use Array	Select the checkbox to use a structure as an array.
		Number of elements*1	Set the number of elements of each dimension of an array (1 to 128).*2,*3
	Data Type		Select a structure to use for the data type of a structure label. ☞ Page 42 Structure Definition Setting
[Next] button			Click this to move to the next screen. ☞ Page 33 Address

*1 Can be set when the checkbox of "Use Array" is selected.
*2 When a value greater than or equal to '1' is set for "Dim. 1", a value can be set for "Dim. 2".
*3 When a value greater than or equal to '1' is set for "Dim. 2", a value can be set for "Dim. 3".

Precautions

If returning to this screen after setting an address or tag in their screens, then selecting another structure for "Data Type" and clicking the [Next] button, the setting for the address or tag will be initialized.

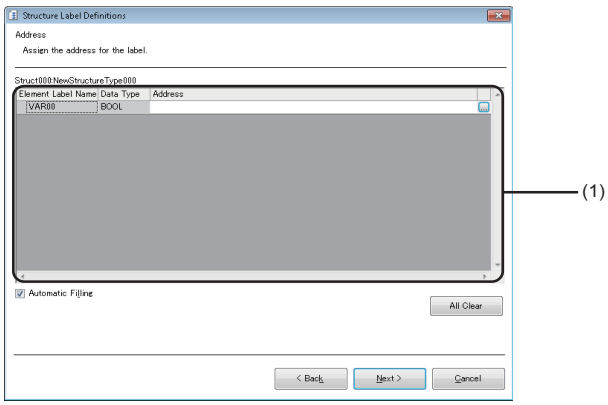
Address

The following shows the screen to assign an address to each member of a structure.

■When the checkbox of "Use Array" is not selected in the screen to set a label

Window

Click the [Next] button in the screen for setting labels.



Displayed items

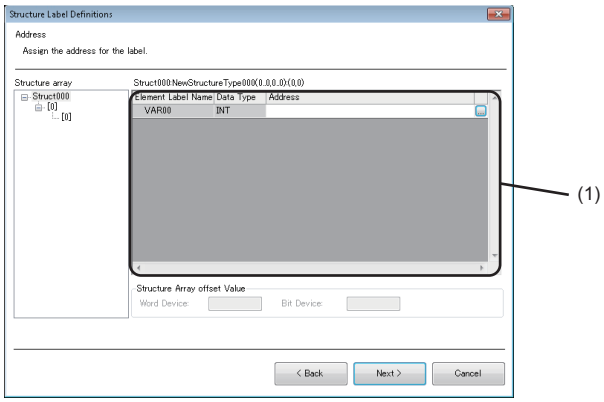
Item		Description
(1) Member list	Element Label Name	The name of a member of the structure is displayed.
	Data Type	The data type of a member of the structure is displayed.
	Address	Set an address to assign to a member of the structure.*1 It can also be set in the "Address Setting" screen displayed by clicking the [...] button. ☞ Page 35 Address setting When selecting the checkbox of "Automatic filling", an address is automatically assigned to the subsequent members*2 of a member for which an address is set.*3,*4,*5,*6
Automatic Filling		Select the checkbox to automatically assign an address*7.
[All Clear] button		Click this to delete addresses in a batch.
[Back] button		Click this to move to the previous screen. ☞ Page 32 Label
[Next] button		Click this to move to the next screen. ☞ Page 36 Tag

*1 If an invalid address is set, it is displayed in red.
*2 Excluding members for which an address is already set. To automatically assign an address, delete an address set for a target member.
*3 Assigned without duplication.
*4 Assigned to a member the data type of which is BOOL when a bit device is set for an address.
*5 Assigned to a member other than one the data type of which is BOOL when a word device is set for an address.
*6 Assigned depending on the size of a data type.
*7 Performed when a valid address is set for any member of a structure. (If the address already set for a member is changed, it is performed when a valid address different from one before the change is set.)

■When the checkbox of "Use Array" is selected in the screen to set a label

Window

Click the [Next] button in the screen for setting labels.



Displayed items

Item		Description
Structure array		Array elements of a structure array are displayed in a tree.
(1) Member list	Element Label Name	The name of a member of the structure is displayed.
	Data Type	The data type of a member of the structure is displayed.
	Address	Set an address to assign to a member of the structure.*1,*2 It can also be set in the "Address Setting" screen displayed by clicking the [...] button. ☞ Page 35 Address setting
Structure Array Offset Value		Set an offset value*3 of a structure array. Regardless of the size of the structure, a round number can be set for the start address of each array element. • Word device: Set an offset value for a member of a word device. • Bit device: Set as an offset value for a member of a bit device.
[Back] button		Click this to move to the previous screen. ☞ Page 32 Label
[Next] button		Click this to move to the next screen. ☞ Page 36 Tag

*1 If an invalid address is set, it is displayed in red.

*2 It can be set only for the following members:
The first member among members the data type of which is BOOL type
The first member among members the data type of which is not BOOL type

*3 Can be set up to 99999.

Ex.

The following table shows examples of addresses if setting an offset value when using the structure array shown below.

Start device: D0, structure size: 13, number of elements: 3

Array element	Address of an array element	
	If an offset value is not set	If an offset value is set to 100
1	D0 to D12	D0 to D12
2	D13 to D25	D100 to D112
3	D26 to D38	D200 to D212

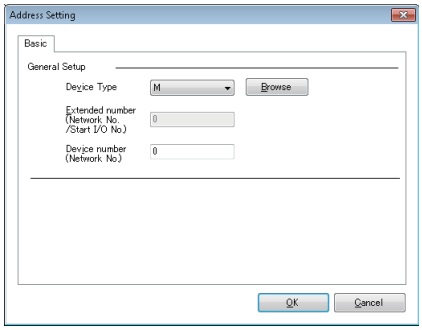
Precautions

Addresses overlap among array elements. Do not set an offset value smaller than the structure size.

■Address setting

Set an address to assign to each member of a structure.

Window



Displayed items

Refer to "General Setup" in the "Address Space(Data Tag)" screen.

Note that the items "Access Rights" and "Data Type" are not displayed.

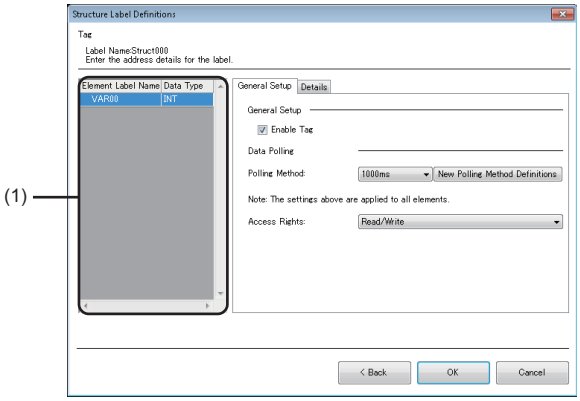
☞ Page 27 [Basic] tab

Tag

The following shows the screen to set details of each member of a structure.

Window

Click the [Next] button in the screen for setting addresses.



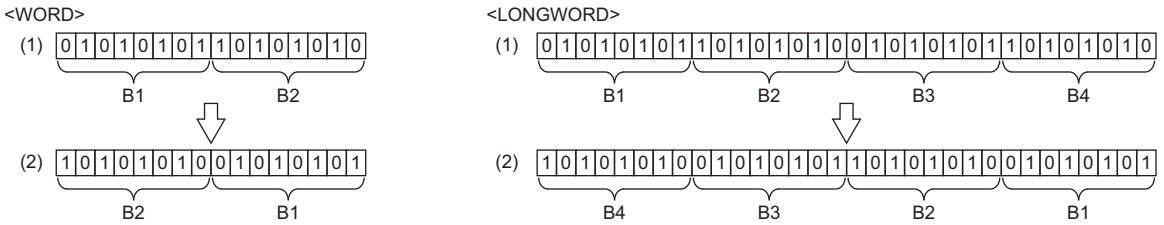
Displayed items

Item		Description
(1) Member list	—	Members of the structure are displayed in a tree. The setting contents of a member selected in the tree are displayed on the right in the screen.
	Element Label Name	The name of a member of the structure is displayed.
	Data Type	The data type of a member of the structure is displayed.
[General Setup] tab	Enable Tag	Select the checkbox to enable the tag. (Applies to all members of the structure.)
	Polling Method	Select a polling definition. (It applies to all members of the structure.)
	[New Polling Method Definitions] button	Click this to open the "Polling Method Definitions" screen. ☞ Page 41 Polling Definition Setting
	Access Rights	Select an access right of a member of the selected structure.
[Details] tab	Swap Word/Byte Order	Select the checkbox to swap the order of bytes in data. The data type of a device is WORD type: B1/B2 ↔ B2/B1 The data type of a device is LONGWORD type: B1/B2 B3/B4 ↔ B4/B3 B2/B1
	Convert to Word*1	Select the checkbox to convert a tag value to the word size or double-word size when reading data from or writing data to an OPC UA client is requested. ■INT type tag • Reading: Data is converted to the double-word size and read from an OPC UA client. (A sign is considered.) • Writing: Data is converted to the word size and written to a tag. ■DINT type tag • Reading: Data is converted to the word size and read from an OPC UA client. • Writing: Data is converted to the double-word size and written to a tag. (A sign is considered.)
	Use Conversion	Select the checkbox to use a conversion definition.
	Conversion	Select a conversion definition.
	[New Conversion Definitions] button	Click this to open the "Conversion Definitions" screen. ☞ Page 39 Conversion Definition Setting
[Back] button		Click this to move to the previous screen. ☞ Page 33 Address

*1 Can be set when the data type of a member of the selected structure is any of the following:
INT
UINT
DINT
UDINT

Ex.

The following shows examples for swapping the order of bytes.



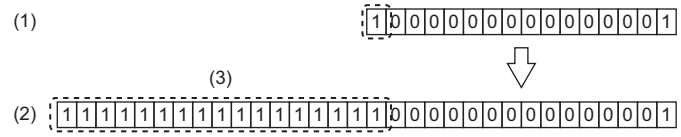
(1) Tag value

(2) Value in an OPC UA client

Ex.

The following shows examples of converting an INT type tag into the word size.

Reading

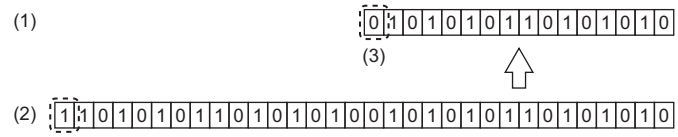


(1) Tag value

(2) Value in an OPC UA client

(3) Sign (considered)

Writing



(1) Tag value

(2) Value in an OPC UA client

(3) Sign (not considered)

Group setting

The following shows the screen to set tags as a group.
A group can also be created as a member of a group.

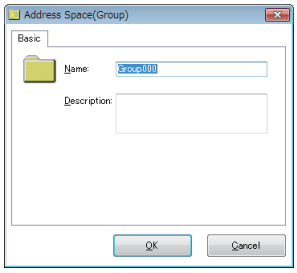
Window

■When newly adding

1. Select an item (or) under "Address Space" in the tree view.
2. Select [Edit] ⇨ [New Group].

■When editing

1. Double-click an item ( ) under "Address Space" in the tree view.



Displayed items

Item	Description
Name	Set the name of a group (up to 50 characters).
Description	Set the description of a group (up to 128 characters).

2.4 Conversion Definition Setting

This section shows the screen to set a definition to convert device values to values in engineering unit.

For conversion, refer to the following:

☞ Page 18 Conversion function

To apply a conversion definition to a tag, refer to the following:

☞ Page 28 [Details] tab

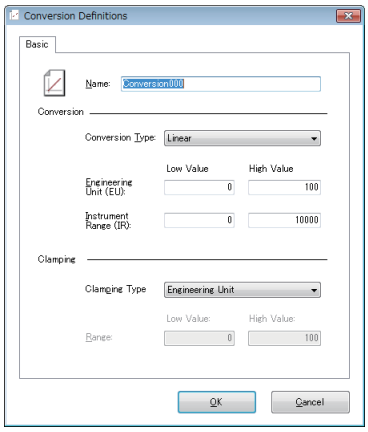
Window

■When newly adding

1. Select "Conversion Definitions" in the tree view.
2. Select [Edit] ⇨ [New Conversion Definitions].

■When editing

1. Select "Conversion Definitions" in the tree view.
2. Double-click an item ( ) in the list view.



Displayed items

Item		Description
Name		Set the name of a conversion definition (up to 50 characters).
Conversion	Conversion Type	Select a conversion type.
	Engineering Unit (EU)*1	Set the maximum value and the minimum value of the engineering unit. Setting range: -1.79769313486231E+308 to 1.79769313486231E+308
	Instrument Range (IR)*1	Set a device value equivalent to the engineering unit. Setting range: -1.79769313486231E+308 to 1.79769313486231E+308
Clamping	Clamping Type	Select a clamping type.
	Range*1	Set the maximum value and the minimum value of clamping. (Range of the Double type) Setting range: -1.79769313486231E+308 to 1.79769313486231E+308

*1 If setting the number of digits of the mantissa part to a value greater than or equal to 16 digits, the setting value will be converted to an exponential notation when clicking the [OK] button. (The 16th digit of the setting value is rounded off.)
(Example) When setting '1234567890123456', the value is converted to '1.23456789012346E+15'.

Precautions

Values exceeding the setting range are not handled in conversion operations.

If a device value is not converted according to either of the formulas shown in the following sections, review the setting value.

☞ Page 18 Linear function conversion, Page 19 Quadratic function conversion

Ex.

The following shows the example for each clamp type when converting the device value 3000 according to the following specification.

Conversion type: Linear

Range of the engineering unit (EU): 0 to 400

Range of the device value (IR): 0 to 2000

Clamping Type	Range	Value after conversion
None	—	600
Engineering Unit	0 to 400 (range of the engineering unit (EU))	400
Details	0 to 200	200

2.5 Polling Definition Setting

This section shows the screen to set a cycle for polling performed by an OPC UA server module to an access target device.
To apply a polling definition to a tag, refer to the following:
☞ Page 27 [Basic] tab

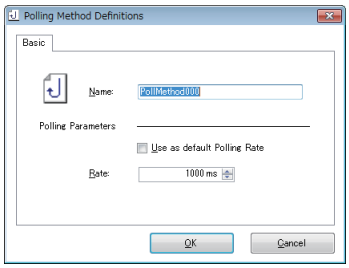
Window

■When newly adding

1. Select "Polling Method Definitions" in the tree view.
2. Select [Edit] ⇨ [New Polling Method Definitions].

■When editing

1. Select "Polling Method Definitions" in the tree view.
2. Double-click an item ( ) in the list view.



Displayed items

Item		Description
Name		Set the name of a polling definition (up to 50 characters).
Polling Parameters	Use as default Polling Rate	Select the checkbox to use it as an initial setting.
	Rate	Set a polling cycle.

2.6 Structure Definition Setting

This section shows the screen to set a structure that can be used for the data type of a structure label in the address space.
For structure labels, refer to the following:
☞ Page 31 Structure label setting

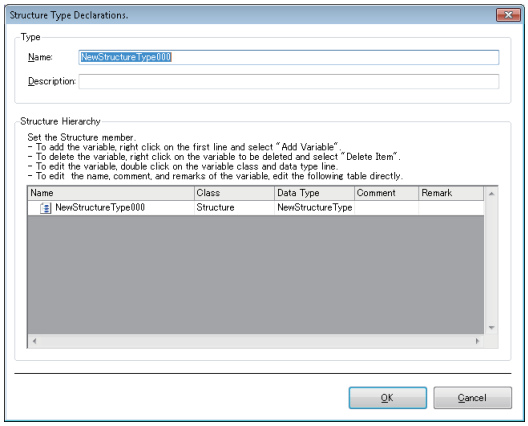
Window

■When newly adding

1. Select "Structure Type Declarations" in the tree view.
2. Select [Edit] ⇨ [New Structure Type Declarations].

■When editing

1. Select "Structure Type Declarations" in the tree view.
2. Select an item ( ) in the list view, then select [Edit] ⇨ [Properties].



Displayed items

Item		Description
Type	Name	Set the name of a structure (1 to 50 characters). When changing this item, the content in "Name" of the structure in the first row in "Structure Hierarchy" is also changed.
	Description	Set a description of the structure (up to 128 characters). When changing this item, the content in "Comment" of the structure in the first row in "Structure Hierarchy" is also changed.
Structure Hierarchy	—	Data structure of a structure is displayed in a tree. A member can be added in the "Add Variable" screen displayed by right-clicking the first row in the structure hierarchy and selecting [Add Variable]. ☞ Page 43 Adding a member
	Name	The name of a member of the structure is displayed. Double-click to edit the name (1 to 50 characters).
	Class	The class of a member of the structure is displayed. Double-click to open the "Add Variable" screen and change the class. ☞ Page 43 Adding a member
	Data Type	The data type of a member of the structure is displayed. Double-click to open the "Add Variable" screen and change the data type. ☞ Page 43 Adding a member
	Comment	A comment is displayed. Double-click to edit a comment (up to 128 characters).
	Remark	A remark is displayed. Double-click to edit a remark (up to 128 characters).

Point

- When changing the contents of "Name" or "Comment" of the structure in the first row, those of "Name" or "Description" in "Type" are also changed.
- When adding a structure array ( ) to a member, the name of an array element is displayed as follows:

Three-dimensional array: _A_B_C
Two-dimensional array: _A_B
One-dimensional array: _A
A, B, and C indicate an index number of a one-dimensional, two-dimensional, and three-dimensional array, respectively.

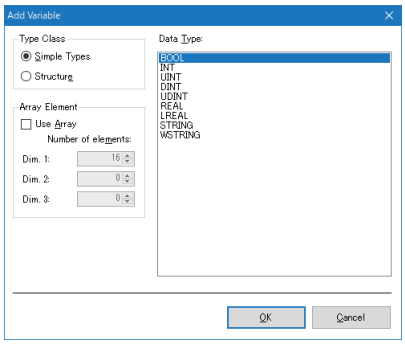
Precautions

- The name of a structure used for the data type of a structure label and a structure which is a member of the structure cannot be changed. If the change is needed, unselect the structure used for the data type and select another one.
- Only the members of a structure in the first row can be deleted and edited. If adding another structure to a member, members of the added structure cannot be deleted and edited.
- Array elements of a structure array cannot be deleted and edited.
- When adding another structure to a member of a structure in the first row, a setting that includes a circular reference to a structure cannot be set.

Adding a member

The following shows the screen to add a member to a structure.

Window



Displayed items

Item		Description
Type Class		Select a type class.
Array Element*1	Use Array	Select the checkbox to add a member as an array.
	Number of elements*2	Set the number of elements of each dimension of an array (1 to 128).*3,*4
String*5	Data Length	Set the length of a string (1 to 128).
Data Type		Select a data type.

*1 Displayed in the following case:
"Simple Types" is selected for "Type Class" and an item other than "STRING" and "WSTRING" is selected for "Data Type"
"Structure" is selected for "Type Class"
*2 Can be set when the checkbox of "Use Array" is selected.
*3 When a value greater than or equal to '1' is set for "Dim. 1", a value can be set for "Dim. 2".
*4 When a value greater than or equal to '1' is set for "Dim. 2", a value can be set for "Dim. 3".
*5 Displayed in the following case:
"Simple Types" is selected for "Type Class" and "STRING" or "WSTRING" is selected for "Data Type"

2.7 Security Setting

This section shows the screen to set the following authentication to access an OPC UA server module.

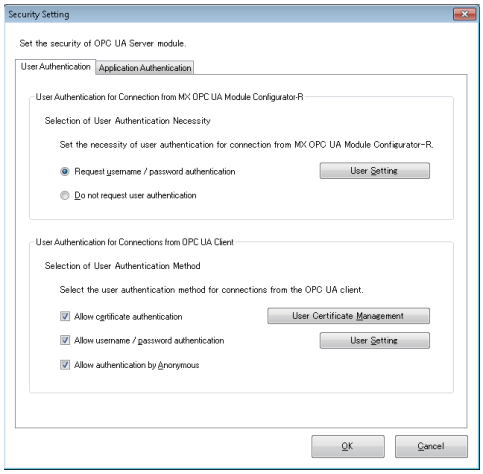
- User authentication for access from the configuration tool or an OPC UA client to an OPC UA server module
- Application authentication for access from an OPC UA client to an OPC UA server module

For the security setting for an OPC UA server which runs on an OPC UA server module, refer to the following:

☞ Page 48 OPC UA Server Setting

Window

Select [Tool] ⇨ [Security Setting].



