MITSUBISHI ELECTRIC

Programmable Controller

MELSEC iQ-F series

MELSEC iQ-F
FX5 OPC UA Module User's Manual

-FX5-OPC

SAFETY PRECAUTIONS

(Read these precautions before use.)

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

This manual classifies the safety precautions into two categories: [⚠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.

Depending on the circumstances, procedures indicated by [⚠CAUTION] may also cause severe injury.

It is important to follow all precautions for personal safety.

Store this manual in a safe place so that it can be read whenever necessary. Always forward it to the end user.

[DESIGN PRECAUTIONS]

⚠WARNING

- Make sure to set up the following safety circuits outside the PLC to ensure safe system operation even during external power supply problems or PLC failure. Otherwise, malfunctions may cause serious accidents.
  - Most importantly, set up the following: an emergency stop circuit, a protection circuit, an interlock circuit for opposite movements (such as normal vs. reverse rotation), and an interlock circuit (to prevent damage to the equipment at the upper and lower positioning limits).
  - Note that when the CPU module detects an error, such as a watchdog timer error, during self-diagnosis, all outputs are turned off. Also, when an error that cannot be detected by the CPU module occurs in an input/output control block, output control may be disabled. External circuits and mechanisms should be designed to ensure safe machinery operation in such a case.
  - Note that when an error occurs in a relay, transistor or triac of an output circuit, the output might stay on or off. For output signals that may lead to serious accidents, external circuits and mechanisms should be designed to ensure safe machinery operation in such a case.
- 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.
- For the operating status of each station after a communication failure of the network, refer to relevant manuals for the network. Incorrect output or malfunction may result in an accident.
- Construct an interlock circuit in the program so that the whole system always operates on the safe side before executing the control (for data change) of the PLC in operation.
  Read the manual thoroughly and ensure complete safety before executing other controls (for program change, parameter change, forcible output and operation status change) of the PLC in operation. Otherwise, the machine may be damaged and accidents may occur due to erroneous operations.
- Especially, in the case of a control from an external device to a remote programmable controller, immediate action cannot be taken for a problem on the programmable controller due to a communication failure. Determine the handling method as a system when communication failure occurs along with configuration of interlock circuit on a program, by considering the external equipment and CPU module.
- Do not write any data to the "system area" and "write-protect area" of the buffer memory in the intelligent function module. Executing data writing to the "system area" or "write-protect area" may cause malfunction of the programmable controller alarm. For the "system area" or "write-protect area", refer to ☞ Page 91 Buffer Memory.
- If a communication cable is disconnected, the network may be unstable, resulting in a communication failure of multiple stations. Construct an interlock circuit in the program so that the system always operates on the safe side even if communications fail. Incorrect output or malfunction may result in an accident.

[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.
- When an inductive load such as a lamp, heater, or solenoid valve is controlled, a large current (approximately ten times greater than normal) may flow when the output is turned from off to on. Take proper measures so that the flowing current dose not exceed the value corresponding to the maximum load specification of the resistance load.
- Do not power off the CPU module or reset the CPU module while the settings are being written. Doing so will make the data in the flash ROM undefined. The values need to be set in the buffer memory and written to the flash ROM again. Doing so also may cause malfunction or failure of the module.

[SECURITY PRECAUTIONS]

⚠WARNING

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

[INSTALLATION PRECAUTIONS]

⚠WARNING

- Make sure to cut off all phases of the power supply externally before attempting installation or wiring work. Failure to do so may cause electric shock or damage to the product.
- Use the product within the generic environment specifications described in the User's Manual (Hardware) of the CPU module used.
  Never use the product in areas with excessive dust, oily smoke, conductive dusts, corrosive gas (salt air, Cl_2, H_2S, SO_2 or NO_2), flammable gas, vibration or impacts, or expose it to high temperature, condensation, or rain and wind.
  If the product is used in such conditions, electric shock, fire, malfunctions, deterioration or damage may occur.

[INSTALLATION PRECAUTIONS]

⚠CAUTION

- Do not touch the conductive parts of the product directly. Doing so may cause device failures or malfunctions.
- When drilling screw holes or wiring, make sure that cutting and wiring debris do not enter the ventilation slits of the PLC. Failure to do so may cause fire, equipment failures or malfunctions.
- For the product supplied together with a dust proof sheet, the sheet should be affixed to the ventilation slits before the installation and wiring work to prevent foreign objects such as cutting and wiring debris.
  However, when the installation work is completed, make sure to remove the sheet to provide adequate ventilation. Failure to do so may cause fire, equipment failures, or malfunctions.
- Install the product on a flat surface. If the mounting surface is rough, undue force will be applied to the PC board, thereby causing nonconformities.
- Install the product securely using a DIN rail or mounting screws.
- Work carefully when using a screwdriver such as installation of the product. Failure to do so may cause damage to the product or accidents.
- Connect the extension cables, peripheral device cables, input/output cables and battery connecting cable securely to their designated connectors. Loose connections may cause malfunctions.
- Turn off the power to the PLC before attaching or detaching the following devices. Failure to do so may cause equipment failures or malfunctions.
  - Peripheral devices, expansion board, expansion adapter, and connector conversion adapter
  - Extension modules, bus conversion module, and connector conversion module
  - Battery

[WIRING PRECAUTIONS]

⚠WARNING

- Make sure to cut off all phases of the power supply externally before attempting installation or wiring work. Failure to do so may cause electric shock or damage to the product.
- Make sure to attach the terminal cover, provided as an accessory, before turning on the power or initiating operation after installation or wiring work. Failure to do so may cause electric shock.
- The temperature rating of the cable should be 80℃ or more.
- Make sure to properly wire to the spring clamp terminal block in accordance with the following precautions. Failure to do so may cause electric shock, equipment failures, a shortcircuit, wire breakage, malfunctions, or damage to the product.
  - The disposal size of the cable end should follow the dimensions described in the manual.
  - Twist the ends of stranded wires and make sure that there are no loose wires.
  - Do not solder-plate the electric wire ends.
  - Do not connect more than the specified number of wires or electric wires of unspecified size.
  - Affix the electric wires so that neither the terminal block nor the connected parts are directly stressed.

[WIRING PRECAUTIONS]

⚠CAUTION

- Perform class D grounding (grounding resistance: 100Ω or less) of the grounding terminal on the CPU module and extension modules with a wire 2 ㎟ or thicker. Do not use common grounding with heavy electrical systems (refer to the User's Manual (Hardware) of the CPU module used).
- Individually ground the FG terminal of the programmable controller with a ground resistance of 100Ω or less. Failure to do so may result in electric shock or malfunction.
- Install module so that excessive force will not be applied to terminal blocks, or communication cables. Failure to do so may result in wire damage/breakage or PLC failure.
- Make sure to observe the following precautions in order to prevent any damage to the machinery or accidents due to malfunction of the PLC caused by abnormal data written to the PLC due to the effects of noise.
  - Do not bundle the control line and communication cables together with or lay them close to the main circuit, high-voltage line, load line or power line. As a guideline, lay the power line, control line and communication cables at least 100 mm away from the main circuit, high-voltage line, load line or power line.
  - Ground the shield of the shielded wire or shielded cable at one point on the PLC. However, do not use common grounding with heavy electrical systems.
- For Ethernet cables to be used in the system, select the ones that meet the specifications described in ☞ Page 47 Wiring Products. If not, normal data transmission is not guaranteed.

[STARTUP AND MAINTENANCE PRECAUTIONS]

⚠WARNING

- Do not touch any terminal while the PLC's power is on. Doing so may cause electric shock or malfunctions.
- Before cleaning or retightening terminals, cut off all phases of the power supply externally. Failure to do so in the power ON status may cause electric shock.
- Before modifying the program in operation, forcible output, running or stopping the PLC, read through this manual carefully, and ensure complete safety. An operation error may damage the machinery or cause accidents.
- Do not change the program in the PLC from two or more peripheral equipment devices at the same time. (i.e. from an engineering tool and a GOT) Doing so may cause destruction or malfunction of the PLC program.