Displayed items

Item			Description
[User Authentication] tab	User Authentication for Connection from MX OPC UA Module Configurator-R	Request username / password authentication	Select this to perform user authentication with a user name or password when accessing an OPC UA server module from the configuration tool.
		[User Setting] button	Click this to open the "User Setting" screen. ☞ Page 45 User setting
		Do not request user authentication	Select this not to perform user authentication with a user name or password when accessing an OPC UA server module from the configuration tool.
	User Authentication for Connections from OPC UA Client	Allow certificate authentication	Select the checkbox to allow user authentication with a certificate when accessing an OPC UA server module from an OPC UA client.
		[User Certificate Management] button	Click this to open the "Manage User Certificate" screen. ☞ Page 71 User certificate management
		Allow username / password authentication	Select the checkbox to allow user authentication with a user name or password when accessing an OPC UA server module from an OPC UA client.
		[User Setting] button	Click this to open the "User Setting" screen. ☞ Page 45 User setting
		Allow authentication by Anonymous	Select the checkbox to allow an anonymous logon. The connection from an anonymous user is allowed.
[Application Authentication] tab	Application Authentication for Connections from OPC UA Clients	Use automatic certificate exchange	Select the checkbox to exchange certificates automatically. When selecting this checkbox, a client certificate is automatically trusted and the connection is allowed. When not selecting this checkbox, store a client certificate in "Trust List" in the "Manage Application Certificate" screen. (☞ Page 69 Application certificate management)
		[Manage Application Certificate] button	Click this to open the "Manage Application Certificate" screen. ☞ Page 69 Application certificate management

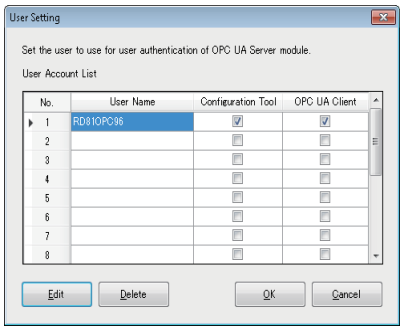
Precautions

- Automatically exchanging certificates is not recommended in an open network environment such as the internet or an intranet because it allows the connections from all OPC UA clients.
- An automatically exchanged certificate is not displayed in the "Manage Application Certificate" screen. (☞ Page 69 Application certificate management)
- Allowing an anonymous logon is not recommended in an open network environment such as the internet or an intranet because it allows the connections from all users.

User setting

The following shows the screen to set a user account used for user authentication for accessing an OPC UA server module from the configuration tool and an OPC UA client.

Window



Displayed items

Item		Description
User Account List	User Name	The user name of a user account is displayed.
	Configuration Tool	Whether a user can access an OPC UA server module from the configuration tool is displayed.
	OPC UA Client	Whether a user can access an OPC UA server module from an OPC UA client is displayed.
[Edit] button		Click this to open the "User Account Setting" screen of a selected row. ☞ Page 46 User account setting
[Delete] button		Click this to delete the setting of a selected row.

User account setting

The following shows the procedure for setting details of a user account.

Operating procedure

1. Click the [Edit] button in the "User Setting" screen.
2. Enter a user name and password (up to 32 characters, case-sensitive).
3. Select the checkbox of a target for user authentication.
4. Click the [OK] button.

Point

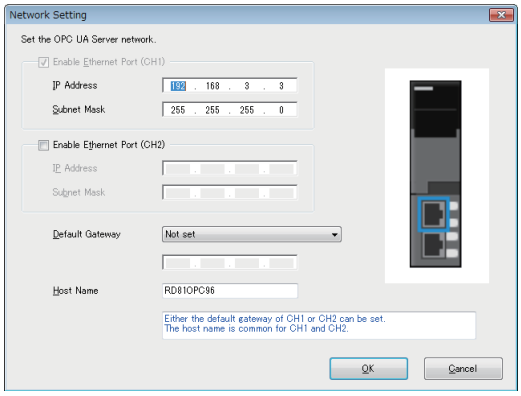
When only changing a target for user authentication, a new password does not need to be entered.

2.8 Network Setting

This section shows the screen to set the setting necessary for network connection.

Window

Select [Tool] ⇨ [Network Setting].



Displayed items

Item		Description
Ethernet port (CH1)	Enable Ethernet Port (CH1)	Select the checkbox to use the Ethernet port (CH1).*1
	IP Address	Set the IP address (CH1) of an OPC UA server module in decimal.*2
	Subnet Mask	When using a subnet mask, set it in decimal.
Ethernet port (CH2)	Enable Ethernet Port (CH2)	Select the checkbox to use the Ethernet port (CH2).
	IP Address	Set the IP address (CH2) of an OPC UA server module in decimal.*2
	Subnet Mask	When using a subnet mask, set it in decimal.
Default Gateway		Select the necessity of default gateway, and set an IP address.*3
Host Name		Set a host name.

*1 The checkbox status cannot be changed.

*2 A same IP address or an IP address of the same network cannot be set to both CH1 and CH2.

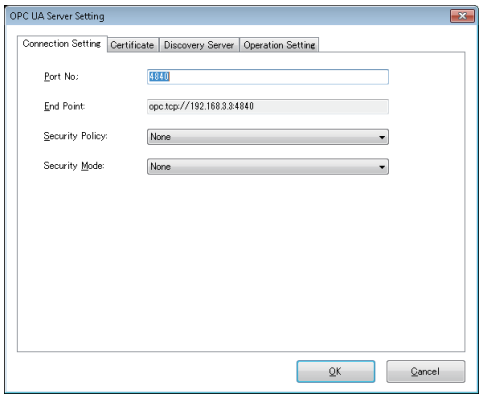
*3 Only one of CH1 or CH2 can be registered.
Communication with the same network as each CH is performed from each corresponding CH only.
(Even if a default gateway is set in other CH, communication is not performed from the other CH.)

2.9 OPC UA Server Setting

This section shows the screen to set the setting for an OPC UA server which runs on an OPC UA server module.
When connecting from an OPC UA client, use this setting.

Window

Select [Tool] ⇨ [OPC UA Server Setting].



Displayed items

■[Connection Setting] tab

Item	Description
Port No.	Set the port number of an OPC UA server.
End Point	The endpoint URL of an OPC UA server module is displayed.*1
Security Policy	Select a security policy. • None: No security • Basic128Rsa15: 128 bit encryption • Basic256: 256 bit encryption • Basic256Sha256: 256-bit encryption (using Sha256 algorithm)
Security Mode	Select a security mode. • None: No security • Sign: Add a signature to data • Sign & Encrypt: Add a signature to data and encrypt it

*1 When changing both the port number and the IP address of the Ethernet port (CH1), the endpoint URL is also changed.

■[Certificate] tab

Item	Description
OPC UA Server Name	Set the name of an OPC UA server.
Organization name	Set the name of an organization.
Organization Unit	Set the unit of an organization.
Locality	Set the name of a region.
State	Set a state.
Country	Enter the abbreviation for a country name.

Point

A certificate (der) is created in the SD memory card inserted in an OPC UA server module with the contents set in the [Certificate] tab.

■[Discovery Server] tab

Item	Description
Discovery Server URL	Set the URL of a discovery server. When using a discovery server, an OPC UA client can acquire an endpoint to access each OPC UA server by querying the discovery server.
Registration Interval	Set an interval for registering an endpoint for a discovery server.

■[Operation Setting] tab

Item		Description
Enable Log Output		Select the checkbox to output a communication event log between the configuration tool and an OPC UA server module to an SD memory card. For a log file to be output, refer to the following: ☞ Page 117 Log File Format
Specify the waiting time for the module operation start	—	Select the checkbox to specify a waiting time until 'Module READY' (X0) turns ON after an OPC UA server module is ready.
	Waiting time	Set a waiting time until 'Module READY' (X0) turns ON.

Point

- A log is not output when the free space of an SD memory card is less than 100 MB.
  Access an SD memory card from a personal computer and others, and delete an unnecessary log.
- To continuously output logs, it is recommended to secure 200 MB or more free space of an SD memory card.
- The waiting time for the module operation start is measured after the power is turned OFF to ON, the CPU module is reset, or the online module change function is performed. (The operation after the online module change function is performed is same as an operation after the power is turned OFF to ON or the CPU module is reset.)
  The connection with an OPC UA server module can be established after the waiting time elapses.

2.10 Global Label and Common Device Comment Import Function

This section describes the function to import global labels (including module labels) and common device comments set in an engineering tool into a project in the configuration tool (they are imported as data of a tag in an OPC UA server module).
Data imported from global labels is referred to as related data.
Related tags can be updated depending on the changes of global labels in a project created in an engineering tool.
Data which can be imported is as follows:
○: Available, ×: Not available, —: No data

Item	Engineering tool	Import source project
Common device comment	○	GX Works3 project (.gx3)
Device comment for each program	×	
Global label (Global)	○	
Module label (M+Global)	○	
Local label	×	
System label	—	

For global labels and device comments, refer to the following:
GX Works3 Operating Manual

Considerations for importing data

■Importing global labels

- Global labels can be imported only from a GX Works3 project, not from a GX Works2 project.
- An engineering tool (GX Works3 Version 1.050C or later) must be installed to import global labels.
- GX Works3 projects that require entering a user name and password or cannot be opened in an installed GX Works3 cannot be imported.
- Devices (data type) which cannot be set in the configuration tool and global labels whose devices/labels are not assigned are not imported. (However, these devices and labels are displayed in the import list.)
- When 32769 or more global labels are set in one GX Works3 project, those exceeding 32768 are not displayed in the list. If a target global label is not displayed, perform the following operations:
  Create a tag or structure label in the configuration tool.
  Reduce the number of global labels set in one GX Works3 project.
- Do not import global labels while operating a project created in an engineering tool. If attempted, the project may not be saved properly.
- When importing global labels, the following information is imported:
  Label name
  Data type
  Assignment (device)
- For related data, the following items cannot be edited.
  Name, device type, extended number (network No. or start I/O No.), IO address (PLC device No.), data type (☞ Page 27 [Basic] tab)
  Extended data type (☞ Page 28 [Details] tab)
- Data imported from a module label is not used as related data.
- When importing module labels, their details are applied to "Description".
- If imported global labels are copied or cut, and pasted to another access target device, they will not be used as related data.
- If there are multiple labels with a same name set in a project created in an engineering tool, global labels are updated to the content set in the first label.
- If an imported global label is a structure, the data structure of the structure is imported into the structure definition.

☞ Page 42 Structure Definition Setting

■Importing common device comments

- Common device comments can be imported only from a GX Works3 project, not from a GX Works2 project.
- An engineering tool (GX Works3 Version 1.050C or later) must be installed to import common device comments.
- GX Works3 projects that require entering a user name and password or cannot be opened in an installed GX Works3 cannot be imported.
- When 32769 or more common device comments are set in one GX Works3 project, those exceeding 32768 are not displayed in the list. If a target common device comment is not displayed, perform the following operations:
  Create a tag in the configuration tool.
  Reduce the number of common device comments set in one GX Works3 project.
- Do not import common device comments while operating a project created in an engineering tool. If attempted, the project may not be saved properly.
- When one or more comments are set for each device name to the imported common device comments, all the comments are displayed in the list.
- When importing common device comments, the following information is imported:
  Comment
  Device name
- When common device comments are imported, the setting of each comment title is ignored.
  (Example) Common device comments can be imported in the configuration tool regardless of its language (Japanese, English, etc.)

Importing global labels

The following shows the procedure for importing global labels set in an engineering tool as data.
If global labels created in an engineering tool are changed, they are updated in a batch. It is therefore necessary to link the global labels.

Operating procedure

1. Select an item (or) under "Address Space" in the tree view.
2. Select [Edit] ⇨ [Import Global Label].
3. Select an import source project for global labels in the "Import Global Label (Select Project)" screen, and click the [OK] button.

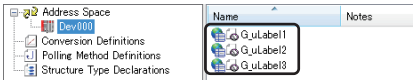
☞ Page 54 "Import Global Label (Select Project)" screen

4. Select global labels to import in the "Import Global Label (Select Data)" screen, and click the [OK] button.

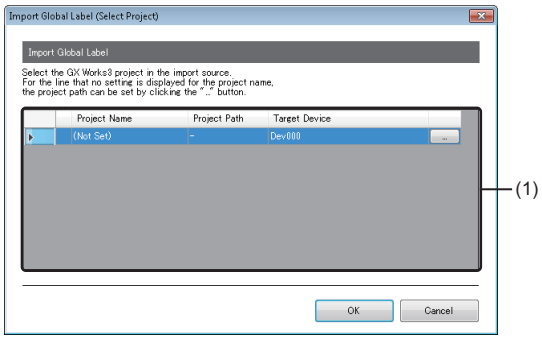
☞ Page 54 "Import Global Label (Select Data)" screen

Point

- Regardless of an item (or) selected under "Address Space" in the tree view, global labels are imported immediately under an access target device selected in the "Import Global Label (Select Project)" screen.
- Tags that import global labels are displayed as related data as shown below.

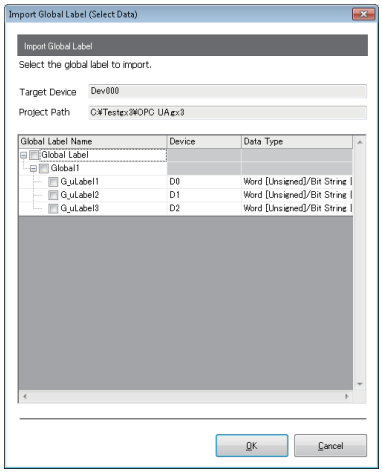


■"Import Global Label (Select Project)" screen



Item	Description
(1) Import source list	A project created in an engineering tool and an access target device that are set as an import source for global labels are displayed. If no project is set in an access target device, "(Not Set)" is displayed. Specify a project in the "Address Space(Target Device)" screen displayed by clicking the [...] button. ☞ Page 23 Address space (access target device) setting
[OK] button	Click this to apply the setting and open the screen to specify global labels to import. ☞ Page 54 "Import Global Label (Select Data)" screen

■"Import Global Label (Select Data)" screen



Item	Description
Target Device	An access target device selected in the "Import Global Label (Select Project)" screen is displayed.
Project Path	The path of a project selected in the "Import Global Label (Select Project)" screen is displayed.
Global Label Name	A global label name (set in an engineering tool) is displayed.*1 Select the checkbox of a global label to be imported.
Device	The device of a global label is displayed.
Data Type	The data type of a global label is displayed.
[OK] button	Click this to import a specified global label and close the screen.

*1 For module labels, any one of the following is displayed for the name. If a name includes 51 or more characters, those exceeding the number are deleted to display.
(instance name)_(module number)_(label name)
(instance name)_(module number)_(label name)_D
For an instance name, module number, label name, or _D, refer to each of the following:
☞ Page 93 Instance name, Page 93 Module number, Page 93 Label name, Page 93 _D

Precautions

- If the number of tags[*1] exceeds 10000 after importing global labels, the global labels cannot be imported. Reduce the number of global labels to import in the configuration tool, and then import them again.

*1 When using a structure label, a member of a structure is also used as a tag.

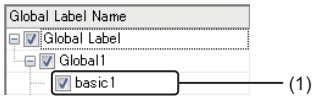
- Global labels that apply to any of the following conditions cannot be imported.

Item	Condition
Label name	• A character other than one shown in the following section is used. ☞ Page 110 Available ASCII characters • 51 or more characters are set. • The checkbox of a global label with the same name is already selected.
Device	• A device is not assigned. • A device type or representation that is not supported by an OPC UA server module is used. • Digit specification or bit specification is used.
Data type	• A data type that is not supported by an OPC UA server module is used. • When the data type is a character string, the number of characters exceeds 128.
Array	• The first element number of each dimension of an array is set to a number other than '0'. • The product of the number of elements of each dimension of an array exceeds 128. • For a bit device, the product of the number of elements of each dimension of an array is set to a number other than a multiple of 16.

■Global Label Name

- Basic data

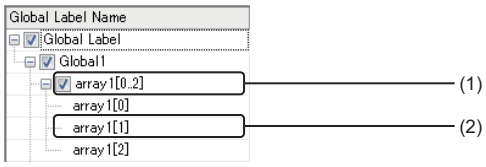
A display example when a global label is basic data and one of a tag name after import are as follows:



Type	Display example of a global label name	Display example of a tag name after import
(1) Basic data	basic1	basic1

- Array

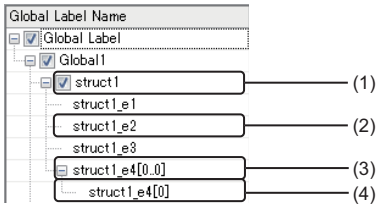
A display example when a global label is an array and one of a tag name after import are as follows:



Type	Display example of a global label name	Display example of a tag name after import
(1) Array data	array1[0..2]	array1
(2) Array element	array1[1]	—

- Structure

A display example when a global label is a structure and one of a structure label name and tag name after import are as follows:

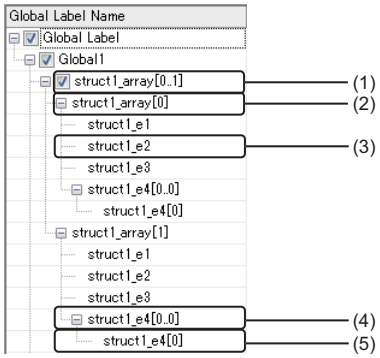


Type	Display example of a global label name	Display example of a structure label name after import	Display example of a tag name after import
(1) Structure data	struct1	struct1	—
(2) Structure element	struct1_e2	—	struct1_e2

Type	Display example of a global label name	Display example of a structure label name after import	Display example of a tag name after import
(3) Structure element [array]	struct1_e4[0..0]	—	—
(4) Array element	struct1_e4[0]	—	struct1_e4

• Structure array

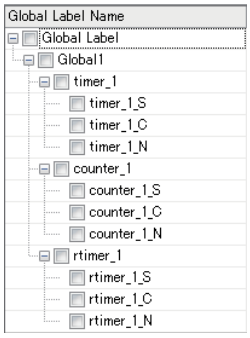
A display example when a global label is a structure array and one of a structure label name and tag name after import are as follows:



Type	Display example of a global label name	Display example of a structure label name after import	Display example of a tag name after import
(1) Structure array data	struct1_array[0..1]	struct1_array	—
(2) Structure array element	struct1_array[0]	—	—
(3) Structure element	struct1_e2	—	struct1_e2
(4) Structure element [array]	struct1_e4[0..0]	—	—
(5) Array element	struct1_e4[0]	—	struct1_e4

• Timer/counter/retentive timer

A display example when a global label is a timer, counter, or retentive timer and one of a tag name after import are as follows:



Type		Display example of a global label name*1,*2	Display example of a tag name after import
Timer	Contact	timer_1_S	timer_1_S
	Coil	timer_1_C	timer_1_C
	Current value	timer_1_N	timer_1_N
Counter	Contact	counter_1_S	counter_1_S
	Coil	counter_1_C	counter_1_C
	Current value	counter_1_N	counter_1_N
Retentive timer	Contact	rtimer_1_S	rtimer_1_S
	Coil	rtimer_1_C	rtimer_1_C
	Current value	rtimer_1_N	rtimer_1_N

*1 A contact, coil, and current value are displayed as follows:
Contact: (label name)_S
Coil: (label name)_C
Current value: (label name)_N

*2 When a timer, counter, or retentive timer is set as an array, they are displayed as an array of a contact, coil, and current value.

■Data type

The following table shows the data types of global labels and those of tags after import.

○: Available, ×: Not available

Data type of global label	Import	Data type of a tag
Bit	○	BOOL
Word [signed]	○	INT
Double word [signed]	○	DINT
Word [unsigned]/Bit string [16-bit]	○	UINT
Double word [unsigned]/Bit string [32-bit]	○	UDINT
Single-precision real number	○	REAL
Double-precision real number	○	LREAL
String (n)*1	○	STRING
String [Unicode] (n)*1	○	WSTRING
Timer	○	Contact: BOOL Coil: BOOL Current value: INT
Counter	○	
Retentive timer	○	
Long timer	○	Contact: BOOL Coil: BOOL Current value: DINT
Long counter	○	
Long retentive timer	○	
Time	×	—
Pointer	×	—

*1 'n' indicates the number of characters. Importing to a project of the configuration tool is available only when 'n' is 1 to 128.

Releasing relation to global labels

The following shows the procedure for releasing the relation between a global label of an engineering tool and related data.

Operating procedure

1. Select and right-click an item (or) under "Address Space" in the tree view or related data in the list view, then select [Release Relation to Global Label].

Point

- When selecting an item (or), all related data under the item is the target.
- The relation can also be released when unselecting the checkbox of "Use the global label/common device comment" in the "Address Space(Target Device)" screen. (☞ Page 23 Address space (access target device) setting)

Precautions

To link the data whose relation was once released, import the global label again.

Updating data related to global labels

The following shows the procedure for updating data related to a global label of an engineering tool to the latest value.
If it cannot be updated, the relation will be released.

Operating procedure

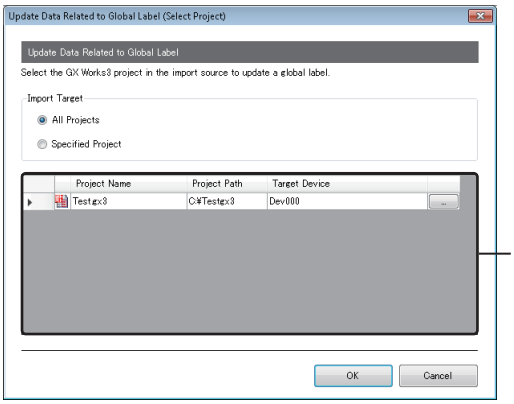
1. Select an item (or) under "Address Space" in the tree view.
2. Select [Edit] ⇨ [Update Data Related to Global Label].
3. Select a project to update and click the [OK] button in the "Update Data Related to Global Label (Select Project)" screen.