[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 PLC. Doing so may cause fire, equipment failures, or malfunctions. For repair, contact your local Mitsubishi Electric representative.
- Turn off the power to the PLC before attaching or detaching the following devices. Failure to do so may cause equipment failures or malfunctions.
  - Peripheral devices, expansion board, expansion adapter, and connector conversion adapter
  - Extension modules, bus conversion module, and connector conversion module
  - Battery
- Read relevant manuals carefully and ensure the safety before performing online operations (operation status change) with peripheral devices connected to the CPU modules of other stations. Improper operation may damage machines or cause accidents.

[OPERATION PRECAUTIONS]

⚠CAUTION

- Construct an interlock circuit in the program so that the whole system always operates on the safe side before executing the control (for data change) of the PLC in operation.
  Read the manual thoroughly and ensure complete safety before executing other controls (for program change, parameter change, forcible output and operation status change) of the PLC in operation.
  Otherwise, the machine may be damaged and accidents may occur by erroneous operations.
- Do not power off the CPU module or reset the CPU module while the setting values in the buffer memory are being written to the flash ROM in the intelligent function module. Doing so will make the data in the flash ROM card undefined. The values need to be set in the buffer memory and written to the flash ROM again. Doing so can cause malfunction or failure of the module.
- Note that the whole system may not be reset by the RUN/STOP/RESET switch when the CPU module or intelligent function module detects an error, such as a watchdog timer error, during self-diagnosis. In such cases, turn the power off and on again.

[DISPOSAL PRECAUTIONS]

⚠CAUTION

- Please contact a certified electronic waste disposal company for the environmentally safe recycling and disposal of your device.

[TRANSPORTATION PRECAUTIONS]

⚠CAUTION

- The PLC is a precision instrument. During transportation, avoid impacts larger than those specified in the general specifications of the User's Manual (Hardware) of the CPU module by using dedicated packaging boxes and shock-absorbing palettes. Failure to do so may cause failures in the PLC. After transportation, verify operation of the PLC and check for damage of the mounting part, etc.

INTRODUCTION

Thank you for purchasing MELSEC iQ-F series programmable controllers.
This manual contains text, diagrams and explanations which will guide the reader in the correct installation, safe use and operation of the FX5-OPC OPC UA module of iQ-F series.
It should be read and understood before attempting to install or use the module.
Always forward it to the end user.

Regarding use of this product

- This product has been manufactured as a general-purpose part for general industries, and has not been designed or manufactured to be incorporated in a device or system used in purposes related to human life.
- Before using the product for special purposes such as nuclear power, electric power, aerospace, medical, or passenger movement vehicles, please contact Mitsubishi Electric sales office.
- This product has been manufactured under strict quality control. However, when installing the product where major accidents or losses could occur if the product fails, install appropriate backup or failsafe functions in the system.

Note

- If in doubt at any stage during the installation of the product, always consult a professional electrical engineer who is qualified and trained in the local and national standards. If in doubt about the operation or use, please contact your local Mitsubishi Electric representative.
- Since the examples indicated by this manual, technical bulletin, catalog, etc. are used as a reference, please use the product after confirming the function and safety of the equipment and system.
- This manual content, specification etc. may be changed, without a notice, for improvement.
- The information in this manual has been carefully checked and is believed to be accurate; however, if you notice a doubtful point, an error, etc., please contact your local Mitsubishi Electric representative. When doing so, please provide the manual number given at the end of this manual.

CONTENTS

RELEVANT MANUALS

Manual name <manual number>	Description
MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware) <SH-082452ENG>	Describes the details of hardware of the CPU module, including performance specifications, wiring, installation, and maintenance.
MELSEC iQ-F FX5 User's Manual (Application) <JY997D55401>	Basic knowledge required for program design, functions of a CPU module, devices/labels, and parameters
MELSEC iQ-F FX5 Programming Manual (Program Design) <JY997D55701>	Specifications of ladder, ST, FBD/LD, and other programs and labels
MELSEC iQ-F FX5 Programming Manual (Instructions, Standard Functions/Function Blocks) <JY997D55801>	Specifications of instructions and functions that can be used in programs
MELSEC iQ-F FX5 OPC UA Module User's Manual <SH-082250ENG>(this manual)	Functions of an OPC UA module
GX Works3 Operating Manual <SH-081215ENG>	System configuration, parameter settings, and online operations of GX Works3

TERMS

Unless otherwise specified, this manual uses the following terms.

Term	Description
Address space	Data that contains information of a target device, a group, and a tag.
Anonymous	A user who do not use both an account name and a password.
Certificate authority	An agency that registers, issues, and revokes electronic certificates.
Certificate revocation list	A certificate revocation list managed by a certificate authority.
Client certificate	The certificate of an OPC UA client used for OPC UA communication. A generic term for user certificates and application certificates.
Endpoint	A server or client connected at the end of network. It physically refers to the personal computer or OPC UA module at the end.
Engineering tool	A generic product name of software packages for the MELSEC programmable controllers.
OPC UA Module Configuration Tool	A product name for OPCUAMCT.
Server certificate	The certificate of an OPC UA server used for application authentication in OPC UA communication.

GENERIC TERMS AND ABBREVIATIONS

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

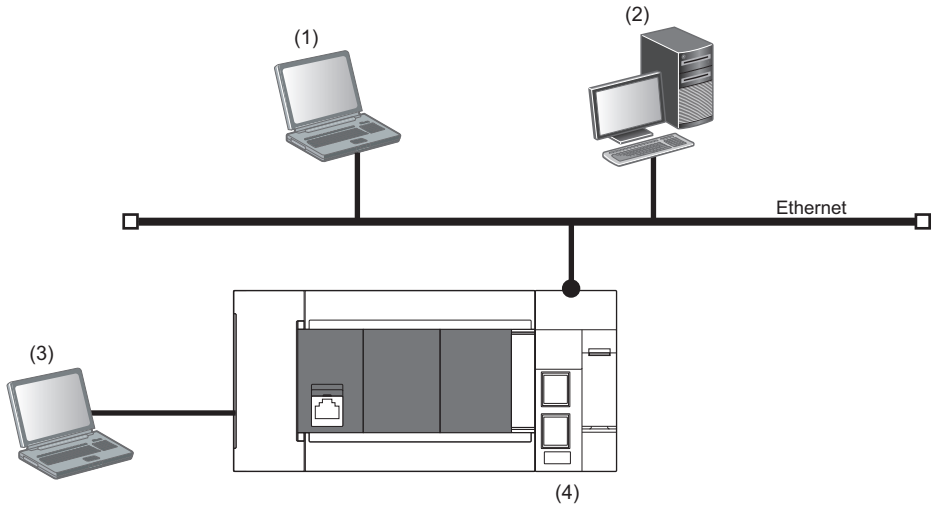
Generic term/abbreviation	Description
FX5 CPU module	A generic term for FX5UJ CPU module, FX5U CPU module, and FX5UC CPU module.
FX5-OPC	An abbreviation for FX5-OPC OPC UA module.
GX Works3	A generic product name for SWnDND-GXW3. ('n' indicates its version.)
OPC	An abbreviation for OLE for Process Control, which is 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.
SCADA	An abbreviation for Supervisory Control And Data Acquisition. An industrial control system for system monitoring and process control by using a computer.
Intelligent function module	A generic term for FX5-4AD, FX5-4DA, FX5-8AD, FX5-4LC, FX5-20PG-P, FX5-20PG-D, FX5-40SSC-S, FX5-80SSC-S, FX5-ENET, FX5-ENET/IP, FX5-CCLIEF, FX5-CCL-MS, FX5-ASL-M, FX5-DP-M, FX5-OPC, FX3U-4AD, FX3U-4DA, FX3U-4LC, FX3U-1PG, FX3U-2HC, FX3U-16CCL-M, FX3U-64CCL, FX3U-128ASL-M, FX3U-32DP.
Intelligent module	An abbreviation for intelligent function modules.

1 OVERVIEW

FX5-OPC OPC UA module (hereinafter referred to as FX5-OPC) is an intelligent function module for making programmable controller data such as inputs, outputs, or internal registers available to external devices and applications via an OPC UA server interface.

OPC UA communication

OPC UA is an architecture to exchange information between applications and devices.
In the form which an FX5-OPC supports, information is exchanged between an OPC UA client (external application or device) and an OPC UA server (FX5-OPC).
Information to be exchanged is modeled as a set of objects and references. The dedicated protocol built on a TCP/IP network layer is used for information transmission.
OPC UA communication is suitable in all kinds of networks including the Internet by a strong end-to-end security.