☞ Page 60 "Update Data Related to Global Label (Select Project)" screen

4. Select a global label to update and click the [OK] button in the "Update Data Related to Global Label (Select Project)" screen.

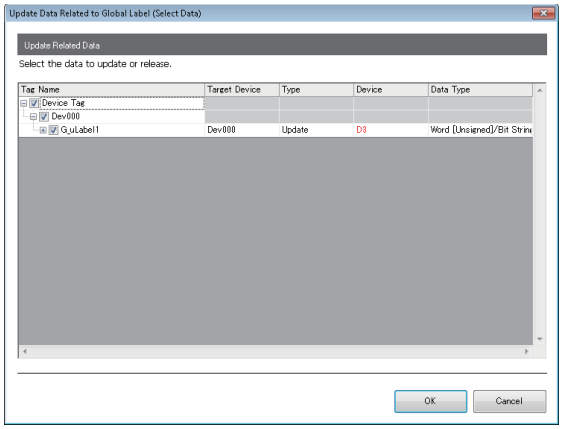
☞ Page 60 "Update Data Related to Global Label (Select Data)" screen

■"Update Data Related to Global Label (Select Project)" screen



Item	Description
All Projects	Select this to update related data of all projects.
Specified Project	Select this to update related data of a specified project.
(1) Import source list	A project created in an engineering tool and an access target device that are set as an import source for global labels are displayed. If no project is set in an access target device, "(Not Set)" is displayed. Specify a project in the "Address Space(Target Device)" screen displayed by clicking the [...] button. ☞ Page 23 Address space (access target device) setting
[OK] button	Click this to apply the setting and open the screen to specify global labels to update. ☞ Page 60 "Update Data Related to Global Label (Select Data)" screen

■"Update Data Related to Global Label (Select Data)" screen



Item	Description
Tag Name	The name of a tag is displayed. Select the checkbox of related data to update.
Target Device	An access target device is displayed.
Type	Either of the following items is displayed. • Update: When related data, devices, or data types are different from the previous data, the values are updated. • Relation Release: The relation is released when related data is not found or there is an inconsistency due to update.*1
Device	A device after update is displayed. If a device is changed after update, the device name is displayed in red.
Data Type	A data type after update is displayed. If a data type is changed after update, the data name is displayed in red.
[OK] button	Click this to update specified related data or release the relation.

*1 Applies to the following cases:
The global label name does not exist in an import source project.
A device, data type, or character string size that cannot be used for an OPC UA server module is specified.
A device that cannot be combined with a data type is used.

Importing common device comments

The following shows the procedure for importing common device comments set in an engineering tool as data.

Operating procedure

1. Select an item (or) under "Address Space" in the tree view.
2. Select [Edit] ⇨ [Import Common Device Comment].
3. Select an import source project for common device comments in the "Import Common Device Comment (Select Project)" screen, and click the [OK] button.

☞ Page 62 "Import Common Device Comment (Select Project)" screen

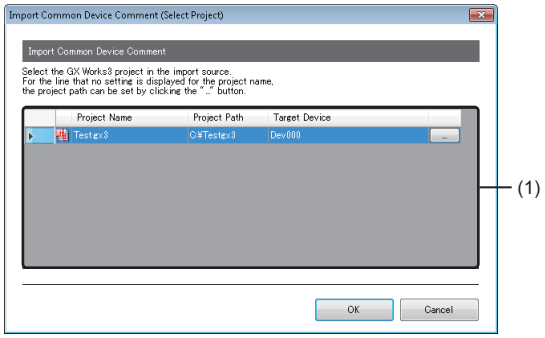
4. Select common device comments to import in the "Import Common Device Comment (Select Data)" screen, and click the [OK] button.

☞ Page 62 "Import Common Device Comment (Select Data)" screen

Point

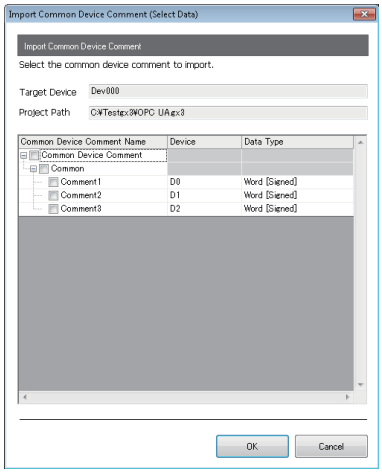
Regardless of an item (or) selected under "Address Space" in the tree view, common device comments are imported immediately under an access target device selected in the "Import Common Device Comment (Select Project)" screen.

■"Import Common Device Comment (Select Project)" screen



Item	Description
(1) Import source list	A project created in an engineering tool and an access target device that are set as an import source for common device comments are displayed. If no project is set in an access target device, "(Not Set)" is displayed. Specify a project in the "Address Space(Target Device)" screen displayed by clicking the [...] button. ☞ Page 23 Address space (access target device) setting
[OK] button	Click this to apply the setting and open the screen to specify common device comments to import. ☞ Page 62 "Import Common Device Comment (Select Data)" screen

■"Import Common Device Comment (Select Data)" screen



Item	Description
Target Device	An access target device selected in the "Import Common Device Comment (Select Project)" screen is displayed.
Project Path	The path of a project selected in the "Import Common Device Comment (Select Project)" screen is displayed.
Common Device Comment	A common device comment (set in an engineering tool) is displayed. Select the checkbox of a common device comment to import.
Device	A device with a common device comment is displayed.
Data Type	The data type of a device is displayed.
[OK] button	Click this to import a specified common device comment and close the screen.

Precautions

- If the number of tags[*1] exceeds 10000 after importing common device comments, the common device comments cannot be imported. Reduce the number of common device comments to import in the configuration tool, and then import them again.

*1 When using a structure label, a member of a structure is also used as a tag.

- Common device comments that apply to any of the following conditions cannot be imported.

Item	Condition
Comment	• A character other than one shown in the following section is used. ☞ Page 110 Available ASCII characters • 51 or more characters are set. • The checkbox of a common device comment with the same name is already selected.
Device	• A device is not assigned. • A device type or representation that is not supported by an OPC UA server module is used. • Digit specification or bit specification is used.
Data type	• A data type that is not supported by an OPC UA server module is used. • When the data type is a character string, the number of characters exceeds 128.

■Data type

The correspondence between the data types of devices for which common device comments are set and those of tags after import is same as that shown in the following section.

☞ Page 57 Data type

2.11 Online

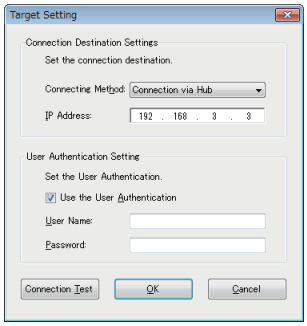
This section shows the online operations performed to an OPC UA server module connected on a network.

Connection destination setting

The following shows the screen to set and edit connection destination information.
Perform the user authentication when connecting actually.

Window

Select [Online] ⇨ [Target Setting].



Displayed items

Item		Description
Connection Destination Settings	Connecting Method	Select a connection method.
	IP Address	Set the IP address for connection destination.
User Authentication Setting	Use the User Authentication	Select the checkbox to perform the user authentication.
	User Name	Specify the user name for user authentication.
	Password	Specify the password for user authentication.
[Connection Test] button		Click this to perform a connection test with a set connection destination.

Online data operations

The following shows the operations for reading, writing, verifying, and updating a setting (project) in an OPC UA server module.

Restriction

If verifying a setting written to a module in the configuration tool the version of which is '1.01B' or later in the configuration tool the version of which is '1.00A', it cannot be verified correctly. Update the configuration tool to the latest version before verification.

Reading from an OPC UA server module

A setting in an OPC UA server module specified in the "Connection Setting" screen can be read by the following operation.

Operating procedure

Select [Online] ⇨ [Read from OPC UA Server Module].

Writing to an OPC UA server module

A setting can be written to the SD memory card inserted in an OPC UA server module specified in the "Connection Setting" screen by the following operation.

Operating procedure

Select [Online] ⇨ [Write to OPC UA Server Module].

Verification with an OPC UA server module

A setting in an OPC UA server module specified in the "Connection Setting" screen can be verified with one of a project being edited by the following operation.

Operating procedure

Select [Online] ⇨ [Verify with OPC UA Server Module].

Setting update of an OPC UA server module

A setting of an OPC UA server module specified in the "Connection Setting" screen can be updated by the following operation.

Operating procedure

Select [Online] ⇨ [Update setting of OPC UA Server Module].

Server operation

The following shows the operations for restarting and stopping a server operation of an OPC UA server module.

Restart of an OPC UA server module

A server operation of an OPC UA server module specified in the "Connection Setting" screen can be restarted by the following operation.

Operating procedure

Select [Online] ⇨ [Restart the OPC UA Server Module].

Stop of an OPC UA server module

A server operation of an OPC UA server module specified in the "Connection Setting" screen can be stopped by the following operation.

Operating procedure

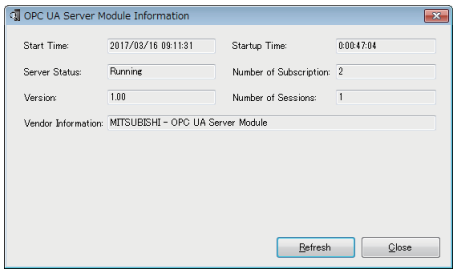
Select [Online] ⇨ [Stop the OPC UA Server Module].

Information of an OPC UA server module

The following shows the screen to display the operating status of an OPC UA server module.

Window

Select [Online] ⇨ [OPC UA Server Module Information].



Displayed items

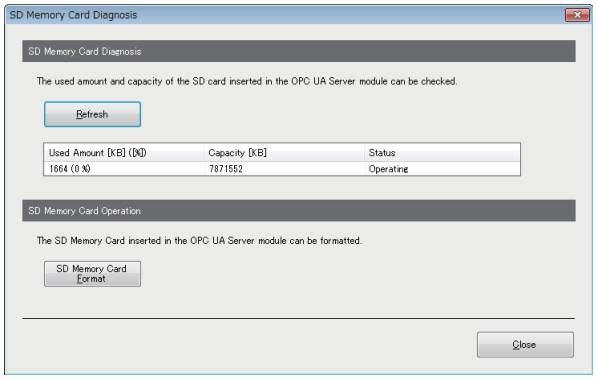
Item	Description
Start Time	The date and time when a server started is displayed.
Startup Time	The elapsed time since a server started is displayed.
Server Status	The status of a server is displayed.
Number of Subscription	The number of accumulated subscriptions since a server started is displayed.
Version	The software version of a server is displayed.
Number of Sessions	The number of sessions of OPC UA clients connected to a server is displayed.
Vendor Information	The vendor information is displayed.
[Refresh] button	Click this to update the operating status of a server to the latest information.

SD memory card diagnostic

The following shows the screen to display the current use status of the SD memory card inserted in an OPC UA server module and format the SD memory card.

Window

Select [Online] ⇨ [SD Memory Card Diagnosis].



Displayed items

Item		Description
SD Memory Card Diagnosis	[Refresh] button	Click this to update the status of an SD memory card to the latest information.
	Used Amount [KB] ([%])	The used amount and use rate of an SD memory card are displayed.
	Capacity [KB]	The capacity of an SD memory card is displayed.
	Status	The SD memory card status is displayed.
SD Memory Card Operation	[SD Memory Card Format] button	Click this to format an SD memory card.

Precautions

All the settings of OPC UA server module will be lost if the SD memory card is formatted since the settings are saved in the SD memory card.

Read the current setting as necessary, and write the setting after formatting the card.

If the power is turned OFF to ON or the CPU module is reset without writing the setting in the SD memory card, the IP address of the OPC UA server module returns to the initial state (192.168.3.3).

Application certificate management

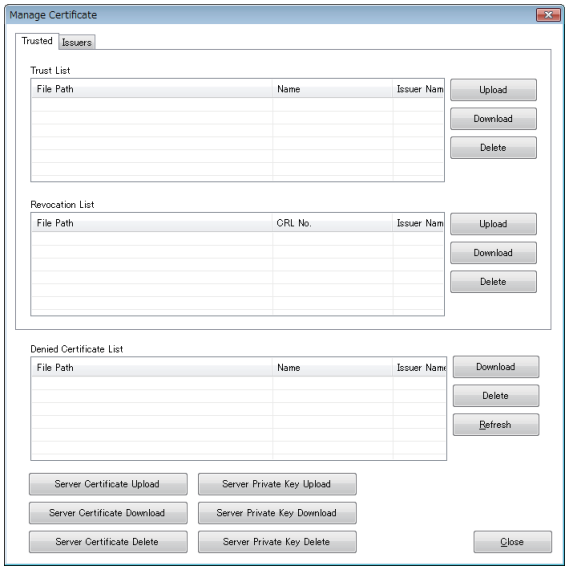
The following shows the screen to manage an application certificate in an OPC UA server module.
When certificates are exchanged automatically, a client certificate is not displayed. (☞ Page 44 Security Setting)
The [Trusted] tab is used for communicating with an OPC UA client by using a normal authentication method, and the [Issuers] tab for the communication by using Issuers authentication.
For managing certificates certified by a certificate authority, refer to the following:
☞ Page 115 Handling Certificates Certified by a Certificate Authority

Point

Communication with higher security than a normal authentication method is available with Issuers authentication.
For Issuers authentication, upload an electronic certificate issued by a certificate authority to "Trust List" in the [Issuers] tab, and a client certificate to trust to "Trust List" in the [Trusted] tab.

Window

Select [Online] ⇨ [Manage Application Certificate].



Displayed items

■[Trusted] tab/[Issuers] tab

Item		Description
Trust list	—	A list to register the certificate of a client (der) which is allowed to connect. When trusting an OPC UA client which requests to connect and allowing the connection, click the [Upload] button to upload a client certificate (der) to trust to the trust list. ■When communicating by using a certificate certified by a certificate authority Upload an electronic certificate issued by a certificate authority. The connection only from an OPC UA client using the certificate listed on the electronic certificate is allowed.
	[Upload] button	Click this to transfer an arbitrary certificate from a configuration personal computer to the SD memory card inserted in an OPC UA server module.
	[Download] button	Click this to transfer an arbitrary certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer.
	[Delete] button	Click this to delete an arbitrary certificate in the SD memory card inserted in an OPC UA server module.

Item		Description
Revocation List	—	A client certificate (der_NG) is automatically stored when the trust of the certificate stored in "Trust List" is lost (such as expiration). ■When communicating by using a certificate certified by a certificate authority Upload the certificate revocation list (crl) issued by a certificate authority. The connection from an OPC UA client using the certificate listed on the certificate revocation list is denied.
	[Upload] button	Click this to transfer an arbitrary certificate from a configuration personal computer to the SD memory card inserted in an OPC UA server module.
	[Download] button	Click this to transfer an arbitrary certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer.
	[Delete] button	Click this to delete an arbitrary certificate in the SD memory card inserted in an OPC UA server module.
Denied Certificate List	—	A client certificate denied when connecting is automatically stored. To allow the connection, click the [Download] button to download the certificate and upload it to "Trust List".
	[Download] button	Click this to transfer an arbitrary certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer.
	[Delete] button	Click this to delete an arbitrary certificate in the SD memory card inserted in an OPC UA server module.
	[Refresh] button	Click this to update the denied certificate list to the latest information.
[Server Certificate Upload] button		Click this to transfer a server certificate from a configuration personal computer to the SD memory card inserted in an OPC UA server module. Use this button to upload a certificate (such as one issued by a certificate authority) other than one with the contents set in the following section. ☞ Page 49 [Certificate] tab
[Server Certificate Download] button		Click this to transfer a server certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer. A downloaded certificate is used for issuing an electronic certificate and others.
[Server Certificate Delete] button		Click this to delete a server certificate in the SD memory card inserted in an OPC UA server module. When a certificate is deleted, a certificate with the contents set in the following section is created once the power is turned OFF to ON or the CPU module is reset. ☞ Page 49 [Certificate] tab
[Server Private Key Upload] button		Click this to transfer the server private key of an OPC UA server module from a configuration personal computer to the SD memory card inserted in an OPC UA server module. The server private key paired with a certificate uploaded by clicking the [Server Certificate Upload] button is uploaded.
[Server Private Key Download] button		Click this to transfer the server private key of an OPC UA server module from the SD memory card inserted in an OPC UA server module to a configuration personal computer. A downloaded server private key is used for issuing an electronic certificate and others.
[Server Private Key Delete] button		Click this to delete the server private key of an OPC UA server module in the SD memory card inserted in an OPC UA server module. If the server private key is deleted, a server private key paired with a certificate set in the following section is created once the power is turned OFF and ON or the CPU module is reset. ☞ Page 49 [Certificate] tab

User certificate management

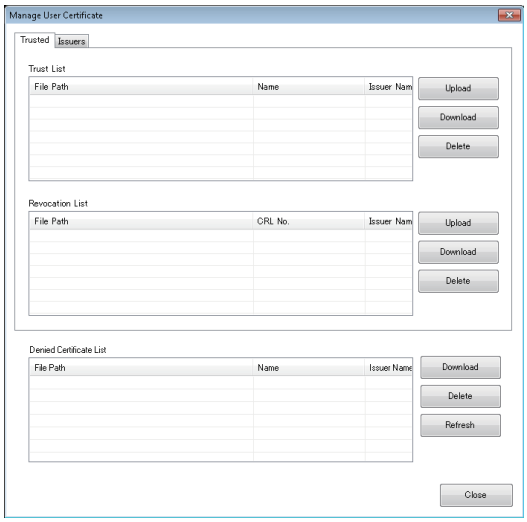
The following shows the screen to manage a user certificate in an OPC UA server module.
The [Trusted] tab is used for communicating with an OPC UA client by using a normal authentication method, and the [Issuers] tab for the communication by using Issuers authentication.
For managing certificates certified by a certificate authority, refer to the following:
☞ Page 115 Handling Certificates Certified by a Certificate Authority

Point

Communication with higher security than a normal authentication method is available with Issuers authentication.
For Issuers authentication, upload an electronic certificate issued by a certificate authority to "Trust List" in the [Issuers] tab, and a client certificate to trust to "Trust List" in the [Trusted] tab.

Window

Select [Online] ⇨ [Manage User Certificate].



Displayed items

The screen items are same as those described in the following section.
☞ Page 69 [Trusted] tab/[Issuers] tab
Note that the following items are not displayed.

- [Server Certificate Upload] button
- [Server Certificate Download] button
- [Server Certificate Delete] button
- [Server Private Key Upload] button
- [Server Private Key Download] button
- [Server Private Key Delete] button

2.12 Help

This section shows the help function for the following operations.

- Opening the user's manual
- Version information

Opening the user's manual

The user's manual (operation help) can be opened by the following operation.

Operating procedure

1. Select [Help] ⇨ [Help].

Version information

The version information of the configuration tool can be checked by the following operation.

Operating procedure

1. Select [Help] ⇨ [Version Information].

3 PARAMETER SETTING

This chapter explains each setting that can be set in the parameter setting of an engineering tool.

3.1 Parameter Setting Procedure

1. Add an OPC UA server module to an engineering tool.

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ right-click [Add New Module]

2. Set two types of parameters, the basic setting and refresh setting, by selecting in the tree in the screen displayed by the following operation.

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [RD81OPC96]

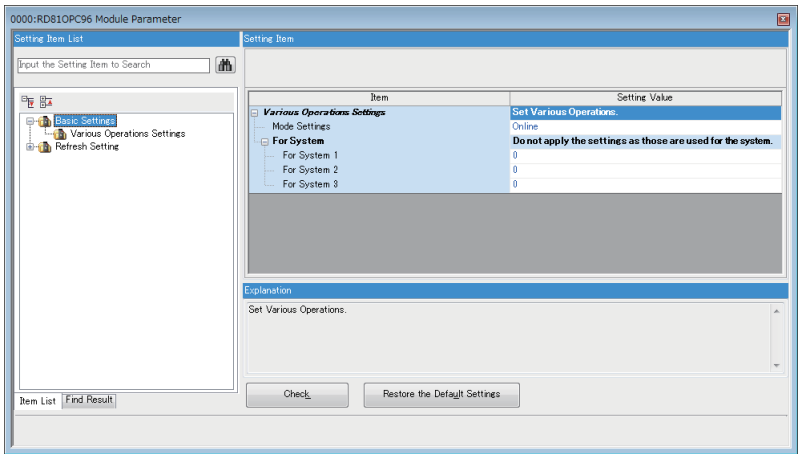
3. Write the settings to a CPU module in the engineering tool.

[Online] ⇨ [Write to PLC]

4. The settings are applied by resetting the CPU module or turning the power OFF and ON.

3.2 Basic Setting

This section shows the various operation settings of an OPC UA server module.



Various operation settings

The mode setting and the response monitoring time setting of an access target device for an OPC UA server module can be set.

Item name		Description	Setting range
Mode Settings*1		Set the operation mode of an OPC UA server module. • Online: Normal operation mode • Online (Asynchronous Mode): An OPC UA server module and a CPU module start without synchronization. • Automatic hardware test: Hardware such as ROM/RAM/Ethernet of an OPC UA server module is tested. • Hardware test for LED check: LED of an OPC UA server module is tested.	• Online • Online (Asynchronous Mode)*2 • Automatic hardware test • Hardware test for LED check (Default: Online)
For System	For System 1 to 3	Do not use these since they are used only for the system.	—

*1 For the difference between 'online' and 'online (asynchronous mode)', refer to the following:
☞ Page 74 Online and online (asynchronous mode)

*2 Available for the following combinations of versions.
OPC UA server module: Firmware version is '02' or later.
GX Works3: Software version is "1.055H" or later.

Online and online (asynchronous mode)

The following explains the difference between 'online' and 'online (asynchronous mode)'.

■Online

A CPU module and an OPC UA server module synchronize each other and complete their start processing, then start at the same time. (A CPU module stands by until an OPC UA server module completes its start processing.)

■Online (asynchronous mode)

A CPU module and an OPC UA server module start individually when their start processing is completed without waiting for the completion of the processing of the other module.

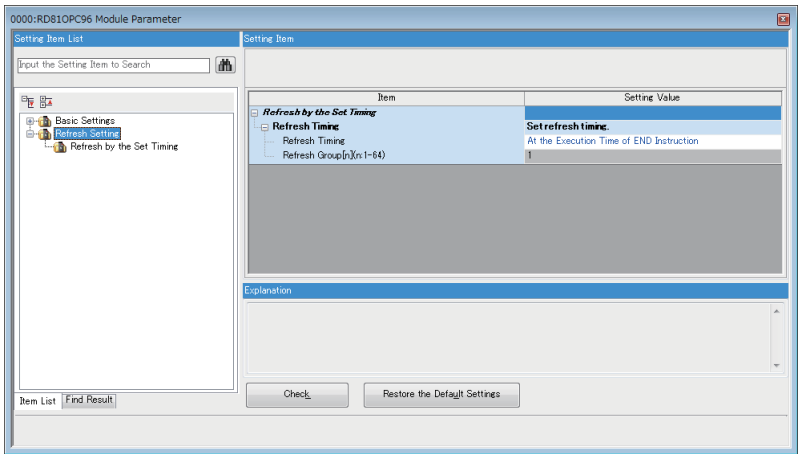
Precautions

The following shows the considerations for using 'online (asynchronous mode)'.

- Do not access the buffer memory of an OPC UA server module until the module is started after a CPU module is started.
  Otherwise, an indefinite value may be acquired and a sequence program may not run as intended.
  When accessing the buffer memory, make sure that 'Module READY' (X0) is turned ON.

3.3 Refresh Setting

This section shows the setting of the refresh timing of the specified target.



Setting value	Description
At the Execution Time of END Instruction	To refresh at the END processing in a CPU module.
At the Execution Time of Specified Program	To refresh when executing a program specified in "Refresh Group [n]".

4 TROUBLESHOOTING

This chapter explains the errors which may occur when using an OPC UA server module and the troubleshooting.

4.1 Checking Method for Error Descriptions

The following are the methods to check error descriptions.

Checking method	Details
System monitor of an engineering tool	Error codes*1 can be checked by the system monitor of an engineering tool. ☞ Page 77 Checking Module Status
Buffer memory	Error codes*1 can be checked in the following buffer memory. ☞ Page 106 Error code (Un\G7168) ☞ Page 108 Error log 1 to 16 (Un\G13058 to 13217)
Dot matrix LED	Error codes*1 can be checked with the dot matrix LED on the front of an OPC UA server module.

*1 Error code
If the same error occurs repeatedly, the error is output only for the first time. (Detailed information is also output only for the first occurrence of the error.)
When the same error occurs several times in different causes, take action to correct the error in the order of occurrence based on the error code and detailed information that were outputted at the first occurrence of the error.
If clearing the error (or resetting and turning the power OFF to ON) after taking the corrective action, error information is output when the same error occurs again.

Error type

There are two types of errors of an OPC UA server module as follows:

Error type	ERR LED	Module status	Corrective action
Module stop error	Flashing	An OPC UA server function of a module stops.	Take action for the error according to the error code, and turn the 'ERR LED' OFF by any of the following operations: • Error clear request (Y10) • Turn the power OFF to ON • Reset the CPU module • Update the setting from the configuration tool
Module continuation error	ON	An OPC UA server function of a module continues.	

4.2 Checking Module Status

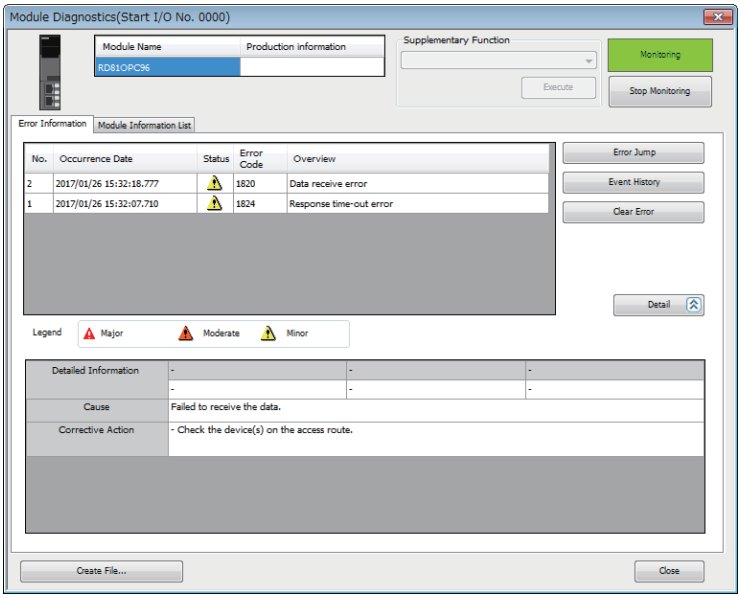
The following functions can be used on the "Module Diagnostics" screen of an engineering tool.

Function	Purpose
Error Information	To display the description of an error currently occurred. The history of an error detected in an OPC UA server module can be checked by clicking the [Event History] button.
Module Information List	To display the information of each status of an OPC UA server module.

Error information

The description of an error currently occurred and a corrective action can be checked.

Window



Displayed items

Item	Description
Detailed Information	Up to three details of each error is displayed.
Cause	The detail of an error cause is displayed.
Corrective Action	A corrective action for an error is displayed.

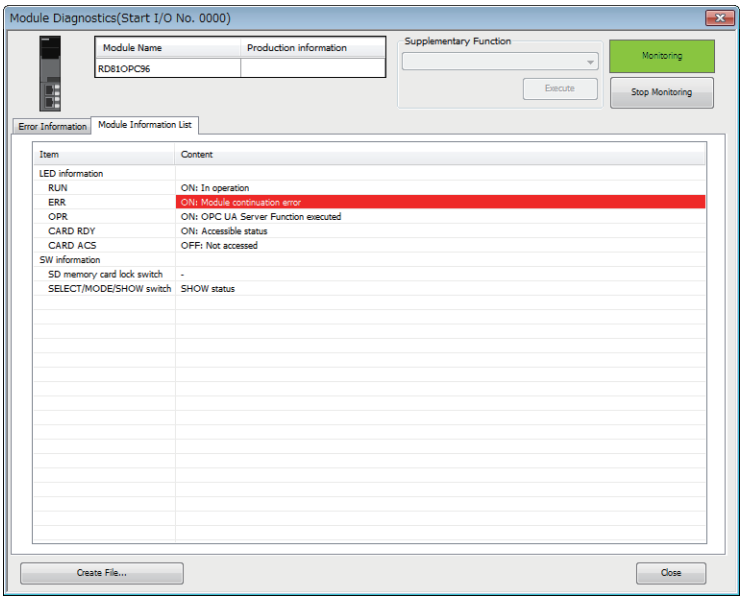
Restriction

An error in an OPC UA server module cannot be cleared with the [Clear Error] button.
To clear an error, update the setting in the configuration tool. (☞ Page 65 Setting update of an OPC UA server module)

Module information list

The information for each status of an OPC UA server module can be checked by switching to the [Module Information List] tab.

Window



Checking LED information

The LED status or the self-diagnostic status of an OPC UA server module can be checked.

When executing the automatic hardware test or the hardware test for LED check, "Automatic hardware test is being executed" or "Hardware test for LED check is being executed" is displayed for all LED information.

When an error occurs, refer to the following section and take corrective action.

☞ Page 83 Troubleshooting by Symptom

Displayed items

Item	Description
RUN	• ON: In operation • Flashing: In selection for online module change • OFF: Watchdog timer error (hardware failure)
ERR	• ON: Module continuation error or watchdog timer error (hardware failure) • Flashing: Module stop error • OFF: In normal status
OPR	• ON: OPC UA server function performed • OFF: OPC UA server function stopped
CARD RDY	• ON: Accessible status • Flashing: In preparation or formatting • OFF: Inaccessible status
CARD ACS	• ON: Accessing • OFF: Not accessed

Checking the switch information

The switch information or the self-diagnostic status of an OPC UA server module can be checked.

When executing the automatic hardware test or the hardware test for LED check, "Automatic hardware test is being executed" or "Hardware test for LED check is being executed" is displayed for all switch information.

Displayed items

Item	Description
SD memory card lock switch	• — • Stop instruction
SELECT/MODE/SHOW switch	• SELECT status • MODE status • SHOW status

Self-diagnostic test

Automatic hardware test

The following explains the test on a hardware such as ROM/RAM/Ethernet of an OPC UA server module.

Restriction

The value of buffer memory cannot be referred in an engineering tool during the automatic hardware test.

Operating procedure

1. Select "Automatic hardware test" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" in the module parameter of an OPC UA server module in the parameter setting of an engineering tool.
2. Disconnect a cable if it is connected to a 1000BASE-T/100BASE-TX/10BASE-T interface.
3. Remove the SD memory card if is inserted.
4. Set the CPU module to the STOP state, and write the parameters.
5. Reset the CPU module.
6. After resetting the CPU module, the automatic hardware test is performed.

The LED display when diagnosing is as follows:

Status		RUN LED status	ERR LED status	Dot matrix LED status
Diagnosing		ON	OFF	"H.T." (Flashing)
Complete diagnosing	Normal completion	ON	OFF	"OK" (ON)
	Abnormal completion	ON	ON	"ERR" (ON)

7. When the test completed normally, select "Online" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" in the module parameter of an OPC UA server module in the parameter setting of an engineering tool and reset the CPU module.
8. When the test completed abnormally, check if measures are taken to reduce noise of the system, and perform the automatic hardware test again.

If the test completed abnormally again, a hardware failure may occur in OPC UA server module. Please consult your local Mitsubishi representative.

Do not use an electric screwdriver when removing the module. Loose the module fixing screws completely to remove the module.

Hardware test for LED check

The following explains the LED hardware diagnostic of an OPC UA server module. For the diagnostic, the LED of a OPC UA server module needs to be turned ON.

Restriction

The value of buffer memory cannot be referred in the engineering tool during the hardware test for LED check.

Operating procedure

1. Select "Hardware test for LED check" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" in the module parameter of an OPC UA server module in the parameter setting of an engineering tool.
2. Set the CPU module to the STOP state, and write the parameters.
3. Reset the CPU module.
4. After the CPU module is reset, the hardware test for LED check is performed automatically.

The following contents are displayed. Check visually whether there is no error.

LED name	Display color	Display status
RUN	Green	ON
ERR	Red	ON
OPR	Green	ON
CARD RDY	Green	ON
CARD ACS	Green	ON
Dot matrix LED	Orange	☞ Page 82 Patterns for dot matrix LED check

Since the LED under the OPR LED is used for the system, the test is performed as well as other LEDs. (Display color: green, display status: ON)

5. When the test completed normally, select "Online" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" in the module parameter of an OPC UA server module in the parameter setting of an engineering tool and reset the CPU module.
6. When the test completed abnormally, check if measures are taken to reduce noise of the system, and perform the hardware test for LED check again.

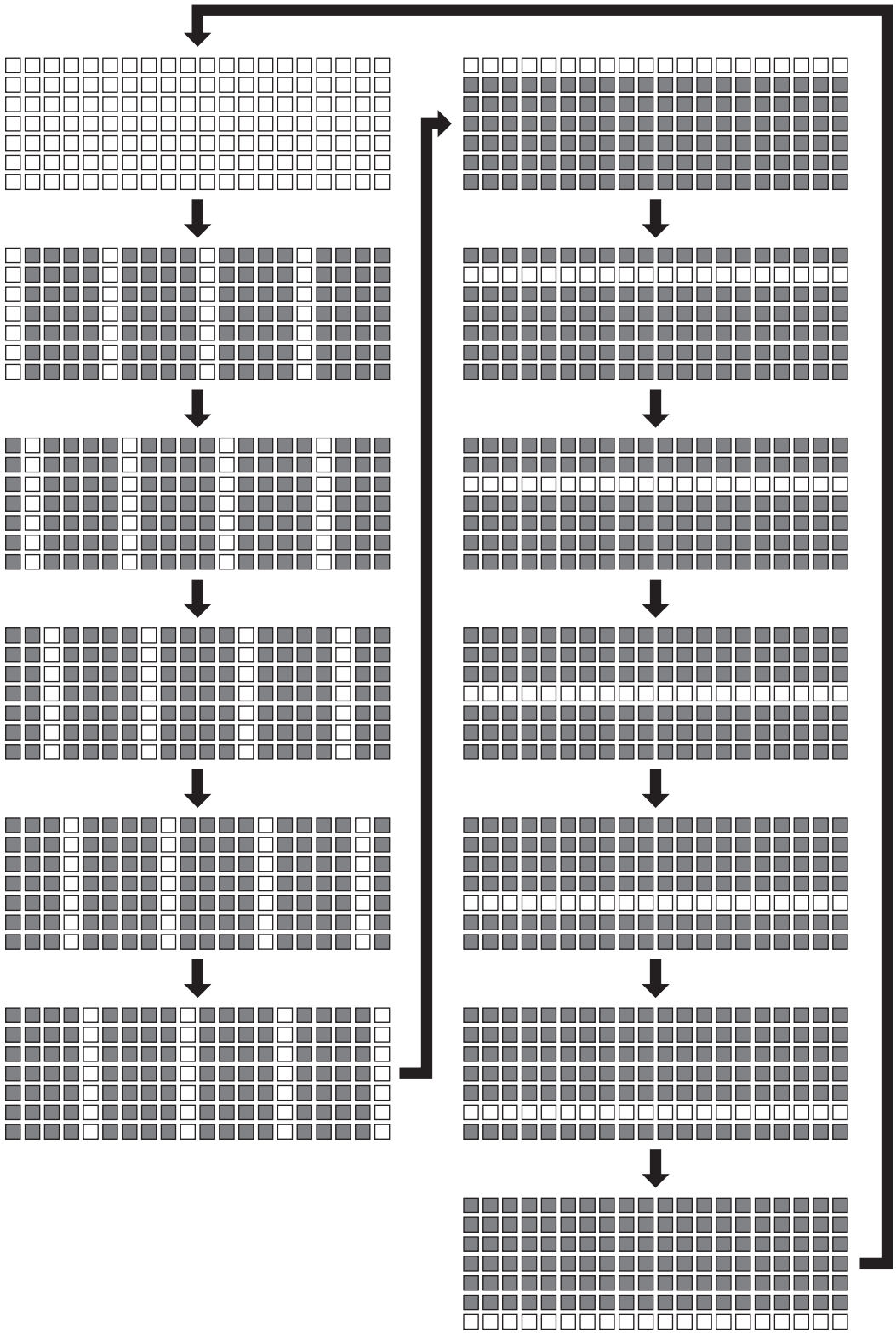
If the test completed abnormally again, a hardware failure may occur in OPC UA server module. Please consult your local Mitsubishi representative.

■Patterns for dot matrix LED check

Test patterns are turned ON in turn on the dot matrix LED.

The pattern switches every one second.

□: ON, ■: OFF



4.3 Troubleshooting by Symptom

Troubleshooting on the configuration tool

Symptom	Check point	Corrective action
Unable to connect the configuration tool to the OPC UA server module.	Is there any disconnection in the connection route?	• Connect the cables properly.
	Is the IP address specified in the connection destination specification correct?	• Review the IP address setting.
	Is the user authentication setting, the user name and the password specified in the connection destination specification correct?	• Review the user authentication setting, the user name, and the password.
	Is the IP address duplicated?	• Review the IP address setting.
	Is there a firewall and/or a proxy server in the connection route?	• Consult your network administrator about the firewall setting and/or the setting contents of the proxy server.
	Is the "Online" is selected for the mode setting of RD81OPC96?	• Select "Online" for the mode setting in an engineering tool.
	Is there any problem on the personal computer?	• Replace it with another computer.
	Is it connected directly using the Ethernet (CH2)?	• Connect it directly using the Ethernet (CH1). • When using the Ethernet (CH2), connect it via a hub.
	Is it connected to the Ethernet port which is not selected to use in the network setting?	• Connect to the Ethernet port which is selected to use in the network setting. • Enable the setting of the connected Ethernet port.
	Are multiple IP addresses enabled on the personal computer side at the same time?	• When using direct connection, review the network setting so that multiple IP addresses are not enabled on the personal computer. • Disable the wireless LAN.
	Is the direct connection specified for the connection destination?	• When using direct connection, connect the OPC UA server module (CH1) to the personal computer on a 1:1 basis.
	Is "Use the user authentication" unselected in the connection destination specification at the first startup of an OPC UA server module?	• At the first startup of an OPC UA server module, select "Use the user authentication" in the connection destination specification, and enter the default user name and password to connect. For details, refer to 'PROCEDURE BEFORE OPERATION' in the following manual. (MELSEC iQ-R OPC UA Server Module User's Manual (Startup))
	Is any one of the following input signals OFF? • Module READY (X0) • OPC UA server status (X1) • Ethernet port status (X5)	• Wait for the input signal to turn ON.
	Has a setting file error (error code: 1C10H) occurred?	❶ Use the latest version of the configuration tool. ❷ Access the OPC UA server module as the default user. ❸ Delete the settings of the functions that are not supported by the firmware version of the OPC UA server module, and write the settings again. (☞ Page 130 Added and Changed Functions)
	Has a setting file error (error code: 1C12H) occurred?	❶ Use the latest version of the configuration tool. ❷ Access the OPC UA server module as the default user. ❸ Review the security setting, and write the setting again. (☞ Page 44 Security Setting)

Symptom	Check point	Corrective action
Unable to open the project file.	Is an old version of the configuration tool used?	• Use the latest version of the configuration tool.
	Is a file which has the extension other than '.mxcfg' specified?	• Specify a file which has the '.mxcfg' extension.
	Is the specified project file corrupted?	• Specify another project file.
Unable to read the data from the OPC UA server module or display the information of the OPC UA server module.	Is a project file in the module corrupted?	• Replace the SD memory card. • Format the SD memory card in the SD memory card diagnostic of the configuration tool.
When verifying a setting between the configuration tool and an OPC UA server module to which the same setting as one set in the configuration tool is written, the result is mismatched.	Is the setting verified in the configuration tool the version of which is '1.00A'?	Update the configuration tool to the latest version before verification.

Troubleshooting on LED indication and I/O signals

Symptom	Check point	Corrective action
The RUN LED does not turn ON.	Is the module in preparation?	• Wait for the startup of the OPC UA server module to complete. (It may take several minutes for the RUN LED to turn ON depending on the system configuration.)
	Is 'Module READY' (X0) OFF?	• The watchdog timer error may occur. Please consult your local Mitsubishi representative.
	Is "Online(Asynchronous Mode)" selected for the mode setting of an OPC UA server module the firmware version of which is '01'?	• Change the mode setting to "Online". (☞ Page 74 Various operation settings) • Use an OPC UA server module the firmware version of which is '02' or later.
The RUN LED is flashing.	Is the module selected as the target for online module change?	• Turn ON the module selection cancel request flag (SM1615).
The RUN LED is OFF.	Is the module ready to be exchanged in the process of online module change?	• Perform the online module change function. For details, refer to the following: (📖MELSEC iQ-R Online Module Change Manual)
The ERR LED is ON or flashing.	Is any of the input signals (X10 to X14) ON?	• According to the error code stored by the error detection shown on the left side, check the error description and take a corrective action. (☞ Page 87 Error Code List)
	Check the error code in the system monitor of an engineering tool.	• By the error code, check the error description and take a corrective action. (☞ Page 87 Error Code List)
'Module READY' (X0) does not turn ON, or it takes time to turn ON.	Is the module in preparation?	• Wait for the startup of the OPC UA server module to complete. (It may take several minutes for 'Module READY' (X0) to turn ON depending on the number of access target device settings.)
	Is an SD memory card containing unnecessary files used?	• Format the SD memory card in the SD memory card diagnostic of the configuration tool, and write the setting to use.
	Is the RUN LED turned OFF?	• The watchdog timer error may occur. Please consult your local Mitsubishi representative.
The contents of the dot matrix LED display cannot be switched even though the dot matrix LED display mode switch (SELECT/MODE/SHOW switch) is operated.	Is the contents of SELECT/MODE/SHOW switch item blank in [Module Diagnostics] ⇨ [Module Information List] of the engineering tool?	• The dot matrix LED display mode switch (SELECT/MODE/SHOW switch) failure may occur. Please contact your local Mitsubishi Electric sales office or representative.