(1) OPC UA client
(2) SCADA
(3) GX Works3 or OPC UA Module Configuration Tool
(4) FX5-OPC (OPC UA server)

Features

The following shows main features of an FX5-OPC.

- Data access to an FX5 programmable controller via an OPC UA server interface
- Physical connection to an OPC UA client via Ethernet
- Secure communication in accordance with the OPC UA standards
- OPC UA address space generation from labels of a GX Works3 project

MEMO

2 SPECIFICATIONS

This chapter explains the specifications of an FX5-OPC.

2.1 General Specifications

The general specifications other than below are the same as those of the CPU module to be connected.
For the general specification, refer to the following:
MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware)

Item	Specification	
Dielectric withstand voltage	500 VAC for one minute	Between all terminals and ground terminal
Insulation resistance	10 MΩ or higher by 500 VDC insulation resistance tester	

2.2 Power Supply Specifications

The following shows the power supply specifications.

Item	Specification	
Internal power supply	Power supply voltage	24 VDC
	Current consumption	110 mA

2.3 Performance Specifications

The following shows the performance specifications.

Item				Specification
OPC UA server	OPC UA version			1.03
	Profiles			Micro Embedded Device Server Profile For details on supported profiles and facets, refer to the following: ☞ Page 16 Supported profiles and facets
	Services			☞ Page 17 Supported services
	Address space			☞ Page 19 Address space specifications
	User authentication			User name and password
	Maximum number of parallel sessions			4
	Maximum number of subscriptions per session			2
	Maximum number of monitored items per subscription			500
	Minimum sampling interval of a monitored item			100 ms
	Maximum number of trusted certificates			10
	Time information			☞ Page 18 Server time
	Network topology			Star topology
Ethernet	Transmission specifications	Data transmission speed		100/10Mbps
		Communication mode		Full-duplex or half-duplex*1
		Transmission method		Base band
		Interface		RJ45 connector
		Maximum segment length		100m *2
		Number of cascade connections	100BASE-TX	2 levels maximum*3
			10BASE-T	4 levels maximum*3
	Hub*1			Hubs with 100BASE-TX or 10BASE-T ports*4 can be used.
	Connection cable*5			100BASE-TX, 10BASE-T
	Number of ports			2
Number of occupied I/O points				8 points
Number of connectable modules				1 module

*1 IEEE802.3x flow control is not supported.
*2 For maximum segment length (length between hubs), consult the manufacturer of the hub used.
*3 This number applies when a repeater hub is used. When using a switching hub, check the number of cascaded stages with the manufacturer of the hub to be used.
*4 The ports must comply with the IEEE802.3 100BASE-TX or IEEE802.3 10BASE-T standards.
*5 A straight/cross cable can be used.

OPC UA server specifications

An FX5-OPC is compliant with OPC UA Version 1.03.

Supported profiles and facets

The following shows the profiles and facets supported by an FX5-OPC.

Profile/facet name	Description
ComplexType Server Facet	Values of all structure members can be read or written at once by a single operation. They can also be accessed one by one. For details, refer to the following: ☞ Page 20 User-defined structure
Micro Embedded Device Server Profile Nano Embedded Device Server Profile	These profiles define the transport layer to be UA-TCP UA-SC UA-Binary. In addition, they contain requirements for a minimum number of supported parallel sessions. For the number of parallel sessions supported by an FX5-OPC, refer to the following: ☞ Page 15 Performance Specifications
Core Server Facet	All mandatory features contained in this facet are supported. For details on supported services and address space, refer to the following: ☞ Page 17 Supported services, Page 19 Address space specifications
User Token ― User Name Password Server Facet	Authentication of users based on a user name and password is supported. For details, refer to the following: ☞ Page 34 User authentication
SecurityPolicy ― None	The None security policy is supported. An FX5-OPC exposes the endpoint of None security policy only if unsecured connections are enabled in the security configuration. For the method to enable unsecured connections, refer to the following: ☞ Page 75 Enabling Unsecured Connections
UA-TCP UA-SC UA-Binary	The UA-TCP protocol with a binary encoding is used on the transport layer. Other protocol bindings, HTTPS for example, are not supported.
Embedded DataChange Subscription Server Facet	Services of the Subscription and MonitoredItem service sets are supported. The number of subscriptions per session and that of monitored items per subscription have their respective upper limits. For details, refer to the following: ☞ Page 15 Performance Specifications
SecurityPolicy ― Basic128Rsa15 SecurityPolicy ― Basic256 SecurityPolicy ― Basic256Sha256	For details on security, refer to the following: ☞ Page 27 Security
Device Integration Model (DI)	This model is used as a base for the PLCopen® model. The following facets are supported: • BaseDevice_Server_Facet • BlockDevice_Server_Facet For details, refer to the following: ☞ Page 19 Address space specifications
PLCopen Model	This model is used to map a GX Works3 project to the address space of an OPC UA server. The Controller Operation Server Facet is supported. For details, refer to the following: ☞ Page 19 Address space specifications

Supported services

The following shows the OPC UA services defined in OPC UA Version 1.03 and whether each service is supported by an FX5-OPC.

○: Supported, ×: Not supported

Service set name	Service name	Status
Discovery	FindServers	○
	FindServersOnNetwork	×
	GetEndpoints	○
	RegisterServer	×
	RegisterServer2	×
SecureChannel	OpenSecureChannel	○
	CloseSecureChannel	○
Session	CreateSession	○
	ActivateSession	○
	CloseSession	○
	Cancel	×
NodeManagement	AddNodes	×
	AddReferences	×
	DeleteNodes	×
	DeleteReferences	×
View	Browse	○
	BrowseNext	○
	TranslateBrowsePathsToNodeIds	○
	RegisterNodes	○
	UnregisterNodes	○
Query	QueryFirst	×
	QueryNext	×
Attribute	Read	○
	HistoryRead	×
	Write	○
	HistoryUpdate	×
Method	Call	×
MonitoredItem	CreateMonitoredItems	○
	ModifyMonitoredItems	○
	SetMonitoringMode	○
	SetTriggering	×
	DeleteMonitoredItems	○
Subscription	CreateSubscription	○
	ModifySubscription	○
	SetPublishingMode	○
	Publish	○
	Republish	○
	TransferSubscriptions	×
	DeleteSubscriptions	○

■Server time

An FX5-OPC uses the time setting of a CPU module for its time stamps of all operations.

The CPU module clock can be set automatically with the time setting function (SNTP client).

Alternatively, it can be set manually in GX Works3.

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

📖MELSEC iQ-F FX5 User's Manual (Communication)

📖GX Works3 Operating Manual

Changing the time setting of a CPU module while an OPC UA server is running affects the FX5-OPC operation as follows.

- When the time is changed forward:
  An OPC UA server automatically follows the time newly set; however, connected OPC UA clients may get disconnected due to a session timeout if a set time before and after the change is significantly different.
- When the time is changed backwards by more than 10 ms:
  An OPC UA server automatically restarts and notifies an event (0820H). (☞ Page 86 Event List)
  After the restart, the server operates with an updated time.

Address space specifications

The following shows details on facets that define the structure of the FX5-OPC address space.

Category	Facet name	Supported conformance unit
Data Access	ComplexType Server Facet	All mandatory units
PLCopen	Controller Operation Server Facet	All mandatory units and an optional unit 'Ctrl References'
OPC UA for devices	BaseDevice_Server_Facet	All mandatory units
	BlockDevice_Server_Facet	All mandatory units

Namespace URIs used in the address space are as follows:

Index	Namespace URI	Remarks
0	http://opcfoundation.org/UA/	OPC UA namespace
1	urn:Mitsubishi:FX5-OPC:[GUID]	FX5-OPC specific namespace (Example) urn:Mitsubishi:FX5-OPC:bd608061-f8c9-4e70-a9cc-b995ee7*****
2	http://PLCopen.org/OpcUa/IEC61131-3/	PLCopen OPC UA Information Model namespace
3	http://opcfoundation.org/UA/DI/	OPC UA for Devices namespace

In the namespace with the index 1, node IDs and browse names of all application specific nodes (including user-defined variables, objects, etc.) exist.

■Simple data types

The following shows the simple data types which can be set as labels in GX Works3 and their corresponding OPC UA data types.

Only labels of data types supported also by OPC UA can be published in the FX5-OPC address space.

GX Works3 data type	OPC UA data type	Available device assignment
Bit	Boolean	• Automatic-assign • Non bit-specified: X, Y, M, L, B, F, SB, SM • Bit-specified*1: D, R, W, SW, SD, G
Word [Unsigned]	WORD*2	• Automatic-assign • D, R, W, SW, SD, G, K, H
Double Word [Unsigned]	DWORD*2	
Word [Signed]	Int16	
Double Word [Signed]	Int32	
FLOAT [Single Precision]	Float	• Automatic-assign • D, R, W, SW, SD, G, E
Time	No correspondence	—
String	STRING*2	• Automatic-assign • D, R, W, SW, SD
String [Unicode]	No correspondence	—
Pointer	No correspondence	—
Timer	No correspondence	—
Counter	No correspondence	—
Long Counter	No correspondence	—
Retentive Timer	No correspondence	—

*1 A bit array assigned manually to a word type address is not supported. (Example) bit array starting from D0.7
This applies also to a bit array which is a structure member.

*2 Defined in the PLCopen information model and has a node ID outside the namespace 0. (Example) WORD type: ns = 2, id = 3002

■User-defined structure

Structure definitions in a GX Works3 project are represented in the FX5-OPC address space as DataType nodes.
In addition, detailed information of each structure definition is held as a part of the ByteString value of the standard TypeDictionary variable[*1]. (☞ Page 38 User nodes)

*1 Used by an OPC UA client for encoding or decoding a structure value during a read or write operation.
Only the standard OPC binary encoding is supported.

Members of a structure variable can be exposed in the address space as individual component variables by the following setting in GX Works3.

- "Address Space Parameter" ⇨ "Expose structure members as components"

Differences by this setting are as follows:

Item	Expose structure members as components	
	Disabled	Enabled
Data access	An OPC UA client can access a structure variable only as a single value. To encode or decode the value, the client needs to use TypeDictionary provided by the server.	An OPC UA client can access each member of a structure variable individually. Accessing the structure variable as a single value is also available.
Facet support	An OPC UA client needs to support the ComplexType facet which provides rules to encode or decode a structure value by using TypeDescription in a TypeDictionary variable.	An OPC UA client does not need to support the ComplexType facet. Structure members are of simple data types.
Total size of the address space (which has an upper limit)	Decreased.	Increased.

Precautions

Data inconsistency may occur in a structure variable.
(Example: Members of a structure variable may have data read in different cycles even if the structure variable was read as a single value.)

■Arrays

An FX5-OPC supports arrays of all simple data types which are supported by OPC UA.(☞ Page 19 Simple data types)
The maximum number of array elements is 1024 regardless of the data type.
An array is published as a single value. An OPC UA client can access specific ranges of array elements by specifying the index range when accessing value of an array variable via OPC UA services.
In addition, unlike in GX Works3, arrays in an FX5-OPC are always indexed from zero.
If an array the index of which does not start from zero is exposed, the indexes of its elements will be changed accordingly, so that the array indexing starts from zero.
The following is an example:

Item	GX Works3	FX5-OPC
Array definition	The array start value and end value of each dimension are contained. Example: Array (2..3, 4..5)	The number of elements in each dimension is contained. Example: Array (2, 2)
Element indexes	1: [2][4] 2: [2][5] 3: [3][4] 4: [3][5]	1: [0][0] 2: [0][1] 3: [1][0] 4: [1][1]

Precautions

Two elements of a single array may have data read in different cycles.

■Function blocks

FB definitions from GX Works3 are represented in the FX5-OPC address space as ObjectType nodes containing variables such as inputs, outputs, internal variables and external variables.

FB instances are represented as Object nodes.

For details, refer to the following:

☞ Page 38 User nodes

■Considerations

The number of labels that can be exposed in the FX5-OPC address space depends on the usage of the following resources:

(1) ROM space reserved for storing the address space parameters

(2) RAM space reserved for caching variable values read from a CPU module

(3) RAM space reserved for storing node information in the address space

(4) Size of TypeDictionary describing user-defined data types

The following operations may optimize each space/size of (1) to (4).

No.	Optimizing operation
(1)	• Shorten names of files, program blocks, function blocks, structures, and labels. • Disable the setting of "Expose structure members as components."
(2)	• Avoid using strings and arrays with a large number of elements.
(3)	• Avoid using structures and FB instances with a large number of members. • Disable the setting of "Expose structure members as components."
(4)	• Shorten names of structure members.

Considerations for OPC UA clients

The following shows the considerations when using OPC UA clients.

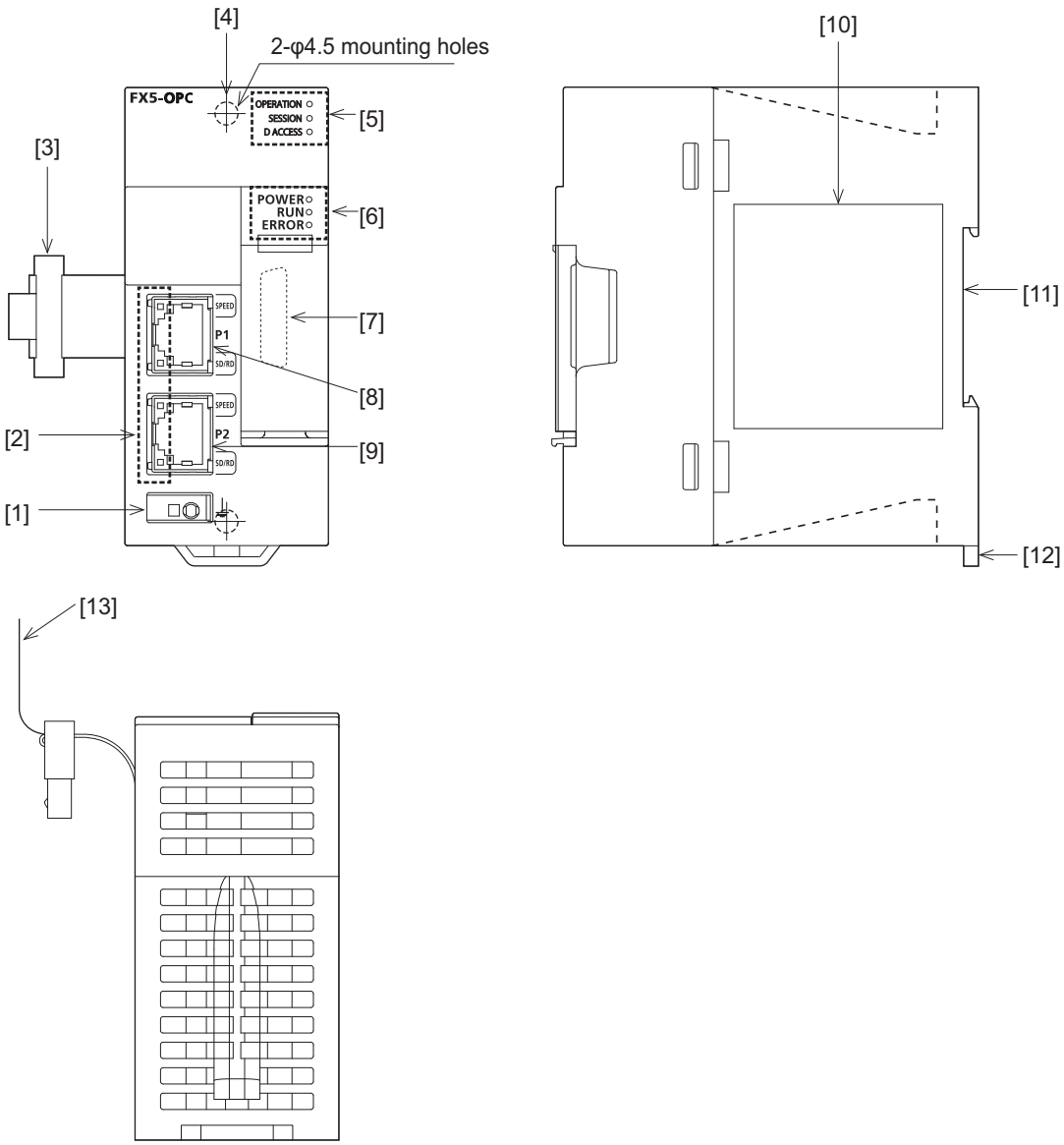
Considerations when using GT SoftGOT2000

When using GT SoftGOT2000 as an OPC UA client, note the following:

- Structures cannot be used.
- If the security mode is SignAndEncrypt and the user token type is with a user name/password, GT SoftGOT2000 cannot be connected.