Troubleshooting on network connection

Symptom	Check point	Corrective action
Unable to access the OPC UA server module.	Is an Ethernet cable connected to CH1 or CH2?	• Connect an Ethernet cable to CH1 or CH2.
	Is there any disconnection in the connection route?	• Connect the cables properly.
	Is the IP address duplicated in other devices on the network?	• Review the IP address setting.
	Is there any problem in the network setting of the personal computer?	• Check the network setting of the personal computer.
	Is it connected directly using the Ethernet (CH2)?	• Connect it directly using the Ethernet (CH1). • When using the Ethernet (CH2), connect it via a hub.
	Is it connected to the Ethernet port which is not selected to use in the network setting?	• Connect to the Ethernet port which is selected to use in the network setting. • Enable the setting of the connected Ethernet port.
	Are multiple IP addresses enabled on the personal computer side at the same time?	• When using direct connection, review the network setting so that multiple IP addresses are not enabled on the personal computer. • Disable the wireless LAN.
	Was an attempt made to connect directly via a hub?	• When using direct connection, connect the OPC UA server module (CH1) to the personal computer on a 1:1 basis.
	Is any one of the following input signals OFF? • Module READY (X0) • OPC UA server status (X1) • Ethernet port status (X5)	• Wait for the input signal to turn ON.

Troubleshooting on access target device communication

Symptom	Check point	Corrective action
Unable to communicate with a specified access target device.	Is there any device for which the remote password setting is enabled on the communication route with an access target device if a response timeout error (error code: 1824H) is notified?	• Disable the remote password setting. • Unlock the remote password.
	Is there any device for which the same IP address is set on the same network when communicating with an access target device via the Ethernet route?	• Do not use the device to which the same IP address is set on the same network. • Set the IP address to devices without duplication.

Troubleshooting on connection with an OPC UA client

Symptom	Check point	Corrective action
Unable to connect from an OPC UA client to an OPC UA server module.	Has an error occurred in the OPC UA client?	• If an error occurs, check the error and take a corrective action.
	Is the setting of the connection destination OPC UA server of the OPC UA client correct?	• Review the setting of the connection destination OPC UA server of the OPC UA client.
	Is there any device to which the same IP address is set on the same network?	• Do not use the device to which the same IP address is set on the same network. • Set the IP address to devices without duplication.
	Are the security settings of the OPC UA server module and the OPC UA client correct?	• Review the security settings of the OPC UA server module and the OPC UA client.
	Are the expiration dates of the server certificate and the client certificate correct?	• Download the server certificate and the client certificate, check their expiration dates, and take a corrective action.
	Is it connected using the Ethernet (CH2)?	• Connect it using the Ethernet (CH1).
	Is any one of the following input signals OFF? • Module READY (X0) • OPC UA server status (X1) • Ethernet port status (X5)	• Wait for the input signal to turn ON.
It takes time or a timeout occurs when connecting from an OPC UA client to an OPC UA server module.	Is the number of certificates uploaded to "Trust List" in the "Manage Application Certificate" screen 100 or less[*1]?	Delete an unnecessary certificate from "Trust List".
	Is the number of certificates uploaded to "Trust List" in the "Manage User Certificate" screen 100 or less[*1] when authenticating a user with a certificate?	Delete an unnecessary certificate from "Trust List".
The list of denied certificates is not updated when connecting from an OPC UA client to an OPC UA server module.	• Is the number of certificates stored in "Denied Certificate List" in the "Manage User Certificate" screen 100 or less? • Is the number of certificates stored in "Denied Certificate List" in the "Manage Application Certificate" screen 100 or less?	• Delete an unnecessary certificate from "Denied Certificate List". • Perform the following procedure. ❶ Download a certificate to trust from "Denied Certificate List". ❷ Upload it to "Trust List". ❸ Delete an unnecessary certificate from "Denied Certificate List".
A tag value in the address space is not updated.	Has an error occurred in the module of the target tag?	• If an error occurs, check the error and take a corrective action.
	Is the polling cycle setting of the OPC UA server module correct?	• Review the polling cycle setting of the OPC UA server module.
A value of the OPC UA client is not applied to a tag of the address space.	Has an error occurred in the module of the target tag?	• If an error occurs, check the error and take a corrective action.
	Was the relevant device value manipulated in the CPU module?	• Do not manipulate the device value in the CPU module at the timing of operating from the OPC UA client.

*1 Reference for reducing the connection time

Troubleshooting on an SD memory card

Symptom	Check point	Corrective action
Settings were erased while the power was OFF	Is there a problem with the type of SD memory card?	• Replace the SD memory card with an available one. MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
	Was the power turned OFF or the control CPU reset during writing to the SD memory card?	• Do not turn the power OFF or reset the control CPU during writing to the SD memory card.
Unable to recognize the SD memory card.	Is the SD memory card inserted correctly?	• Remove the SD memory card once, and insert it again.
	Was the power turned OFF or the control CPU reset during writing to the SD memory card?	• Do not turn the power OFF or reset the control CPU during writing to the SD memory card. • Format the SD memory card in the configuration tool.

4.4 Error Code List

This section shows the error code list.

If a system error occurs, please contact your local Mitsubishi Electric sales office or representative.

Error code	Error name	Error description	Corrective action
1800H	Unsupported device error	A device unsupported by OPC UA Server module exists on the access route.	• Review the device on the access route.
1801H to 1802H	Incorrect access target error	Incorrect setting values in the [Communication Settings].	• Review the settings in the [Communication Settings].
1803H	Incorrect access target error	A device/access route unsupported by OPC UA Server module is set in the [Communication Settings].	• Review the settings in the [Communication Settings]. • Check if there is any problem on the route to the target device.
1804H	Incorrect access target error	A device unsupported by OPC UA Server module is set in the [Communication Settings].	• Review the settings in the [Communication Settings].
1805H	Incorrect access target error	A non-accessible device is set in the [Communication Settings].	• Review the settings in the [Communication Settings].
1806H	Device memory type error	A non-existent device memory type is specified. (Or the size of device memory exceeds the applicable range.)	• Review the device memory type entered in the [Address space(Tag)].
1807H	Device memory No. error	A non-existent device memory No. is specified.	• Review the device memory number entered in the [Address space(Tag)].
1808H	Target device communication error	An error has occurred when accessing the target device.	• Check if the settings in the [Communication Settings] are correct. • Check the status of the target device. • Check if the route to the target device is correct. • Check if there is any problem on the route to the target device.
1809H	Data receive error	Failed to receive the data.	• Review the device on the access route.
180AH	Size error	The device size exceeded the device range.	• Review the device memory number entered in the [Address space(Tag)].
180BH	Block error	The block No. of the specified extension file register is invalid.	• Check the block No. of the extension file register (device type).
180CH	Data receive error	Failed to receive the data.	• Review the device on the access route.
180DH	Write protect error	The block No. of the specified extension file register has been allocated to the write-protect area of the memory cassette.	• Check the block No. of the extension file register (device type). • Check the write-protect DIP switch on the memory cassette of the target device.
180EH	Incorrect access target device error	The device type set in the [Communication Settings] is different from the one of the actual target device.	• Review the settings in the [Communication Settings].
180FH	Incorrect access target error	Incorrect station No. is specified in the [Communication Settings].	• Review the settings in the [Communication Settings].
1810H	ROM operation error	Writing a TC setting value was attempted to the programmable controller CPU that was running the ROM.	• Change the TC setting value during RAM operation.
1811H	Incorrect target device settings error (Start I/O No.)	Incorrect start I/O No. is specified in the [Communication Settings].	• Review the settings (start I/O No.) of the [Communication Settings]. • Check the configuration of the target device (start I/O No.).
1812H to 1813H	Data receive error	Failed to receive the data.	• Review the device on the access route.
1814H	Incorrect target device settings error (IP address)	Incorrect IP address is specified in the [Communication Settings].	• Review the settings (IP address) in the [Communication Settings]. • Check the configuration of the target device (IP address).
1815H to 1816H	Target device communication reception data error	Incorrect data received from the target device.	• Review the settings in the [Communication Settings]. • Check the communication cable status and Access target device status.
1817H	Unsupported device error	A device unsupported by OPC UA Server module exists on the access route.	• Review the device on the access route.

Error code	Error name	Error description	Corrective action
1818H	Data receive error	Multiple responses were received at Ethernet direct communication.	• Check if the direct connection with the module is configured on a 1:1 basis.
1819H	Incorrect target device status error	Unable to set. The OPC UA Server module is communicating with other devices at Ethernet direct communication.	• Check if the direct connection with the module is configured on a 1:1 basis.
181AH	Incorrect target device settings error (Station No./Network No.)	Incorrect Station No./Network No. are specified in the [Communication Settings].	• Review the settings (Station No./Network No.) in the [Communication Settings]. • Check the configuration of the target device (Station No./Network No.).
181BH	Target device communication connection error (IP address)	Incorrect IP address is specified in the [Communication Settings].	• Review the settings (IP address) in the [Communication Settings]. • Check the configuration of the target device (IP address).
181CH	Target device communication time-out error	No response from the target device.	• Check the status of the target device. • Review the settings in the [Communication Settings]. • Adjust the time-out setting.
181DH to 181FH	Data send error	Failed to send the data.	• Review the device on the access route.
1820H to 1823H	Data receive error	Failed to receive the data.	• Review the device on the access route.
1824H	Response time-out error	No response has been received from the other station.	• Check the communication cable status and Access target device status. • Review the time-out setting. • Review the routing parameter set for the CPU(s) on the access route. • Review the control CPU(s) of the network module(s) on the access route to the Access target device module. • Review if the access target PLC series is supported. • Check the configuration of the target device.
18FEH	Target device communication error	An error has occurred when accessing the target device.	• Check if the settings in the [Communication Settings] are correct. • Check the status of the target device. • Check if the route to the target device is correct. • Check if there is any problem on the route to the target device.
18FFH to 1900H	System error	—	—
1904H	Errors detected in the CPU module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of the CPU module.
1907H	Errors detected in the serial communication module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of the serial communication module.
190BH	Errors detected in the CC-Link module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of CC-Link module.
190CH	Errors detected in the Ethernet-equipped module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and refer to the user's manual of the Ethernet-equipped module and check the errors displayed in the source error code.
190DH	Errors detected in the CC-Link IE Field Network module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of CC-Link IE Field Network module.
190EH	Errors detected in the CC-Link IE Controller Network module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of CC-Link IE Controller Network module.
190FH	Errors detected in the MELSECNET/H network module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of MELSECNET/H network module.

Error code	Error name	Error description	Corrective action
1990H	System error	—	—
19E0H	CH1/CH2 address specified in the fourth octet setting error	The value set in the CH1/CH2 address specified in the fourth octet is out of range.	• Check if the value of 1-254 is set to the CH1/CH2 address specified in the fourth octet.
1C00H	OPC UA Server function starting error	Failed to startup OPC UA Server function.	• Please review the OPC UA server setting with configuration tool and refresh the configuration file.
1C01H	Plug-in file error	Failed to find Plug-in file.	• Please consult your local Mitsubishi representative.
1C02H	Setting file error	Failed to find setting file.	• Please consult your local Mitsubishi representative.
1C10H	Setting file error	Failed to load file information in setting file.	• Check the version of the configuration tool matches the version of the module.
1C11H	Setting file error	Failed to find system setting in setting file.	• Please consult your local Mitsubishi representative.
1C12H	Setting file error	Failed to load security setting in setting file.	• Please review the security setting with configuration tool and refresh the configuration file.
1C13H	Setting file error	Failed to load network setting in setting file.	• Please review the Network setting with configuration tool and refresh the configuration file.
1C14H	Setting file error	Failed to load OPC UA Server setting in setting file.	• Please review the OPC UA server setting with configuration tool and refresh the configuration file.
1C16H	Setting file error	Failed to find target device setting in setting file.	• Please consult your local Mitsubishi representative.
1C17H	Setting file error	Failed to load target device setting in setting file.	• Please review the Address space setting with configuration tool and refresh the configuration file.
1C1AH	Setting file error	Failed to find definition setting in setting file.	• Please consult your local Mitsubishi representative.
1C1BH	Setting file error	Failed to load polling method definition in setting file.	• Please review the Polling Method Definitions with configuration tool and refresh the configuration file.
1C1CH	Setting file error	Failed to load conversion definition in setting file.	• Please review the Conversion definitions with configuration tool and refresh the configuration file.
1F20H	Error log output error	No SD memory card has been installed or failed to write the log file.	• Install the SD memory card. • Replace the SD memory card. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
1F21H	Log information error	The log information is corrupted. Restored by deleting the previous information.	• Check the SD memory card.
1F43H	Setting file writing error	Failed to write the setting file.	• Retry the writing of the settings with configuration tool.
2121H	SD Memory card error	An error has been detected in the SD memory card.	• Format the SD memory card. • Reinsert the SD memory card. • Check the SD memory card. • Replace the SD memory card if it is damaged.
2440H	Module major error	In the multiple CPU system, the control CPU setting in the system parameters is different from that of other numbered CPU modules. An error has been detected in the I/O module or intelligent function module during the initial processing.	• Review the system parameters of the second or higher numbered CPU modules and match them with those of the smallest numbered CPU module. • The possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.

Error code	Error name	Error description	Corrective action
2450H	Module major error	A major error has been detected from the I/O module or intelligent function module.	• Check the connection status of the extension cable. • Check if the I/O module or intelligent function module is mounted correctly. • Reset the CPU module and switch it to RUN. If the same error is displayed again, a hardware failure may occur in the module. Please consult your local Mitsubishi representative.
24C0H to 24C1H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module, base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C2H	System bus error	An error was detected on the system bus.	• Check the connection status of the extension cable. • Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module, base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C3H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module, base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C4H to 24C5H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C6H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module or extension cable. Please consult your local Mitsubishi representative.
24C8H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24E0H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module or base unit. Please consult your local Mitsubishi representative.
2701H to 270AH	System error	—	—
3030H	Access target device setting error	Incorrect settings in the [Communication Settings]	• Review the settings in the [Communication Settings].
3060H	System error	—	—
30A1H	System error	—	—
30B0H	SD memory card eject error	SD memory card has been ejected without stopping file access.	• Install the SD memory card and update setting.

Error code	Error name	Error description	Corrective action
30B1H	SD memory card format error	Failed to format the SD memory card.	• Check if the SD memory card is inserted firmly. • Check if an error has occurred in the SD memory card. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
30B2H	SD memory card mount error	Failed to install the SD memory card.	• Check if the SD memory card is inserted firmly. • Replace the SD memory card. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
30B3H	No SD memory card installed	OPC UA Server module has been started without installing the SD memory card.	• Check if the SD memory card is inserted firmly. • Install the SD memory card.
30B4H	System error	—	—
30C0H	System error	—	—
30D1H to 30D2H	System error	—	—
30D3H	Target device communication error	An error has occurred when accessing the target device.	• Check if the settings in the [Communication Settings] are correct. • Check the status of the target device. • Check if the route to the target device is correct. • Check if there is any problem on the route to the target device.
30E0H	System error	—	—
3880H	System error	—	—
3881H	SD memory card access error	Failed to access the SD memory card.	• Check the SD memory card. • Replace the SD memory card if it is damaged. • Check if the SD memory card had been used in other applications. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing). • Check if the connectable SD memory card is used.
3882H	SD memory card error	Unable to operate in this module. The settings for a new version of OPC UA Server module is written in the SD memory card.	• Format the SD memory card and retry the writing of the settings with configuration tool.
3920H	System error	—	—
3921H	SD memory card access error	Failed to access the SD memory card.	• Check the SD memory card. • Replace the SD memory card if it is damaged. • Check if the SD memory card had been used in other applications. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
3940H	System error	—	—
3944H to 3948H	System error	—	—
3980H	System error	—	—
3C00H to 3C03H	Hardware failure	A hardware failure has been detected.	• Take measures to reduce noise. • Reset the CPU module and switch it to RUN. If the same error is displayed again, a hardware failure may occur in OPC UA Server module. Please consult your local Mitsubishi representative.
3C0FH	Hardware failure	A hardware failure has been detected.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.

Error code	Error name	Error description	Corrective action
3C22H	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.
3C2FH	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.
3C32H	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.

APPENDIX

Appendix 1 Module Labels

This section shows the module labels used for setting the I/O signal and buffer memory of an OPC UA server module.

Module label configuration

The name of a module label is defined in the following configurations:

"Instance name"_"Module number"."Label name"

"Instance name"_"Module number"."Label name"_D

Ex.

OPC96_1.bSts_ModuleREADY

■Instance name

The instance name of an OPC UA server module (RD81OPC96) is 'OPC96'.

■Module number

A module number is a number starting from 1, which is added to identify a module that has the same instance name.

■Label name

This is a module unique label name.

■_D

This indicates that the module label is for direct access. Without this symbol, it means a label for refresh. There are some differences between refresh and direct access as shown below.

Type	Description	Access timing
Refresh	Values written to and read from a module label are applied to a module in a batch at the time of refresh. This shortens the program execution time.	At the time of refresh
Direct access	Values written to and read from a module label are immediately applied to a module. Although the program execution time is longer than refresh, the responsiveness will be increased.	At the time of writing to/reading from module label

A

Appendix 2 I/O Signals

This section explains the I/O signals of an OPC UA server module.
The following shows the example of I/O signal assignment when the start I/O number of OPC UA server module is '0'.
A device X indicates an input signal from an OPC UA server module to a CPU module.
A device Y indicates an output signal from a CPU module to an OPC UA server module.

Precautions

As for I/O signals to a CPU module, do not output (turn ON) 'Use prohibited' signals.
Doing so may cause malfunction of a programmable controller system.

I/O signal list

The following shows the I/O signal list of an OPC UA server module.
For details on the I/O signals, refer to the following:
☞ Page 95 Input signal details
☞ Page 98 Output signal details

Input signals

Device No.	Signal name
X0	Module READY
X1	OPC UA server status
X2	Use prohibited
X3	File access status
X4	Use prohibited
X5	Ethernet port status
X6	Use prohibited
X7	Connection status
X8 to XF	Use prohibited
X10	Module stop error status
X11	Module continuation error status
X12 to X13	Use prohibited
X14	Target device error
X15 to X1F	Use prohibited

Output signals

Device No.	Signal name
Y0	Use prohibited
Y1	OPC UA server resume request
Y2	OPC UA server pause request
Y3	File access stop request
Y4	File access stop cancellation request
Y5 to YF	Use prohibited
Y10	Error clear request
Y11 to Y1F	Use prohibited

Input signal details

The following shows the details on the input signals from an OPC UA server module to a CPU module.

Module READY (X0)

This signal turns ON when OPC UA server module becomes ready after the programmable controller is powered ON from OFF or the CPU module is reset.

It turns OFF when a watchdog timer error occurs.

Do not access the buffer memory and perform online operations from configuration tool until the OPC UA server module is in READY status.

OPC UA server status (X1)

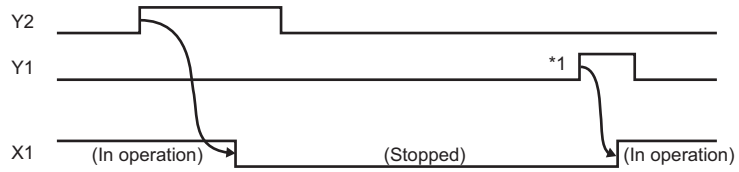
● This signal turns ON when an OPC UA server module is in operation.

It indicates that the processing of an OPC UA server module is executable.

● This signal turns OFF when an OPC UA server module is stopped.

An OPC UA server module stops in the following cases:

- The period after a programmable controller is powered OFF and ON or a CPU module is reset until an OPC UA server module is started
- A server operation is stopped in the configuration tool. (☞ Page 66 Stop of an OPC UA server module)
- A module stop error occurs in an OPC UA server module.
- While updating the settings
- While file access is stopped (📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup))



*1 If an SD memory card is reinserted (if it is unmounted once or more than once), the operation does not start. Restart the operation after updating a setting of the OPC UA server module.

A

File access status (X3)

● This signal turns ON while file access is stopped.

An SD memory card can be inserted or removed while file access is stopped. The file access will be in operation after inserting or removing an SD memory card, and this signal will turn OFF.