2.4 Part Names

This section shows the part names of an FX5-OPC.



No.	Name	Description
[1]	External ground terminal	Connect an external ground. (Spring clamp terminal block)
[2]	Ethernet connection status display LEDs	Indicates the status of the Ethernet connection. (☞ Page 23 LED indication)
[3]	Extension cable	A cable for connecting a preceding module.
[4]	Direct mounting hole	Screw holes (2-ϕ4.5, mounting screw: M4 screw) for direct installation.
[5]	OPC UA server operation status display LED	Indicates the operating status of the OPC UA server function. (☞ Page 23 LED indication)
[6]	Module operation status display LED	Indicates the operating status of an FX5-OPC. (☞ Page 23 LED indication)
[7]	Extension connector	A connector for connecting the extension cable of an extension module.
[8]	Modular jack for P1 (RJ-45) (with cap)	Ports for connecting an FX5-OPC to the network.
[9]	Modular jack for P2 (RJ-45) (with cap)	
[10]	Name plate	The product model name, manufacturer's serial number etc. are shown.
[11]	DIN rail mounting groove	The module can be installed on DIN46277 rail (35 mm wide).
[12]	DIN rail mounting hook	A hook for mounting the module on a DIN rail of DIN46277 (35 mm wide).
[13]	Pull out tab	A tab for drawing out an extension cable.

LED indication

The following shows the indications of the LEDs.

LED name		LED color	Description
OPERATION		Green	Indicates the operating status of an OPC UA server. ON: Server running OFF: Server stopped
SESSION		Green	Indicates the session status between an FX5-OPC and OPC UA client. ON: Active session OFF: No active session
D ACCESS		Green	Indicates whether programmable controller data is being read/written by an OPC UA client or not. ON: Data being read or written by a client OFF: No data being read or written by a client
POWER		Green	Indicates the power supply status. ON: Powered ON OFF: Powered OFF or hardware error
RUN		Green	Indicates the operating status of an FX5-OPC. ON: Initialization or hardware test completed Flashing: Hardware test in process OFF: Initialization not yet completed or a major error
ERROR		Red	Indicates the error status of an FX5-OPC. ON: Minor error Flushing: Moderate error or major error OFF: Normal operation
P1, P2	SPEED	Green	Indicates the transmission speed of each port. ON: Linking-up (100 Mbps) OFF: Linking-up (10 Mbps)
	SD/RD	Green	Indicates the data sending/receiving status of each port. Flashing: Data being sent/received OFF: No data being sent/received

3 PROCEDURES BEFORE OPERATION

This chapter describes the procedures before operation of an FX5-OPC.

Operating procedure

1. Checking the specifications of an FX5-OPC

Check the specifications of an FX5-OPC. (☞ Page 14 SPECIFICATIONS)

2. Attaching an FX5-OPC

Connect an FX5-OPC to a CPU module.

For details, refer to the following:

📖MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware)

3. Wiring an FX5-OPC

Connect the ground and connect an Ethernet cable. (☞ Page 43 WIRING)

4. Configuring an FX5-OPC

Set parameters and select labels to be exposed in the FX5-OPC address space. (☞ Page 48 PARAMETER SETTINGS)

5. Checking the status of an FX5-OPC

Check the operation statuses of an FX5-OPC and its OPC UA server function. (☞ Page 76 TROUBLESHOOTING)

Precautions

An FX5-OPC uses the time setting of a CPU module.

Before starting to use an FX5-OPC, check that the clock of a CPU module (including "Time Zone" in the CPU parameters) is set to the current time.

If the clock is not set to the current time, a server certificate generated in an FX5-OPC may get an invalid date, and thus OPC UA clients would reject the connections with the FX5-OPC.

Operation check of an OPC UA client

The following shows the procedure to check whether an OPC UA client can access an FX5-OPC.

Operating procedure

1. Search an FX5-OPC from an OPC UA client, and connect the module.

2. Check whether a value of any label exposed in an address space can be read and written.

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

Precautions

Depending on the address space size and polling performance, an error may occur due to the overload of an OPC UA server. (☞ Page 97 Performance Considerations)

After connecting an OPC UA client to an FX5-OPC, keep them communicating with each other for a while and check that no error occurs.

If an error occurs, refer to the following for details:

☞ Page 83 Error Code List

MEMO

4 FUNCTIONS

This chapter explains details on the functions of an FX5-OPC.

4.1 List of Functions

The following table shows the function list of an FX5-OPC.

Function name	Description	Reference
OPC UA server function	To operate as an OPC UA server	Page 26 OPC UA Server Function
Firmware update	To update the firmware version of an FX5-OPC	MELSEC iQ-F FX5 User's Manual (Application)
Factory reset	To restore an FX5-OPC to its initial state	Page 40 Factory Reset
IP filter	To identify the IP address of an access source and prevent access by unauthorized IP addresses	Page 40 IP Filter
Hardware test	To self-diagnose the hardware of an FX5-OPC	Page 81 Hardware Test

4.2 OPC UA Server Function

An FX5-OPC operates as an OPC UA server.

Precautions

If an FX5-OPC cannot communicate with OPC UA clients, check the following:

- Are there any problems with the network connection?
- Are the module parameter settings correct?

If the communication with a programmable controller is disconnected during communication with OPC UA clients, do not send safety-related data because there will be no data communication.

Server start/stop

An FX5-OPC automatically starts the OPC UA server function at its startup.

This function can be stopped or restarted with OPC UA Module Configuration Tool at any timing. (☞ Page 74 Module diagnostics)

When requesting to stop this function, an FX5-OPC first closes TCP sessions of all OPC UA clients before going to the 'stopped' state.

The TCP socket assigned to the OPC UA server port is closed while the server is stopped; therefore, new connections will be all rejected.

Point

The operating status of the OPC UA server function can be checked by any of the following methods:

- Check the OPERATION LED. (☞ Page 23 LED indication)
- Check 'server status' (Un\G0) in the buffer memory. (☞ Page 92 Server status (Un\G0))
- Check "Status" in the [Module Diagnostics] tab of OPC UA Module Configuration Tool. (☞ Page 74 Module diagnostics)

Security

The following explains the security functions of an FX5-OPC.
An FX5-OPC supports the full security stack of the OPC UA specifications for transport and application layers.

Security configuration

Security for an FX5-OPC can be configured in GX Works3 and OPC UA Module Configuration Tool.
In module parameters of GX Works3, settings related to IP filter or unsecured connections can be configured. (☞ Page 58 Security settings)
In security parameters of OPC UA Module Configuration Tool, various settings can be edited offline as a part of an OPC UA Module Configuration Tool project. (☞ Page 66 Security parameters)
Moreover, an administrator password can be set to protect the security parameters stored in the project from unauthorized access.
The security parameters can be written to an FX5-OPC with the online function of OPC UA Module Configuration Tool.

Point

Whether security parameters are stored in an FX5-OPC can be checked with 'security status' (Un\G3) in the buffer memory.
For details, refer to the following:
☞ Page 93 Security status (Un\G3)

Precautions

If any of the following conditions is satisfied, an FX5-OPC operates without security:

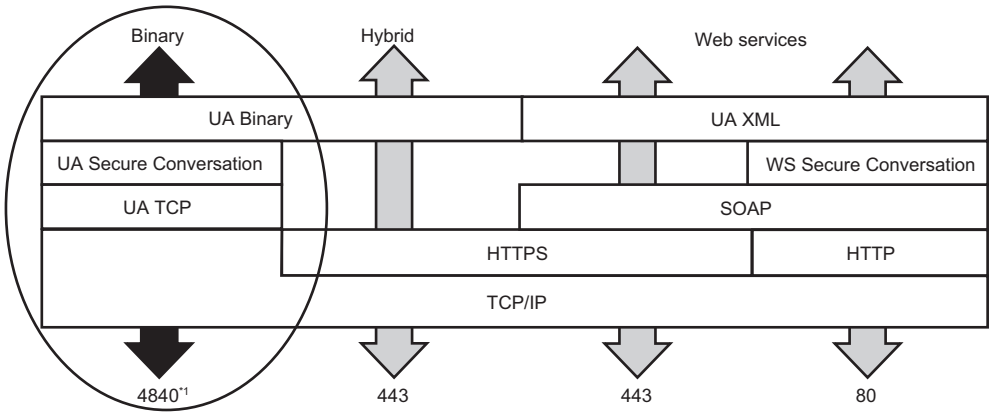
- Security parameters have never been written to an FX5-OPC.
- Security parameters in an FX5-OPC are deleted.

Restriction

Security parameters written in an FX5-OPC cannot be read.

Transport layer

The UA-TCP UA-SC UA-Binary protocol stack which includes UA Secure Conversation is used as the security on the transport layer between an OPC UA client and OPC UA server.



*1 The port number used for communications by an FX5-OPC.

● Security policies

The strength level of OPC UA security is described by security policies.

A combination of a security policy and a message security mode defines a security capability of an endpoint of an OPC UA server.

The following combinations are supported by an FX5-OPC:

Security policy	Message security mode
None	None
Basic128Rsa15	Sign
	SignAndEncrypt
Basic256	Sign
	SignAndEncrypt
Basic256Sha256	Sign
	SignAndEncrypt

For security enhancement, the combination of 'None, None' in the above table is disabled by default.

For the methods to enable this combination, refer to the following:

☞ Page 75 Enabling Unsecured Connections

However, as a security measure, do not use this combination in the network to which another device can connect.

All the security policies other than None are enabled by default. However, they can be disabled individually in "Available Security Policies" in the [Security Parameter] tab of OPC UA Module Configuration Tool.

☞ Page 67 General settings

Point

Whether unsecured connections are enabled can be checked with 'security status' (Un\G3) in the buffer memory.

For details, refer to the following:

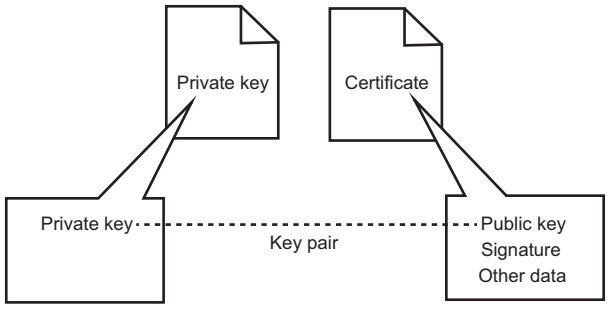
☞ Page 93 Security status (Un\G3)

● Certificates

Certificates with the embedded public keys and their corresponding private keys play a double role in the context of OPC UA security.

First, they are necessary for realizing an asymmetric encryption and message signing, which is used for establishing a secure connection between an OPC UA client and OPC UA server.

Second, they are also used within the PKI (Public Key Infrastructure) for mutual authentication of the client and server.



■Server certificate

For increased security, an FX5-OPC server certificate is not a part of security configuration which can be edited offline and stored in a project file of OPC UA Module Configuration Tool.

A server certificate and its private key exist in an FX5-OPC only.

When OPC UA Module Configuration Tool is connected to an FX5-OPC, the tool displays detailed information of the server certificate read from the FX5-OPC.

A server certificate can be regenerated or deleted with OPC UA Module Configuration Tool. (☞ Page 71 Server certificate)

A server certificate has a fixed validity period.

An FX5-OPC notifies an event (0902H) if 80% of the validity period of a server certificate has passed while the OPC UA server is running. (☞ Page 86 Event List)

Precautions

- A server certificate generated by an FX5-OPC is of the self-signed type.
- The SubjectAltName of a server certificate generated by an FX5-OPC contains the IP address used when generating the certificate.
  If the IP address setting is changed, regenerate the server certificate; otherwise, OPC UA clients may reject to communicate.
- A server certificate may expire while an OPC UA server is running.
  If the certificate expires, OPC UA clients may reject to communicate with the server.

■Server certificate signing request and certificate replacement

A CSR (Certificate Signing Request) generated with a self-signed certificate of an FX5-OPC can be imported in OPC UA Module Configuration Tool and saved as a file.

The saved CSR can be sent to a certificate authority.

The certificate authority then issues a CA-signed certificate for the FX5-OPC based on the CSR.

An existing self-signed certificate can be replaced with the CA-signed certificate by sending it to the FX5-OPC using OPC UA Module Configuration Tool. (☞ Page 71 Server certificate)

Precautions

When creating a server certificate, with an intention to send the corresponding CSR to a certificate authority, it is recommended to use only alphanumeric characters and space in all items.*1 (☞ Page 72 "Generate a New Self-Signed Certificate" screen)

*1 A hyphen (-) and a dot (.) are also available in "Common Name."

■Client certificate

An FX5-OPC uses the following lists of client certificates to authenticate OPC UA client connections.

List	Description
Trusted certificates	A list of self-signed certificates of trusted OPC UA clients and root certificate authorities. This list is managed in security parameters.
Rejected certificates	A list of certificates of rejected OPC UA clients. When a client that is regarded as untrusted based on the current security configuration tries to connect, its client certificate is added to this list. For details on handling of the rejected certificates, refer to the following: ☞ Page 31 Rejected certificate
Issuers certificates	A list of certificates of intermediate certificate authorities, which are signed by a higher level authority. This list is managed in security parameters.
CRLs (Certificate Revocation Lists)	A list of CRLs issued by certificate authorities. This list is managed in security parameters.

Each client certificate list can be checked in the "Client Certificates" field in the [Security Parameter] tab of OPC UA Module Configuration Tool. (☞ Page 68 Client certificates)

Specifications of client certificates are as follows:

Item	Specification
Maximum size of one certificate	2 KB
Maximum size of one CRL	64 KB

Item	Specification
Maximum number of trusted certificates	10
Maximum number of issuers certificates	10
Maximum number of CRLs	20
Maximum number of rejected certificates	10

■Rejected certificate

A rejected certificate is stored in an FX5-OPC.

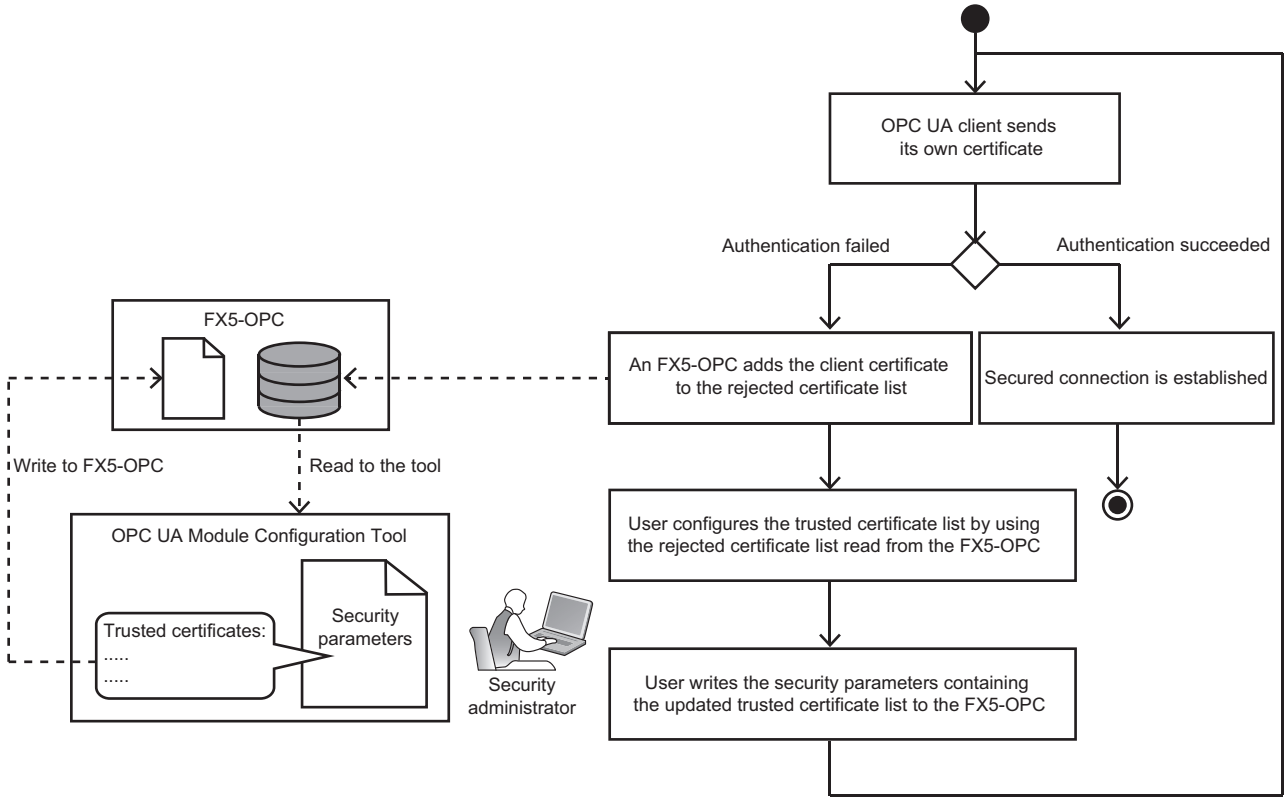
It can be read and displayed in OPC UA Module Configuration Tool.