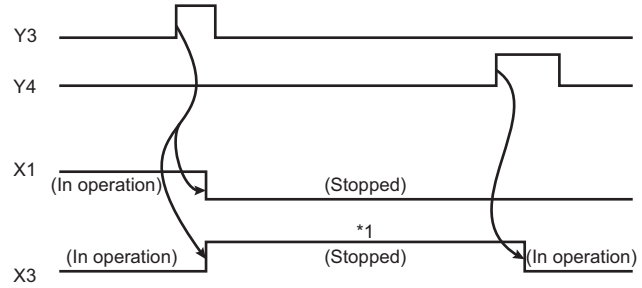
While file access is stopped, operations are as follows:

- Reading from/writing to an SD memory card are disabled.
- The operation of an OPC UA server module is stopped.
- Operations (reading/writing/verification/setting update/each diagnostic except the SD memory card diagnostic) cannot be performed in the configuration tool.

● This signal turns OFF during file access operation.

By turning the power OFF and ON or resetting a CPU module, the file access will be in operation.

However, this signal turns OFF during initialization upon powering ON from OFF.



*1 The following operations are available.

· Replacement of an SD memory card

· Power OFF of a programmable controller

For the considerations when handling an SD memory card while file access is stopped, refer to the following:

MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

Ethernet port status (X5)

This signal turns ON when either Ethernet port is available.

It turns OFF when neither Ethernet ports are available.

Connection status (X7)

This signal turns ON when a connection is established between an OPC UA server module and an OPC UA client (even one session is established).

Module stop error status (X10)

This signal turns ON while a module stop error occurs (ERR LED is flashing).

If an access target device error occurs when 'Module stop error status' (X10) or 'Module continuation error status' (X11) turns ON, 'Target device error' (X14) turns ON.

Module continuation error status (X11)

This signal turns ON while a module continuation error occurs (ERR LED is ON).

It turns OFF when 'Error clear request' (Y10) is turned ON.

Target device error (X14)

This signal turns ON when a communication error or access error with an access target device occurs.

When this signal is ON, an error code is stored in the access target status (device) area (Un\G8448 to 8703).

The signal turns OFF in the following cases:

- 'Error clear request' (Y10) is turned ON.
- The setting is updated in the configuration tool.
- A communication error or an access error has been cleared in all the access target devices.

Output signal details

The following shows the details on the output signals from an OPC UA server module to a CPU module.

OPC UA server resume request (Y1)

This signal starts the operation of an OPC UA server module according to the setting currently stored.
If an SD memory card is reinserted (if it is unmounted once or more than once), the operation does not start.
Restart the operation after updating a setting of the OPC UA server module.
When 'OPC UA server status' (X1) is ON, 'OPC UA server pause request' (Y2) needs to be executed first.
A request is not received in the following cases at the timing when an OPC UA server module monitors the output signals.

- 'OPC UA server module operation stop request' (Y2) is being executed (Y2 is ON).
- This signal turns ON simultaneously with 'OPC UA server module operation stop request' (Y2).

A request is not received before an OPC UA server module operates (it is not received if 'OPC UA server status' (X1) has never turned ON after turning the power ON).

OPC UA server pause request (Y2)

This signal sets the OPC UA server module operation to a stop state.
A request is not received in the following cases at the timing when an OPC UA server module monitors the output signals.

- 'OPC UA server module operation restart request' (Y1) is being executed (Y1 is ON).
- This signal turns ON simultaneously with 'OPC UA server module operation restart request' (Y1).

File access stop request (Y3)

This signal sets the file access to a stop state.
For ON/OFF timing, refer to the following:
☞ Page 96 File access status (X3)
For the considerations when handling an SD memory card while file access is stopped, refer to the following:
📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

File access stop cancellation request (Y4)

This signal cancels the stop state of the file access.
For ON/OFF timing, refer to the following:
☞ Page 96 File access status (X3)

Point

Even if file access is stopped by 'File access stop request' (Y3), it can be restarted by this signal.

Error clear request (Y10)

This signal turns the ERR LED, 'Module continuation error status' (X11), and 'Target device error' (X14) OFF by turning ON while a module continuation error occurs (ERR LED is ON).
It clears the latest error area (Un\G7168 to 7199).
The latest error code displayed on the system monitor of the engineering tool is cleared.

Appendix 3 Buffer Memory

This section explains the buffer memory of an OPC UA server module.

Precautions

- Do not write any data to the "system area" of the buffer memory. Doing so may cause malfunction of the programmable controller system.

A

Buffer memory list

The following table shows the buffer memory list of an OPC UA server module.

R: Read-only, W: Write-only, R/W: Readable/Writable

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
0 (0H)	Module information	LED information	RUN LED status 0: OFF, 1: ON, 2: Flashing	0	R
1 (1H)			ERR LED status 0: OFF, 1: ON, 2: Flashing	0	R
2 (2H)			OPR LED status 0: OFF, 1: ON, 2: Flashing	0	R
3 (3H)			System area	—	—
4 (4H)			CARD RDY LED status 0: OFF, 1: ON, 2: Flashing	0	R
5 (5H)			CARD ACS LED status 0: OFF, 1: ON	0	R
6 to 7 (6H to 7H)			System area	—	—
8 (8H)			Dot matrix LED display mode 1: Error code 2: CH1 IP address 3: CH2 IP address	0	R
9 to 24 (9H to 18H)			Dot matrix LED display character string[*1]	0	R
25 to 29 (19H to 1DH)		Parameter information	System area	—	—
30 (1EH)	Module information	OPC UA server function operating status 0: Initializing, 1: Running, 2: Stopping, 3: Stop		0	R
31 (1FH)		Module error status 0: No error, 1: Continuation error, 2: Stop error		0	R
32 to 85 (20H to 55H)		System area		—	—
86 to 511 (56H to 1FFH)	System area			—	—

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
512 (200H)	Network information	Ethernet port CH1 current value	Valid flag 0: Not use, 1: Use	0	R
513 (201H)		Ethernet port CH2 current value	Valid flag 0: Not use, 1: Use	0	R
514 (202H)		Ethernet port CH1 setting value	Valid flag 0: Not use, 1: Use	0	R
515 (203H)		Ethernet port CH2 setting value	Valid flag 0: Not use, 1: Use	0	R
516 to 525 (204H to 20DH)		System area		—	—
526 to 533 (20EH to 215H)		Ethernet port CH1 current value	IP address (character string)	0	R
534 to 535 (216H to 217H)			IP address	0	R
536 to 537 (218H to 219H)			Subnet mask	0	R
538 to 539 (21AH to 21BH)			Default gateway	0	R
540 to 557 (21CH to 22DH)			System area	—	—
558 to 589 (22EH to 24DH)		Ethernet port CH2 current value	Same as CH1		
590 to 653 (24EH to 28DH)		System area		—	—
654 to 661 (28EH to 295H)		Ethernet port CH1 setting value	IP address (character string)	0	R
662 to 663 (296H to 297H)			IP address	0	R
664 to 665 (298H to 299H)			Subnet mask	0	R
666 to 667 (29AH to 29BH)			Default gateway	0	R
668 to 685 (29CH to 2ADH)			System area	—	—
686 to 717 (2AEH to 2CDH)		Ethernet port CH2 setting value	Same as CH1		
718 to 1037 (2CWH to 40DH)		System area		—	—
1038 to 7167 (40EH to 1BFFH)	System area			—	—
7168 (1C00H)	Module information	Module error information	Error code	0	R
7169 (1C01H)			System area	—	—
7170 to 7177 (1C02H to 1C09H)			Error occurrence date and time	0	R
7178 to 7199 (1C0AH to 1C1FH)			System area	—	—
7200 to 7935 (1C20H to 1EFFH)	System area			—	—

A

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
7936 (1F00H)	SD memory card information	Mounting status 0: Initializing SD memory card status 1: Normal SD memory card mounting 2: Stopped file access 3: Invalid SD card mounting 4: Formatting SD memory card 5: Not inserted		0	R
7937 to 7939 (1F01H to 1F03H)		System area		—	—
7940 to 7941 (1F04H to 1F05H)		Capacity Unit: KB		0	R
7942 to 7943 (1F06H to 1F07H)		Free space Unit: KB		0	R
7944 to 7945 (1F08H to 1F09H)		Used amount Unit: KB		0	R
7946 (1F0AH)		Use rate Unit: %		0	R
7947 to 7999 (1F0BH to 1F3FH)		System area		—	—
8000 to 8447 (1F40H to 20FFH)	System area			—	—
8448 (2100H)	Target device information	Target device (1 to 16) information	Valid flag 0: Not set, 1: Set	0	R
8449 to 8455 (2101H to 2107H)			System area	—	—
8456 to 8457 (2108H to 2109H)			Connection status 0: Not connected, 1: Connecting, 2: Disconnecting	0	R
8458 to 8471 (210AH to 2117H)			System area	—	—
8472 (2118H)			Error information 0: No error, 1: Error	0	R
8473 to 8479 (2119H to 211FH)			System area	—	—
8480 to 8495 (2120H to 212FH)			Error code	0	R
8496 to 8607 (2130H to 219FH)			System area	—	—
8608 to 8703 (21A0H to 21FFH)		System area		—	—
8704 to 8705 (2200H to 2201H)	Access OPC UA client information	Access OPC UA client information	System area	—	—
8706 to 8707 (2202H to 2203H)			Number of connected clients	0	R
8708 to 8743 (2204H to 2227H)			System area	—	—
8744 to 8959 (2228H to 22FFH)		System area		—	—
8960 to 13055 (2300H to 32FFH)	System area			—	—

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
13056 (3300H)	Error log information	Error count		0	R
13057 (3301H)		Latest error log number		0	R
13058 (3302H)		Error log 1	Error code	0	R
13059 (3303H)			System area	—	—
13060 to 13067 (3304H to 330BH)			Error occurrence date and time	0	R
13068 to 13217 (330CH to 33A1H)		Error log 2 to 16	Same as error log 1		
13218 to 13391 (33A2H to 344FH)		System area		—	—
13392 to 40959 (3450H to 9FFFH)	System area			—	—

*1 The displayed characters are updated when switched. (Scrolling the displayed characters will not be considered as switching display characters.)

Buffer memory details

This section explains the buffer memory details of OPC UA server module.

Module information (Un\G0 to 85)

The LED information, OPC UA server function operating status, and module error status of an OPC UA server module are stored in this area.

For the stored values, refer to the following:

☞ Page 100 Buffer memory list

For the specifications, refer to the following:

Item	Reference
LED information	📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

■LED information (Un\G0 to 24)

The LED status, dot matrix LED display mode, and dot matrix LED display character string (ASCII format (within the range from 0x0020 to 0x007E)) are stored.

■OPC UA server function operating status (Un\G30)

The operating status of an OPC UA server function is stored.

■Module error status (Un\G31)

The error status of OPC UA server module is stored.

Network information (Un\G512 to 1037)

The connection status of an OPC UA server module to a network is stored in this area.

■Common setting (Un\G512 to 517)

Common settings for Ethernet port are stored.

Buffer memory name	Address	Description
Ethernet port CH1 current value valid flag	Un\G512	The setting status (use/ not use) of current Ethernet port (CH1) is stored. 0: Not use 1: Use
Ethernet port CH2 current value valid flag	Un\G513	The setting status (use/ not use) of current Ethernet port (CH2) is stored. The setting value is same as 'Ethernet port CH1 current value valid flag' (Un\G512).
Ethernet port CH1 setting value valid flag	Un\G514	The setting status (value set by the configuration tool) of Ethernet port (CH1) is stored. 0: Not use 1: Use
Ethernet port CH2 setting value valid flag	Un\G515	The setting status (value set by the configuration tool) of Ethernet port (CH2) is stored. The setting value is same as 'Ethernet port CH1 setting value valid flag' (Un\G514).

■Ethernet port CH1 current value (Un\G526 to 557)

The current IP address information of Ethernet port (CH1) is stored.

Buffer memory name	Address	Description
IP address (character string)	Un\G526 to 533	IP address is stored in character string. The character string to be stored is set by left justifying. (Example) "192.168.3.3"
IP address	Un\G534 to 535	IP address is stored in double word (32 bit value).
Subnet mask	Un\G536 to 537	Subnet mask is stored in double word (32 bit value).
Default gateway	Un\G538 to 539	Default gateway address is stored in double word (32 bit value). When the default gateway is not set, 0 is stored.

■Ethernet port CH2 current value (Un\G558 to 589)

The current IP address information of Ethernet port (CH2) is stored.

Each item is same as 'Ethernet port CH1 current value' (Un\G526 to 557).

■Ethernet port CH1 setting value (Un\G654 to 685)

The IP address information of the setting value of Ethernet port (CH1) (value set by the configuration tool) is stored.

Each item is same as 'Ethernet port CH1 current value' (Un\G526 to 557).

■Ethernet port CH2 setting value (Un\G686 to 717)

The IP address information of the setting value of Ethernet port (CH2) (value set by the configuration tool) is stored.

Each item is same as 'Ethernet port CH1 current value' (Un\G526 to 557).

Module information (Un\G7168 to 7199)

The latest error information of an OPC UA server module is stored in this area.

■Error code (Un\G7168)

An error code which indicates the error contents is stored. (☞ Page 87 Error Code List)

■Error occurrence date and time (Un\G7170 to 7177)

The time when the error occurred is stored in BCD code.

	b15 ··· b8	b7 ··· b0
Un\G7170	Unused	UTC offset*1
Un\G7171	Month (01H to 12H)	Year (00H to 99H) first 2 digits
Un\G7172	Hour (00H to 23H)	Day (01H to 31H)
Un\G7173	Second (00H to 59H)	Minute (00H to 59H)
Un\G7174	Year (00H to 99H) first 2 digits	Day of the week (00H to 06H)*2
Un\G7175	Lower milliseconds (00H to 99H)*3	Upper milliseconds (00H to 09H)*4
Un\G7176	System area	System area
Un\G7177	System area	System area

*1 UTC offset
-48 to 52: -12 hours to +13 hours (Unit: 15 minutes)
*2 0: Sunday, 1: Monday, 2: Tuesday, 3: Wednesday, 4: Thursday, 5: Friday, 6: Saturday
*3 Lower milliseconds: Tens digit, ones digit
*4 Upper milliseconds: Hundreds digit

SD memory card information (Un\G7936 to 7999)

The status of the SD memory card inserted in an OPC UA server module is stored in this area.

■Mounting status (Un\G7936)

The status of SD memory card is stored.

0: Initializing SD memory card status

1: Normal SD memory card mounting

2: Stopped file access

3: Invalid SD card mounting

4: Formatting SD memory card

5: Not inserted

■Capacity (Un\G7940 to 7941)

The capacity of an SD memory card is stored. (Unit: KB)

■Free space (Un\G7942 to 7943)

The free space of an SD memory card is stored. (Unit: KB)

■Used amount (Un\G7944 to 7945)

The used amount of an SD memory card is stored. (Unit: KB)

■Use rate (Un\G7946)

The use rate of an SD memory card is stored. (Unit: %)

Target device information (Un\G8448 to 8703)

The setting status of a target device is stored in this area.

■Valid flag (Un\G8448)

The setting status of the target device setting is stored.

The corresponding bit of the setting number for the set target device is turned ON.

0: Not set

1: Set

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8448	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

■Connection status (Un\G8456 to 8457)

The connection status of the target device is stored.

Depending on the connection status, values are stored in the corresponding bit of the setting number for the target device as follows:

00b: Not connected (including the case where 'Valid flag' (Un\G8448) is not set (0).)

01b: Connecting

10b: Disconnecting

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8456																
	Target device 8		Target device 7		Target device 6		Target device 5		Target device 4		Target device 3		Target device 2		Target device 1	
Un\G8457																
	Target device 16		Target device 15		Target device 14		Target device 13		Target device 12		Target device 11		Target device 10		Target device 9	

■Error information (Un\G8472)

The error information of the target device is stored.

The corresponding bit of the setting number for the target device where an error has occurred is turned ON.

0: No error

1: Error

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8472	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

■Error code (Un\G8480 to 8495)

An error code which indicates the error contents is stored to the corresponding area of the setting number for the target device in which an error occurs.

Ex.

When an error occurs in the target device set in the target device setting No.16

· Bit 15 of 'Error information' (Un\G8472) is turned ON.

· An error code is stored in 'Error code 16' (Un\G8495).

A

Access OPC UA client information (Un\G8704 to 8959)

The setting status of an access OPC UA client is stored in this area.

■Number of connected clients (Un\G8706 to 8707)

The number of connected access OPC UA clients is stored.

Error log information (Un\G13056 to 13391)

The error history occurred in an OPC UA server module is stored in this area.

■Error count (Un\G13056)

The accumulated count registered in the error log area is stored.

If the count exceeds the maximum value, the maximum value (65535) is stored.

■Latest error log number (Un\G13057)

The error log number in which the latest error log is registered is stored.*1

0: No error (No error log registered)

1 or more: Error log number in which the latest error log is registered

*1 The pointer value of "16" indicates that the latest error log has been registered in the error log area of 16.

■Error log 1 to 16 (Un\G13058 to 13217)

The error history is stored.

Error log area is comprised of 16 error logs with the same data configuration. (continuation error: up to 15, stop error: up to 1)

When a new stop error occurs in the state where a stop error is stored, the information of the stop error is updated.

An error log is not stored in the following cases.

- When an error that has already been stored in the error log area occurs again
- When a new continuation error occurs after a stop error occurs
- When a new continuation error occurs in the state where 15 continuation errors are stored

Buffer memory name	Description
Error code	An error code which indicates the error contents is stored. (☞ Page 87 Error Code List)
Error occurrence date and time	The time when the error occurred is stored in BCD code. (☞ Page 106 Error occurrence date and time (Un\G7170 to 7177))

Appendix 4 Available Characters

This section shows the characters that can be used for each setting item.

Screen	Item	Available character	Reference
Address Space (Target Device)	Name	☞ Page 110 Available ASCII characters	Page 23 Address space (access target device) setting
	Description	Characters that can be represented in Unicode	
Communication Setting	Station No.	Numbers	Page 24 Communication setting
	Start I/O No.		
	Time Out		
	Network No.		
	IP Address		
Address Space (Data Tag) ([Basic] tab)	Name	☞ Page 110 Available ASCII characters	Page 27 [Basic] tab
	Description	Characters that can be represented in Unicode	
	Remark		
	Extended number (Network No./Start I/O No.)	Numbers	
	PLC Device No. (IO Address)		
Address Space (Data Tag) ([Details] tab)	Number of elements		Page 28 [Details] tab
Address Space (Data Tag) ([Multiply] tab)	Start No.		Page 30 [Multiply] tab
	Numeric Places		
Structure Label Definitions	Label Name	☞ Page 110 Available ASCII characters	Page 32 Label
	Comment	Characters that can be represented in Unicode	
	Remark		
	Address	• Available ASCII characters[*1] ☞ Page 110 Available ASCII characters • \	Page 33 Address
Address Space (Group)	Name	☞ Page 110 Available ASCII characters	Page 38 Group setting
	Description	Characters that can be represented in Unicode	
Conversion Definitions	Name	☞ Page 110 Available ASCII characters	Page 39 Conversion Definition Setting
	Engineering Unit	• Numbers • . (decimal point), - (minus)	
	Instrument Range		
	Range		
Polling Method Definitions	Name	☞ Page 110 Available ASCII characters	Page 41 Polling Definition Setting
	Rate	Numbers	
Structure Type Declarations	Name	☞ Page 110 Available ASCII characters	Page 42 Structure Definition Setting
	Description	Characters that can be represented in Unicode	
	Comment		
	Remark		
User Account Setting	User Name	☞ Page 110 Available ASCII characters	Page 46 User account setting
	Password		

A

Screen	Item	Available character	Reference
Network Setting	IP Address	Numbers	Page 47 Network Setting
	Subnet Mask		
	Default Gateway		
	Host Name		
OPC UA Server Setting ([Connection Setting] tab)	Port No.		Page 48 [Connection Setting] tab
	End Point	• Available ASCII characters*1 ☞ Page 110 Available ASCII characters • : (colon), / (slash), . (period)	
OPC UA Server Setting ([Discovery Server] tab)	Discovery Server URL		Page 49 [Discovery Server] tab
	Registration Interval	Numbers	
OPC UA Server Setting ([Operation Setting] tab)	Waiting time		Page 49 [Operation Setting] tab
Target Setting	IP Address		Page 64 Connection destination setting

*1 Excluding underscores '_'.

Available ASCII characters

Characters in the shaded area can be used.

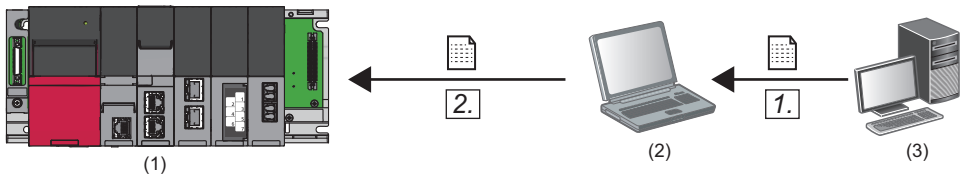
	0	1	2	3	4	5	6	7
0	NUL		(SP)	0	@	P	‘	p
1			!	1	A	Q	a	q
2			"	2	B	R	b	r
3			#	3	C	S	c	s
4			$	4	D	T	d	t
5			%	5	E	U	e	u
6			&	6	F	V	f	v
7			'	7	G	W	g	w
8			(	8	H	X	h	x
9			)	9	I	Y	i	y
A			*	:	J	Z	j	z
B			+	;	K	[	k	{
C			,	<	L		l	|
D			-	=	M	]	m	}
E			.	>	N	^	n	˜
F			/	?	O	_	o	

Appendix 5 Uploading Certificates to the Trust List

This section shows the procedure for uploading certificates to "Trust List" before connecting with an OPC UA client.
When uploading a certificate certified by a certificate authority, refer to the following:
☞ Page 115 Handling Certificates Certified by a Certificate Authority

User authentication with a certificate

For user authentication with a certificate when connecting with an OPC UA client, upload a certificate by the following procedure.



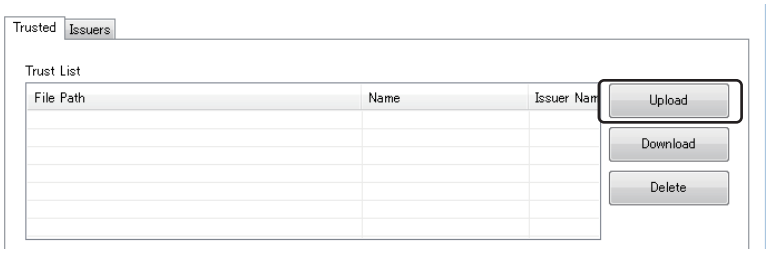
(1) OPC UA server module
(2) Configuration personal computer (configuration tool)
(3) OPC UA client

1. Store a client certificate in a personal computer on which the configuration tool is installed.
For the operation methods of an OPC UA client, refer to the manual of an OPC UA client to use.

Point

If a folder in which a client certificate is stored is unclear, perform the procedure shown in the following section.
☞ Page 112 Uploading a denied certificate to the trust list

2. Click the [Upload] button in the "Manage User Certificate" screen to upload the client certificate to "Trust List".

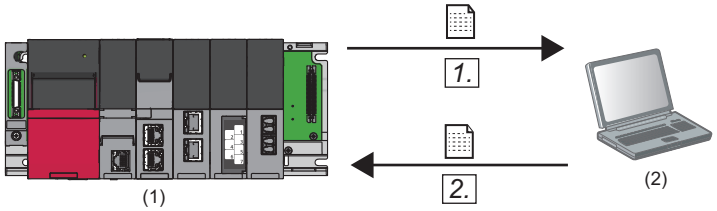


A

Uploading a denied certificate to the trust list

If a client certificate is not uploaded to "Trust List", it will be stored in "Denied Certificate List" when connecting from an OPC UA client to an OPC UA server module, and the connection will not be established.

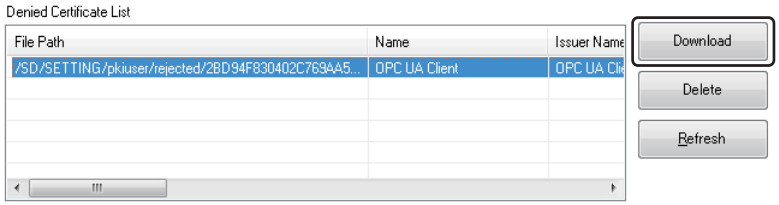
Upload a stored certificate by the following procedure.



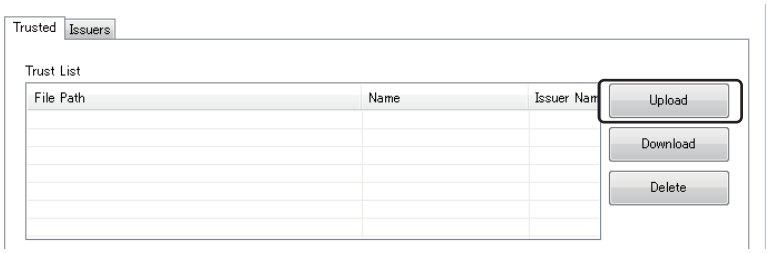
(1) OPC UA server module

(2) Configuration personal computer (configuration tool)

1. Click the [Download] button in the "Manage User Certificate" screen to download a client certificate to a personal computer.

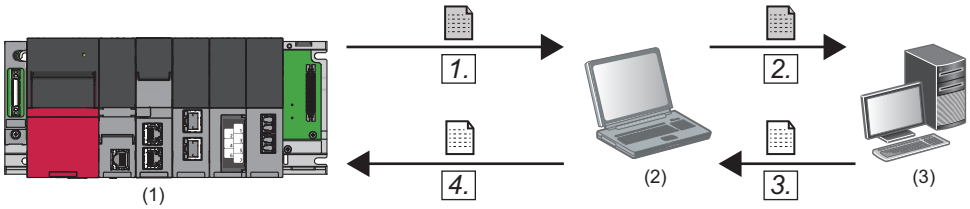


2. Click the [Upload] button in the "Manage User Certificate" screen to upload the client certificate to "Trust List".



Application authentication with a certificate

If not exchanging certificates automatically when performing application authentication with a certificate, upload a certificate by the following procedure.



(1) OPC UA server module
(2) Configuration personal computer (configuration tool)
(3) OPC UA client

1. Click the [Server Certificate Download] button in the "Manage Application Certificate" screen to download a server certificate.

Point

This step can be skipped depending on an OPC UA client to use.

2. Register the server certificate to the trust list of an OPC UA client.

For the method for registering in the trust list, refer to the manual of an OPC UA client to use.

Point

This step can be skipped depending on an OPC UA client to use.

3. Store a client certificate in a personal computer on which the configuration tool is installed.

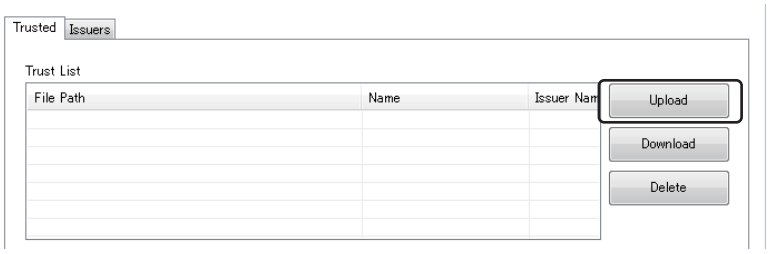
For the operation methods of an OPC UA client, refer to the manual of an OPC UA client to use.

Point

If a folder in which a client certificate is stored is unclear, perform the procedure shown in the following section.

☞ Page 114 Uploading a denied certificate to the trust list

4. Click the [Upload] button in the "Manage Application Certificate" screen to upload the client certificate to "Trust List".

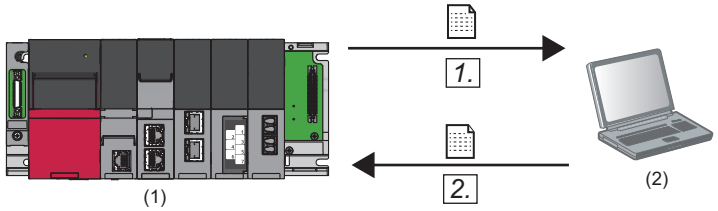


A

Uploading a denied certificate to the trust list

If a client certificate is not uploaded to "Trust List", it will be stored in "Denied Certificate List" when connecting from an OPC UA client to an OPC UA server module, and the connection will not be established.

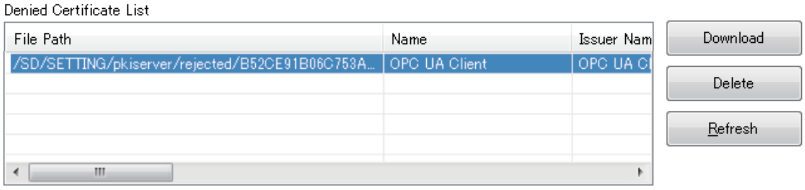
Upload a stored certificate by the following procedure.



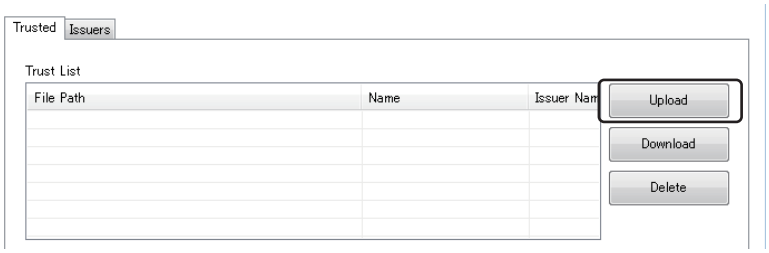
(1) OPC UA server module

(2) Configuration personal computer (configuration tool)

1. Click the [Download] button in the "Manage Application Certificate" screen to download a client certificate to a personal computer.



2. Click the [Upload] button in the "Manage Application Certificate" screen to upload the client certificate to "Trust List".

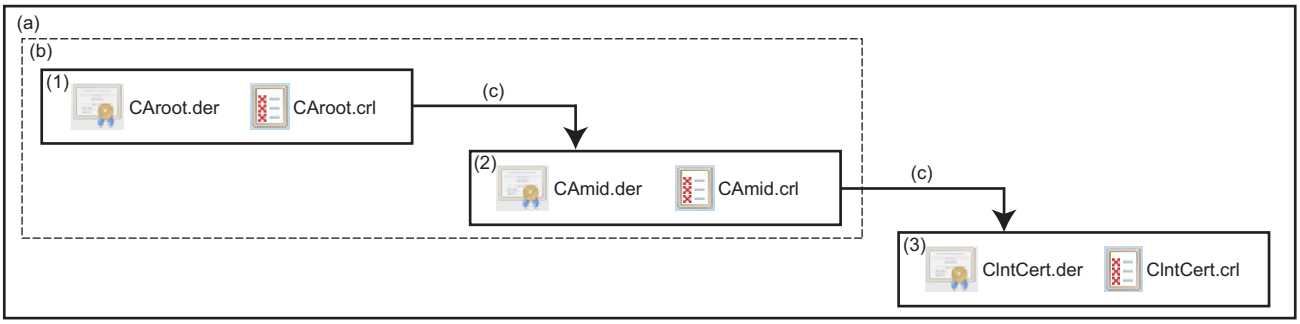


Appendix 6 Handling Certificates Certified by a Certificate Authority

This section describes the handling of certificates certified by a certificate authority.

Certificates and revocation lists that need to be uploaded

When using a certificate certified by a certificate authority, all electronic certificates issued by certificate authorities in the tree (files with the extension 'der') must be uploaded to "Trust List" in the [Trusted] or [Issuers] tab.
In addition, all certificate revocation lists issued by certificate authorities in the tree (files with the extension 'crl') must be uploaded to "Revocation List" in the tab in which electronic certificates issued by certificate authorities are uploaded. Otherwise, the electronic certificates cannot be authenticated.



(a) Certificate tree
(b) Electronic certificate issued by a certificate authority
(c) Certification
(1) Root certificate (CA_root)
(2) Intermediate certificate (CA_mid)
(3) Client certificate (ClientCert)

When uploading an electronic certificate issued by a certificate authority to "Trust List" in the [Trusted] tab, all certificates certified by the certificate authority are authenticated. In this case, a client certificate does not need to be uploaded to "Trust List" in the [Trusted] tab.
When uploading an electronic certificate issued by a certificate authority to "Trust List" in the [Issures] tab, client certificates that can be authenticated can be limited.
The following table shows the client certificates that can be authenticated for each combination of certificates uploaded to "Trust List" in the [Trusted] and [Issuers] tab.

Certificate uploaded to "Trust List" in the [Trusted] tab	Certificate uploaded to "Trust List" in the [Issures] tab	Client certificate that can be authenticated
• (1) Root certificate (CA_root) • (2) Intermediate certificate (CA_mid) • (3) Client certificate (ClientCert)*1	N/A	All client certificates authenticated by (1) root certificate or (2) intermediate certificate (including (3) client certificate (ClientCert))
• (2) Intermediate certificate (CA_mid) • (3) Client certificate (ClientCert)*1	(1) Root certificate (CA_root)	All client certificates certified by (2) intermediate certificate (including (3) client certificate (ClientCert))
(3) Client certificate (ClientCert)	• (1) Root certificate (CA_root) • (2) Intermediate certificate (CA_mid)	(3) Client certificate (ClientCert) only

*1 Not always required.

Appendix 7 Processing Time

This section explains the measurement results for the processing time required for accessing from an OPC UA server module.

The processing time may increase depending on any of the following factors:

- Usage environment (personal computer, network, and SD memory card)
- Access status from a personal computer, HMI, or other intelligent function modules to a CPU module
- Access from a personal computer in the configuration tool
- Settings of an OPC UA server module

Measurement conditions

Item		Description
Personal computer	CPU	Intel® Core™ i5-2400 3.10 GHz
	Memory	4 GB
	OS	Windows® 7 Professional
Access target device	CPU module	R08CPU

Measurement results

■INT type tag

Access target	Access type	Number of tags			
		100	1000	5000	10000
Own station (control CPU)	Reading	31 ms	350 ms	2359 ms	4358 ms
	Writing	46 ms	387 ms	2577 ms	4571 ms
Another station (via Ethernet)	Reading	—	384 ms	1916 ms	4733 ms
	Writing	—	416 ms	2733 ms	5559 ms

■INT type array tag

Access target	Access type	Number of words (number of tags)				
		1000 (8)	5000 (40)	10000 (79)	20000 (157)	50000 (391)
Own station (control CPU)	Reading	10 ms	85 ms	172 ms	554 ms	1018 ms
	Writing	106 ms	735 ms	1666 ms	3129 ms	7651 ms
Another station (via Ethernet)	Reading	—	—	633 ms	1133 ms	—
	Writing	—	—	2067 ms	3818 ms	—

Appendix 8 Log File Format

This section shows the format of a communication event log between OPC UA server modules created by an OPC UA server module.

Format specification

The following table shows the format specification.

Item	Description
Format	CSV format
Storage destination	/SD/SETTING/log
File name	YYYYMMDD-XXXX.log XXXX: Sequential number from 0000 to 9999
Character code	Shift JIS
Log output level	INFO or higher

Format description

The following table shows the format of a log file.

Item	Description
Date	An occurrence date (YYYY-MM-DD) of an event is displayed.
Time	An occurrence time (HH:MM:SS) of an event is displayed.
Category	The type of an event is displayed. • SYSTEM • COMM • OPCUA • UNIT
Level (number)	The level (number) of an event is displayed. • 1: DEBUG • 2: INFO • 3: WARNING • 4: ERROR
Level (character string)	The level (character string) of an event is displayed. • DEBUG • INFO • WARNING • ERROR
Output source	An output source of an event is displayed.
Message	The contents of an event is displayed.

A

Appendix 9 Software Licenses and Copyrights

This section describes the licenses and copyrights of software used in this product.

Jansson 2.9

Copyright© 2009-2016 Petri Lehtinen
Released under the MIT license
http://opensource.org/licenses/mit-license.php

Openssl 1.0.2j

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

■Copyright

Copyright© 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
This Windows version of this product includes software written by Tim Hudson (tjh@cryptsoft.com)

■LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts.

• OpenSSL License

Copyright© 1998-2016 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

• Original SSLeay License

Copyright© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OPC UA

This product includes code that was developed by Unified Automation GmbH for the OPC UA SDK (http://www.unifiedautomation.com/).

Copyright (c) 2006-2016 Unified Automation GmbH. All rights reserved.

The OPC UA SDK is based in part on the ANSI C Stack of the OPC Foundation. Initial version of the ANSI C Stack was founded and copyrighted by OPC Foundation, Inc.

Copyright (C) 2008, 2014 OPC Foundation, Inc., All Rights Reserved.

Appendix 10 Use in a Redundant System

To use an OPC UA server module in a redundant system, a system must be constructed for switching a monitoring target and the system when an error (disconnection between an OPC UA server module and an OPC UA client etc.) is detected in an OPC UA server module.
Switch a monitoring target in an OPC UA client, and create a sequence program for switching the system.

Point

There is no difference in operations of an OPC UA server module when used in each system in the following system configurations:

- A redundant system and a non-redundant system
- A control system and a standby system

Restriction

- For constructing a redundant system, use a process CPU the firmware version of which is '18' or later.
- Set a different IP address of an OPC UA server module for system A and system B.

Procedure for switching a monitoring target

The following shows the procedure for switching a monitoring target.
Switch a monitoring target in an OPC UA client.

Operating procedure

1. Connect to an OPC UA server module.

When the connection is successful, data in system A and system B is acquired.
If it fails, connect to the OPC UA server module again by referring to the following:
☞ Page 86 Troubleshooting on connection with an OPC UA client

2. Switch a monitoring target according to the status of 'Control system judgment flag' (SM1634) of a process CPU (redundant mode).

Status of 'Control system judgment flag' (SM1634)		Monitoring target
System A	System B	
ON	OFF	OPC UA server module in system A
OFF	ON	OPC UA server module in system B
OFF	OFF	No monitoring target Specify contents to display in an OPC UA client.

Point

For a sample (MC Works64) for displaying only data in the control system in an OPC UA client by using the control system judgment flag of a process CPU (redundant mode), refer to the following:
☞ Page 123 Example of switching a monitoring target (MC Works64)
For details on system switching for a process CPU (redundant mode), refer to the following:
MELSEC iQ-R CPU Module User's Manual (Application)

Procedure for system switching

The following shows the procedure for system switching in a redundant system.
Switch the system in a sequence program.

Operating procedure

1. Monitor the status of an OPC UA server module.

An error is detected in any of the following cases:

- 'Module READY' (X0) is OFF.
- 'Module stop error status' (X10) is ON.
- 'Ethernet port status' (X5) is OFF for a certain period of time.

2. If an error is detected, execute the system switching instruction.

Execute the system switching instruction (SP.CONTSW) in a process CPU (redundant mode) in the control system.*1

*1 To execute this instruction, 'System switching by a user' (SM1646) must be turned ON in advance.

Point

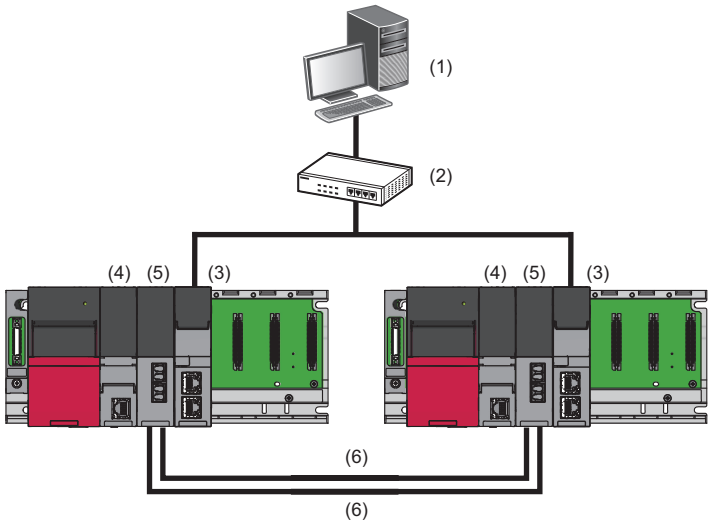
For the sample program for monitoring the link-up state by using 'Ethernet port status' (X5) of an OPC UA server module and switching the system when the link-down is detected, refer to the following:
☞ Page 127 Sample program for system switching
For details on system switching for a process CPU (redundant mode), refer to the following:
MELSEC iQ-R CPU Module User's Manual (Application)

Operation example

The following shows an operation example when using an OPC UA server module in a redundant system.

System configuration

The following shows an example of a system configuration when using an OPC UA server module in a redundant system.



(1) OPC UA client
(2) Hub
(3) OPC UA server module
(4) Process CPU (redundant mode)*1
(5) Redundant function module*1
(6) Tracking cable*1

*1 For details on a process CPU (redundant mode), refer to the following:
MELSEC iQ-R CPU Module User's Manual (Application)

Example of switching a monitoring target (MC Works64)

The following shows an example of displaying only data in the control system in GraphWorX64 in the SCADA software package, MC Works64. To display only data in the control system in GraphWorX64, use Workbench for managing settings for each application of MC Works64.

■Settings for an OPC UA server module

Write the following settings in the configuration tool.

System	IP address	Access target device name	Communication setting	Tag name	Device	Remarks
A	192.168.3.3	Dev000	Host station (default)	CONT_SYS_FLAG	SM1634	Control system judgment flag
		Dev001	Host station (default)	TARGET	D0	Monitoring target (any)
B	192.168.3.4	Same as above				

■Settings for MC Works64

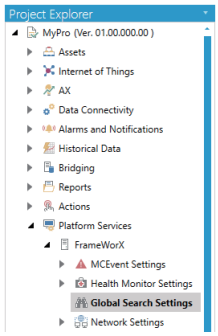
The following shows the procedure for displaying only data in the control system in GraphWorX64.