Any certificate displayed in the list can be moved to the trusted certificate list.

If the authentication of a connecting OPC UA client fails, its client certificate is added to the rejected certificate list.

The following are examples in which connection authentication fails:

- A connecting OPC UA client presented a self-signed certificate; however, the matching certificate is not in the current trusted certificate list.
- A connecting OPC UA client presented a CA-signed certificate; however, the certificate of the certificate authority is not in the current trusted certificate list.



The rejected certificate list is always empty when starting an FX5-OPC.

Every time a new untrusted client tries to connect, its certificate is added to the rejected certificate list.*1

The certificates stored in the rejected certificate list can be cleared at any timing. (☞ Page 68 Rejected certificates)

*1 It is not added if the same certificate already exists.

Point

The number of certificates stored in the rejected certificate list can be checked with 'rejected certificates count' (Un\G4) in the buffer memory.

For details, refer to the following:

☞ Page 93 Rejected certificates count (Un\G4)

■Operations when using self-signed certificates

A certificate can be either self-signed or signed by an external certificate authority.

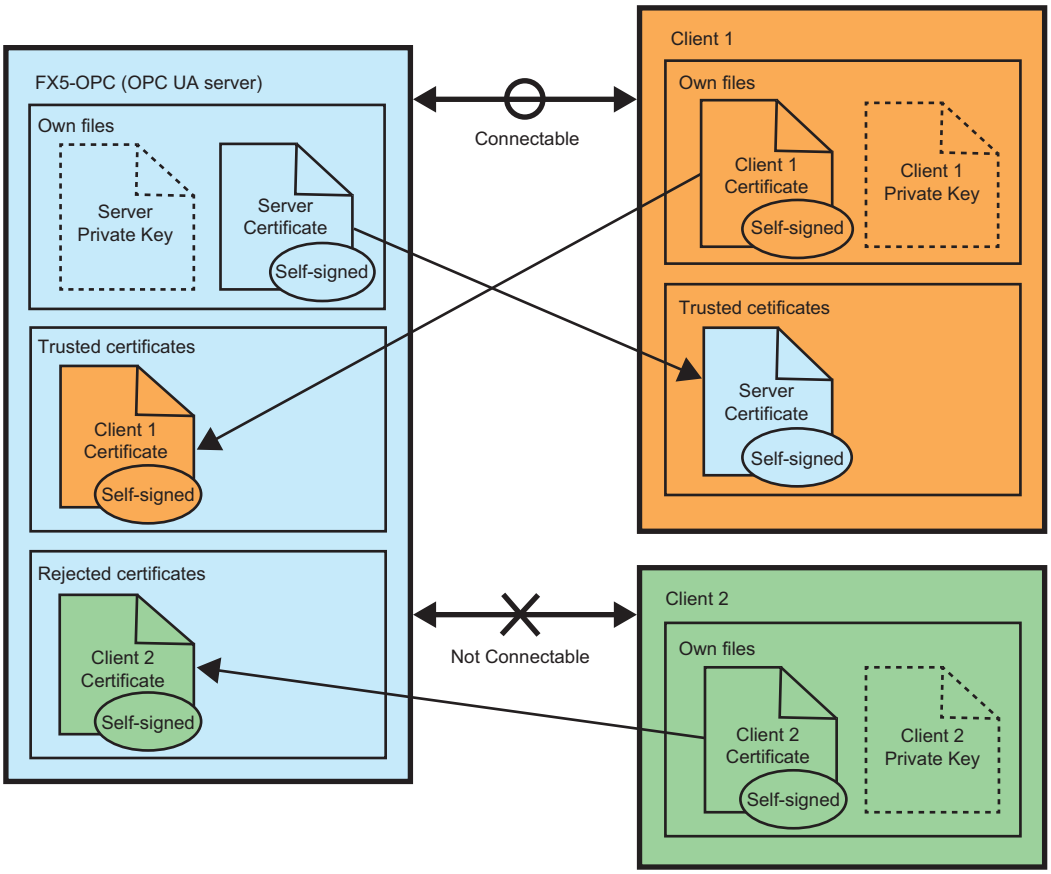
When all OPC UA clients and OPC UA server have self-signed certificates, the server needs to store a client certificate in the trusted certificate list to establish a secure connection with the client.

When an OPC UA client connects to a server, the client sends its own certificate in a connection request.

Then, the server checks whether the client certificate exists in the trusted certificate list.

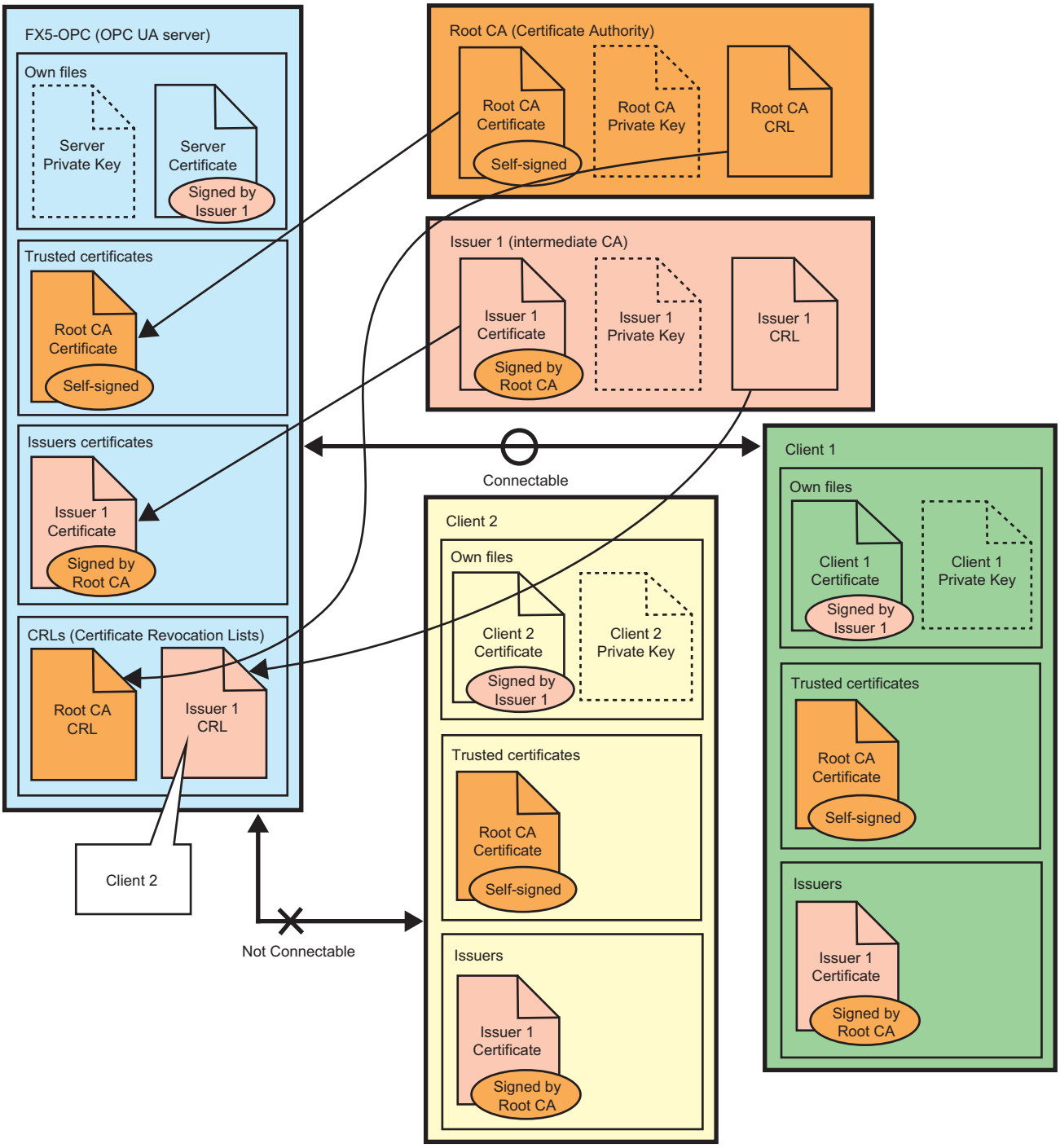
If the certificate exists in the trusted certificate list, a secure connection can be established; otherwise, the certificate is stored in the rejected certificate list.