For details on MC Works64, refer to the following:

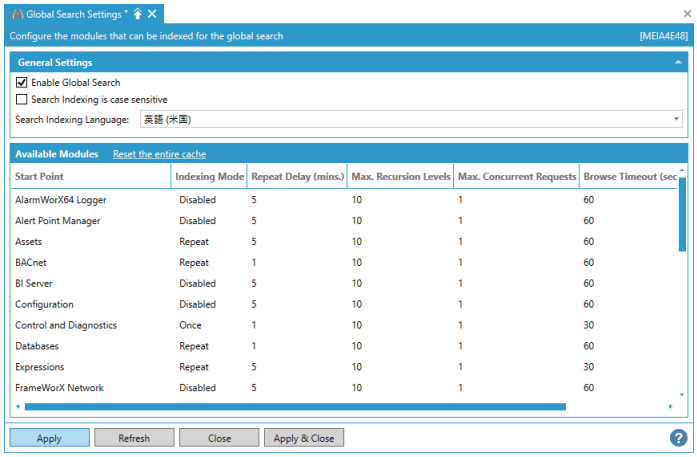
MC Works64 Version 4 Startup Manual

Operating procedure

1. Start Workbench.
2. Select "Platform Services" ⇨ "FrameWorX", and double-click "Global Search Settings".

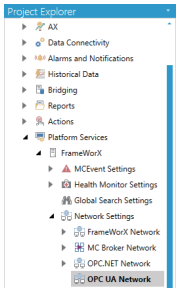


3. Select the checkbox of "Enable Global Search", and click the [Apply] button.

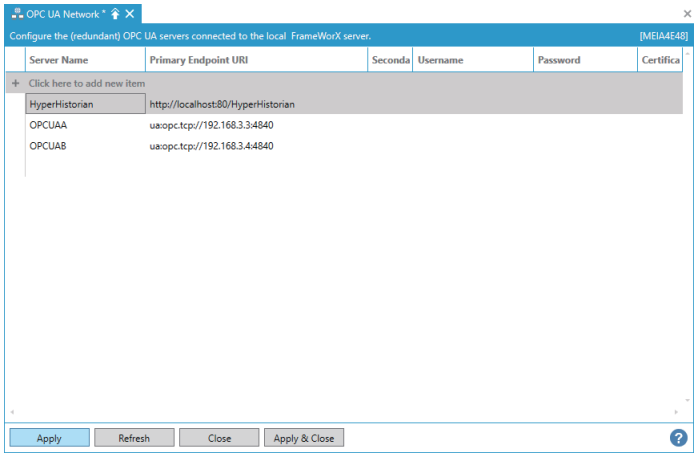


A

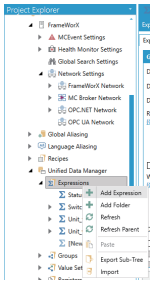
4. Select "Platform Services" ⇨ "FrameWorX" ⇨ "Network Settings", and double-click "OPC UA Network".



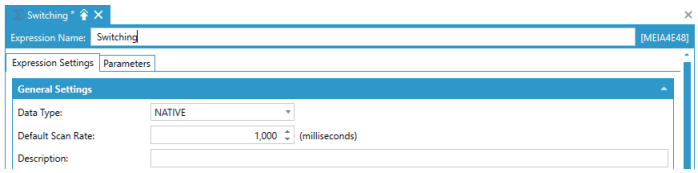
5. Add an OPC UA server module for each system A and system B, and click the [Apply] button.



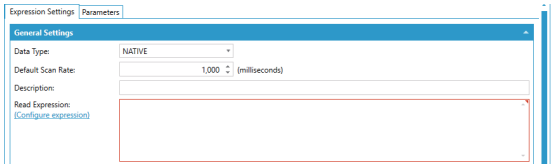
6. Select "Platform Services" ⇨ "Unified Data Manager" and right-click "Expressions", then select "Add Expression".



7. Enter a name for "Expression Name".



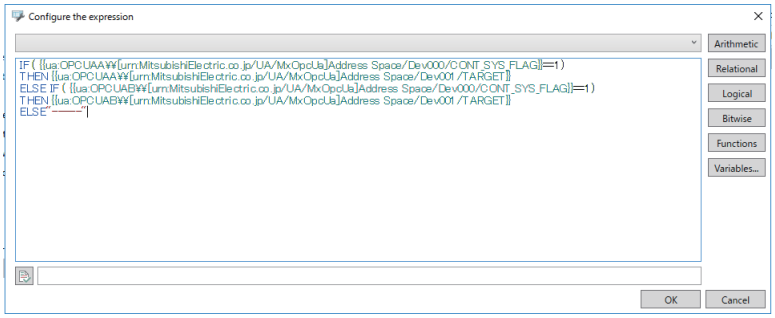
8. Click "(Configure expression)" under "Read Expression" in the [Expression Settings] tab.



9. Enter an expression in the "Configure the expression" screen, and click the [OK] button.

For an expression to enter, refer to the following:

☞ Page 126 Expression example



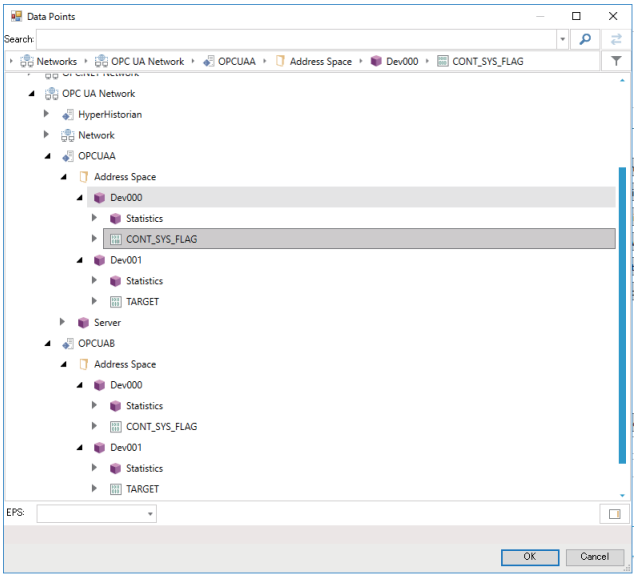
Point

A variable can automatically be entered by clicking it in the "Configure the expression" screen and selecting a target tag in "OPC UA Network" in the "Data Points" screen.

(Example) Select "OPC UA Network" ⇨ "OPCUAA" ⇨ "Address Space" ⇨ "Dev000" ⇨ "CONT_SYS_FLAG" in the "Data Points" screen, and click the [OK] button.

The following is applied in the "Configure the expression" screen.

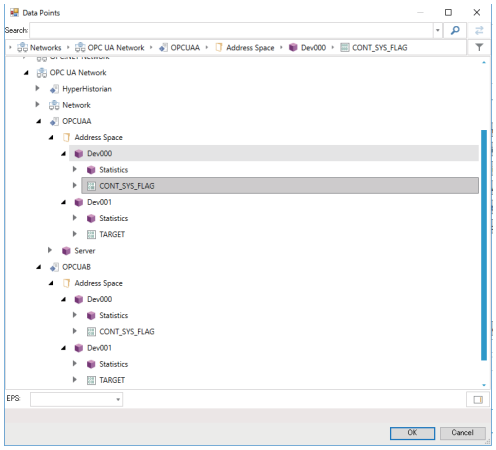
{{ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev000/CONT_SYS_FLAG}}



10. Start GraphWorX64.

11. Assign the expression created in step 9 to a data source such as a process point in the "Data Browser" screen.
The expression created in step 9 is displayed by selecting the following items:

"Platform Services" ⇨ "Expressions"



■Expression example

The following shows an example of processing for switching a monitoring target by using the control system judgment flag.

```
x=IF({{ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev000/CONT_SYS_FLAG}}==1)
THEN({{ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev001/TARGET}})
ELSE IF({{ua:OPCUAB\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev000/CONT_SYS_FLAG}}==1)
THEN({{ua:OPCUAB\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev001/TARGET}})
ELSE("-----")
```

Item	Description
ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]	An OPC UA server module added to an OPC UA network (system A)
ua:OPCUAB\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]	An OPC UA server module added to an OPC UA network (system B)
Dev000	An access target device name set in the configuration tool (system A)
Dev001	An access target device name set in the configuration tool (system B)
CONT_SYS_FLAG	A tag name set in the configuration tool
TARGET	A tag name set in the configuration tool
"-------"	A character string displayed in GraphWorX64 when data missing occurs

Precautions

- When applying this sample program to an actual system, ensure the applicability and confirm that it will not cause system control problems.
- A character string displayed when data missing occurs may be displayed depending on the timing of system switching or system startup.
- Data update in an OPC UA server module and data collection (display) in MC Works64 are not synchronized.
- An OPC UA server module in system A and one in system B do not operate synchronously.

Sample program for system switching

The following shows the sample program for monitoring the link-up state by using 'Ethernet port status' (X5) of an OPC UA server module and switching the system in a process CPU (redundant mode) when link-down is detected.

■Settings for an OPC UA server module

For the setting method of an OPC UA server module, refer to the following:

☞ Page 123 Example of switching a monitoring target (MC Works64)

■Settings for a process CPU (redundant mode)

The following shows the procedure for setting a process CPU (redundant mode).

Operating procedure

1. Start GX Works3.
2. Select [Project] ⇨ [New], and set the following items:

Item	Description
Series	RCPU
Type	R32P
Mode	Redundant
Program Language	Ladder

3. Add module labels.
4. Open the "Module Configuration" window, and set the following modules:

Slot	Module name	Start XY*1
CPU	R32PCPU	3E00
0	R6RFM	0000
1	RD81OPC96	0020

*1 Select [Edit] ⇨ [Start XY Batch Input] to set this item.

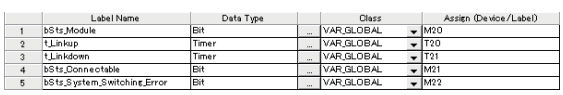
5. Select [Edit] ⇨ [Parameter] ⇨ [Fix] to fix the parameters.
6. Add a module.
7. Set the redundant settings.

For details on the redundant settings, refer to the following:

MELSEC iQ-R CPU Module User's Manual (Application)

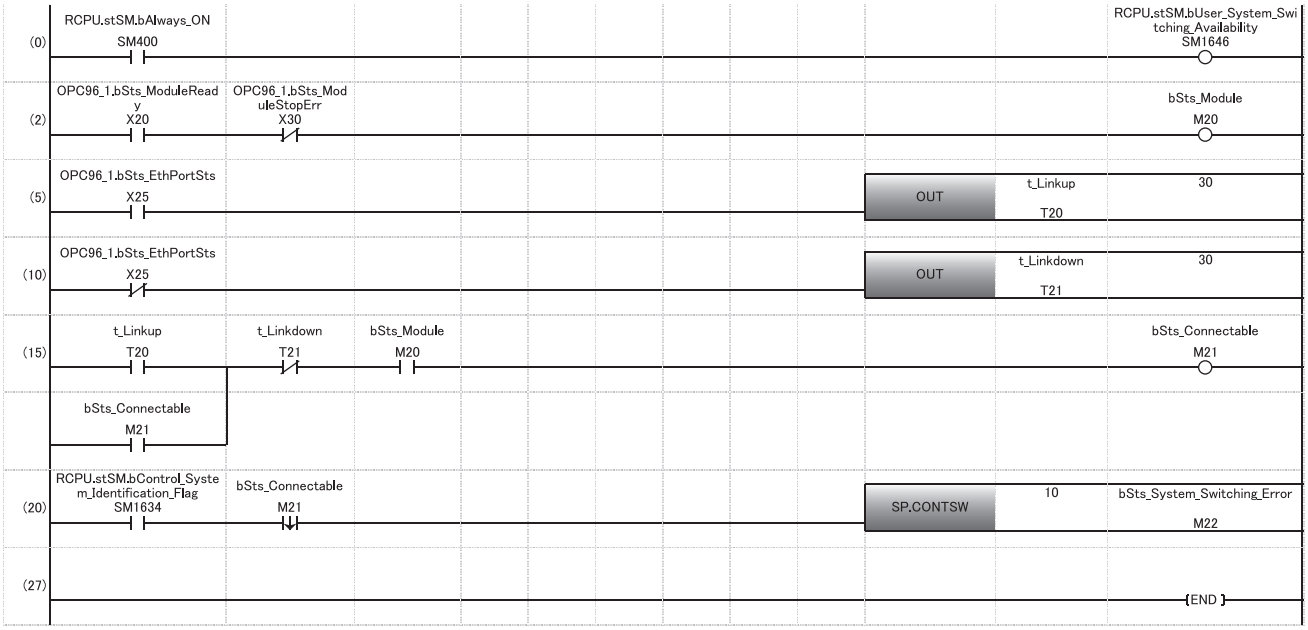
8. Write the sample program for system switching.

■Devices used in the sample program for system switching

Category	Label name	Description	Device
Module labels	RCPU.stSM.bAlways_ON	Always ON	SM400
	RCPU.stSM.bControl_System_Identification_Flag	Control system judgment flag	SM1634
	RCPU.stSM.bUser_System_Switching_Availability	System switching by a user	SM1646
	bSts_ModuleReady	Module READY status	X20
	bSts_ModuleStopErr	Module stop error status	X30
	bSts_EthPortSts	Ethernet port status	X25
Global labels to be defined	Define global labels as follows: 		

	Label Name	Data Type		Class	Assign (Device/Label)
1	bSts_Module	Bit	...	VAR_GLOBAL	M20
2	t_Linkup	Timer	...	VAR_GLOBAL	T20
3	t_Linkdown	Timer	...	VAR_GLOBAL	T21
4	bSts_Connectable	Bit	...	VAR_GLOBAL	M21
5	bSts_System_Switching_Error	Bit	...	VAR_GLOBAL	M22

■Sample program for system switching



(0) Turns 'System switching by a user' (SM1646) ON.

(2) Monitors the status of an OPC UA server module.*1
Uses 'Module READY' (X0) and 'Module stop error status' (X10) of the OPC UA server module to set a condition used for system switching as an internal relay.

(5) Monitors the Ethernet port status of the OPC UA server module.
Sets a timer value used for link-up detection.*1

(10) Monitors the Ethernet port status of the OPC UA server module.
Sets a timer value used for link-down detection.*1

(15) Monitors if the connection with the OPC UA client is available.
Uses (2), (5), and (10) to set a condition used for system switching as an internal relay.

(20) Executes the system switching instruction.
Executes the system switching instruction when the internal relay set in the control system and (15) falls.

*1 Change a condition and a timer value used for system switching according to an environment.

Precautions

The following shows the considerations for using the sample program for system switching and programming for a redundant system.

■Considerations for using the sample program for system switching

- When applying this sample program to an actual system, ensure the applicability and confirm that it will not cause system control problems.
- 'Ethernet port status' (X5) of an OPC UA server module turns ON when link-up is detected in either of Ethernet port (CH1) or Ethernet port (CH2). When monitoring the status between an OPC UA server module and an OPC UA client, do not use Ethernet port (CH2) of an OPC UA server module.
- The link-up state of Ethernet port (CH1) of an OPC UA server module is used for system switching in this sample program. If a hub is used between an Ethernet port of an OPC UA server module and one of an OPC UA client, link-down between the Ethernet port of the OPC UA client and the hub cannot be detected.
- An OPC UA server module in system A and one in system B do not operate synchronously.
- The system is switched regardless of the status of an OPC UA server module in the standby system in this sample program.

■Considerations for programming for a redundant system

- Create a program executed in both systems.
- Exclude a device used for a program from targets for tracking transfer.

Appendix 11 Added and Changed Functions

This section shows the added and changed functions of an OPC UA server module and MX OPC UA Module Configurator-R.

Added/changed contents	Firmware version	Software version	Reference
Importing global labels and common device comments is supported.	—	'1.01B' or later	Page 50 Global Label and Common Device Comment Import Function
Structures and structure labels are supported.	'02' or later		Page 31 Structure label setting Page 42 Structure Definition Setting
Authentication with a user certificate is supported.			Page 44 Security Setting Page 71 User certificate management
A security policy is added. • Basic256Sha256			Page 48 OPC UA Server Setting
OPC UA specification 1.03 is complied with.		—	MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
Multilevel structures*1 are supported.	'03' or later	'1.03D' or later	Page 31 Structure label setting Page 42 Structure Definition Setting

*1 A structure that contains a structure as a member.

MEMO

INDEX

MEMO

REVISIONS

*The manual number is given on the bottom left of the back cover.

Revision date	*Manual number	Description
April 2017	SH(NA)-081694ENG-A	First edition
December 2018	SH(NA)-081694ENG-B	■Added or modified parts TERMS, Section 1.1, Section 2.3, Section 2.6, Section 2.7, Section 2.9, Section 2.10, Section 2.11, Section 4.3, Appendix 4, Appendix 5, Appendix 6, Appendix 10
February 2019	SH(NA)-081694ENG-C	Partial correction
May 2019	SH(NA)-081694ENG-D	■Added or modified part Section 2.6, Appendix 9, Appendix 10, Appendix 11

Japanese manual number: SH-081692-D

WARRANTY

Please confirm the following product warranty details before using this product.

1. Gratis Warranty Term and Gratis Warranty Range

If any faults or defects (hereinafter "Failure") found to be the responsibility of Mitsubishi occurs during use of the product within the gratis warranty term, the product shall be repaired at no cost via the sales representative or Mitsubishi Service Company.

However, if repairs are required onsite at domestic or overseas location, expenses to send an engineer will be solely at the customer's discretion. Mitsubishi shall not be held responsible for any re-commissioning, maintenance, or testing on-site that involves replacement of the failed module.

[Gratis Warranty Term]

The gratis warranty term of the product shall be for one year after the date of purchase or delivery to a designated place. Note that after manufacture and shipment from Mitsubishi, the maximum distribution period shall be six (6) months, and the longest gratis warranty term after manufacturing shall be eighteen (18) months. The gratis warranty term of repair parts shall not exceed the gratis warranty term before repairs.

[Gratis Warranty Range]

(1) The range shall be limited to normal use within the usage state, usage methods and usage environment, etc., which follow the conditions and precautions, etc., given in the instruction manual, user's manual and caution labels on the product.

(2) Even within the gratis warranty term, repairs shall be charged for in the following cases.

1. Failure occurring from inappropriate storage or handling, carelessness or negligence by the user. Failure caused by the user's hardware or software design.
2. Failure caused by unapproved modifications, etc., to the product by the user.
3. When the Mitsubishi product is assembled into a user's device, Failure that could have been avoided if functions or structures, judged as necessary in the legal safety measures the user's device is subject to or as necessary by industry standards, had been provided.
4. Failure that could have been avoided if consumable parts (battery, backlight, fuse, etc.) designated in the instruction manual had been correctly serviced or replaced.
5. Failure caused by external irresistible forces such as fires or abnormal voltages, and Failure caused by force majeure such as earthquakes, lightning, wind and water damage.
6. Failure caused by reasons unpredictable by scientific technology standards at time of shipment from Mitsubishi.
7. Any other failure found not to be the responsibility of Mitsubishi or that admitted not to be so by the user.

2. Onerous repair term after discontinuation of production

(1) Mitsubishi shall accept onerous product repairs for seven (7) years after production of the product is discontinued. Discontinuation of production shall be notified with Mitsubishi Technical Bulletins, etc.

(2) Product supply (including repair parts) is not available after production is discontinued.

3. Overseas service

Overseas, repairs shall be accepted by Mitsubishi's local overseas FA Center. Note that the repair conditions at each FA Center may differ.

4. Exclusion of loss in opportunity and secondary loss from warranty liability

Regardless of the gratis warranty term, Mitsubishi shall not be liable for compensation to:

(1) Damages caused by any cause found not to be the responsibility of Mitsubishi.

(2) Loss in opportunity, lost profits incurred to the user by Failures of Mitsubishi products.

(3) Special damages and secondary damages whether foreseeable or not, compensation for accidents, and compensation for damages to products other than Mitsubishi products.

(4) Replacement by the user, maintenance of on-site equipment, start-up test run and other tasks.

5. Changes in product specifications

The specifications given in the catalogs, manuals or technical documents are subject to change without prior notice.

TRADEMARKS

Ethernet is a registered trademark of Fuji Xerox Co., Ltd. in Japan.
Intel is either a registered trademark or a trademark of Intel Corporation in the United States and/or other countries.
Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Unicode is either a registered trademark or a trademark of Unicode, Inc. in the United States and other countries.
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.

SH(NA)-081694ENG-D(1905)KWIX
MODEL: RD81OPC96-U-OU-E
MODEL CODE: 13JX64

MITSUBISHI ELECTRIC CORPORATION

HEAD OFFICE : TOKYO BUILDING, 2-7-3 MARUNOUCHI, CHIYODA-KU, TOKYO 100-8310, JAPAN
NAGOYA WORKS : 1-14 , YADA-MINAMI 5-CHOME , HIGASHI-KU, NAGOYA , JAPAN