Operations of the OPC UA client are the same. The OPC UA client needs to store the server certificate in its own trusted certificate list to communicate with the server.



■Operations when using CA-signed certificates

Having a root certificate authority, which can sign other certificates, is an alternative to using self-signed certificates.
Instead of storing all client certificates in the trusted certificate list of an OPC UA server, it is enough to store just one certificate of a trusted root certificate authority.
Such an option is especially useful in larger networks, where administrating trusted certificate lists in many nodes would become infeasible.
Certificates of intermediate certificate authorities stored in the issuers certificate list can be used to build a 'chain of trust' in a multiple layer certificate infrastructure.
The CRL (Certificate Revocation List) list is used by certificate authorities to notify the existence of an OPC UA client that became untrusted.



Application layer

■User authentication

Access to an FX5-OPC is controlled by setting a user name and password to prevent access by unauthorized users.
A user name and password can be set in "User Management" in the [Security Parameter] tab of OPC UA Module Configuration Tool. (☞ Page 70 User management)
Specifications for the user account settings are as follows:

Item	Specification
Maximum number of users	10
User name	6 to 31 characters*1
Password	

*1 All Unicode characters are available.

Point

Whether an account is set for user authentication can be checked with 'security status' (Un\G3) in the buffer memory.
For details, refer to the following:
☞ Page 93 Security status (Un\G3)

Endpoint

An FX5-OPC has a URL which can be combined with a set of security profiles according to the security configuration.
The URL is in the format "opc.tcp://(IP address of an FX5-OPC):4840/Mitsubishi/FX5-OPC."
(4840 is the port number used for communications by an FX5-OPC.)
Exposed endpoints differ as follows depending on the security configuration:

- When security parameters of OPC UA Module Configuration Tool are not stored in an FX5-OPC

Module parameters of GX Works3	Security profiles of the exposed endpoints					Buffer memory (Un\G3)
	Endpoint No.	Security policy	Message security mode	User token type	User token policy	
Module parameters are not stored in a CPU.	No endpoints exposed.					0000H
"Unsecure Connection" is disabled.						
"Unsecure Connection" is enabled.	0	None	None	Anonymous	None	0002H

• When security parameters of OPC UA Module Configuration Tool are stored in an FX5-OPC

Security parameters of OPC UA Module Configuration Tool			Security profiles of the exposed endpoints*1					Buffer memory (Un\G3)
User Management	Enable Unsecure Connection	Sign	Endpoint No.	Security policy	Message security mode	User token type	User token policy	
No account set	Disabled	Enabled	0	Basic128Rsa15	Sign	Anonymous	None	0009H
			1		SignAndEncrypt			
			2	Basic256	Sign			
			3		SignAndEncrypt			
			4	Basic256Sha256	Sign			
			5		SignAndEncrypt			
		Disabled	0	Basic128Rsa15	SignAndEncrypt	Anonymous	None	0001H
			1	Basic256				
			2	Basic256Sha256				
	Enabled	Enabled	0	None	None	Anonymous	None	000BH
			1	Basic128Rsa15	Sign			
			2		SignAndEncrypt			
			3	Basic256	Sign			
			4		SignAndEncrypt			
			5	Basic256Sha256	Sign			
			6		SignAndEncrypt			
		Disabled	0	None	None	Anonymous	None	0003H
			1	Basic128Rsa15	SignAndEncrypt			
			2	Basic256				
			3	Basic256Sha256				
Account(s) set	Disabled	Enabled	0	Basic128Rsa15	Sign	UserName	Basic128Rsa15	000DH
			1		SignAndEncrypt		None	
			2	Basic256	Sign		Basic256	
			3		SignAndEncrypt		None	
			4	Basic256Sha256	Sign		Basic256Sha256	
			5		SignAndEncrypt		None	
		Disabled	0	Basic128Rsa15	SignAndEncrypt	UserName	None	0005H
			1	Basic256				
			2	Basic256Sha256				
	Enabled	Enabled	0	None	None	UserName	Basic128Rsa15	000FH
			1	Basic128Rsa15	Sign			
			2		SignAndEncrypt		None	
			3	Basic256	Sign		Basic256	
			4		SignAndEncrypt		None	
			5	Basic256Sha256	Sign		Basic256Sha256	
			6		SignAndEncrypt		None	
		Disabled	0	None	None	UserName	Basic128Rsa15	0007H
			1	Basic128Rsa15	SignAndEncrypt		None	
			2	Basic256				
			3	Basic256Sha256				

*1 The endpoints shown in this table assumes that all security policies are enabled in "Available Security Policies" in the [Security Parameter] tab of OPC UA Module Configuration Tool.
If any security policy is disabled, the corresponding endpoints are not exposed.

The OPC UA security policy considers the strength of certificates.
Therefore, OPC UA clients may not be able to access some endpoints depending on the settings of the stored server certificate.
An FX5-OPC rejects a client connection if the settings of a server certificate (combination of an asymmetric signature algorithm and asymmetric key length) and the security policy of selected endpoint do not match the table below.

Asymmetric signature algorithm	Asymmetric key length		
	1024 bits	2048 bits	3072 bits 4096 bits
Sha1RSA	None Basic128Rsa15 Basic256	None Basic128Rsa15 Basic256	—
Sha256RSA Sha384RSA Sha512RSA	None Basic128Rsa15 Basic256	None Basic128Rsa15 Basic256 Basic256Sha256	None Basic256Sha256

By generating a certificate with the following settings, a high security level is provided and the availability of all security policies is ensured:

- RSA Key Strength: 2048 bits
- Signature Algorithm: SHA-256

For details on the settings, refer to the following:

☞ Page 72 "Generate a New Self-Signed Certificate" screen

Address space

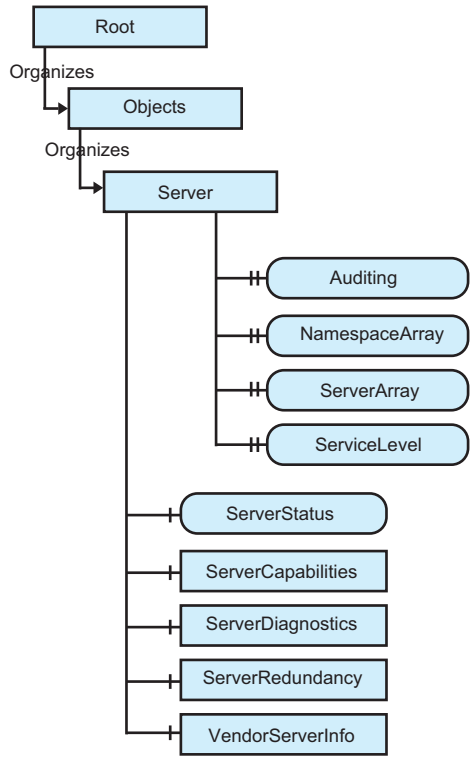
An FX5-OPC supports Core Server Facet of the OPC UA specifications.

Overview

FX5-OPC address space contains variables and objects mapped to data in GX Works3 project (such as labels, data types and POUs), organized according to the PLCopen information model.
The address space also contains the obligatory server object which provides basic information of a server instance.

Server object

An FX5-OPC publishes the server object in the address space, which provides information on the current server status, its settings, and capabilities.

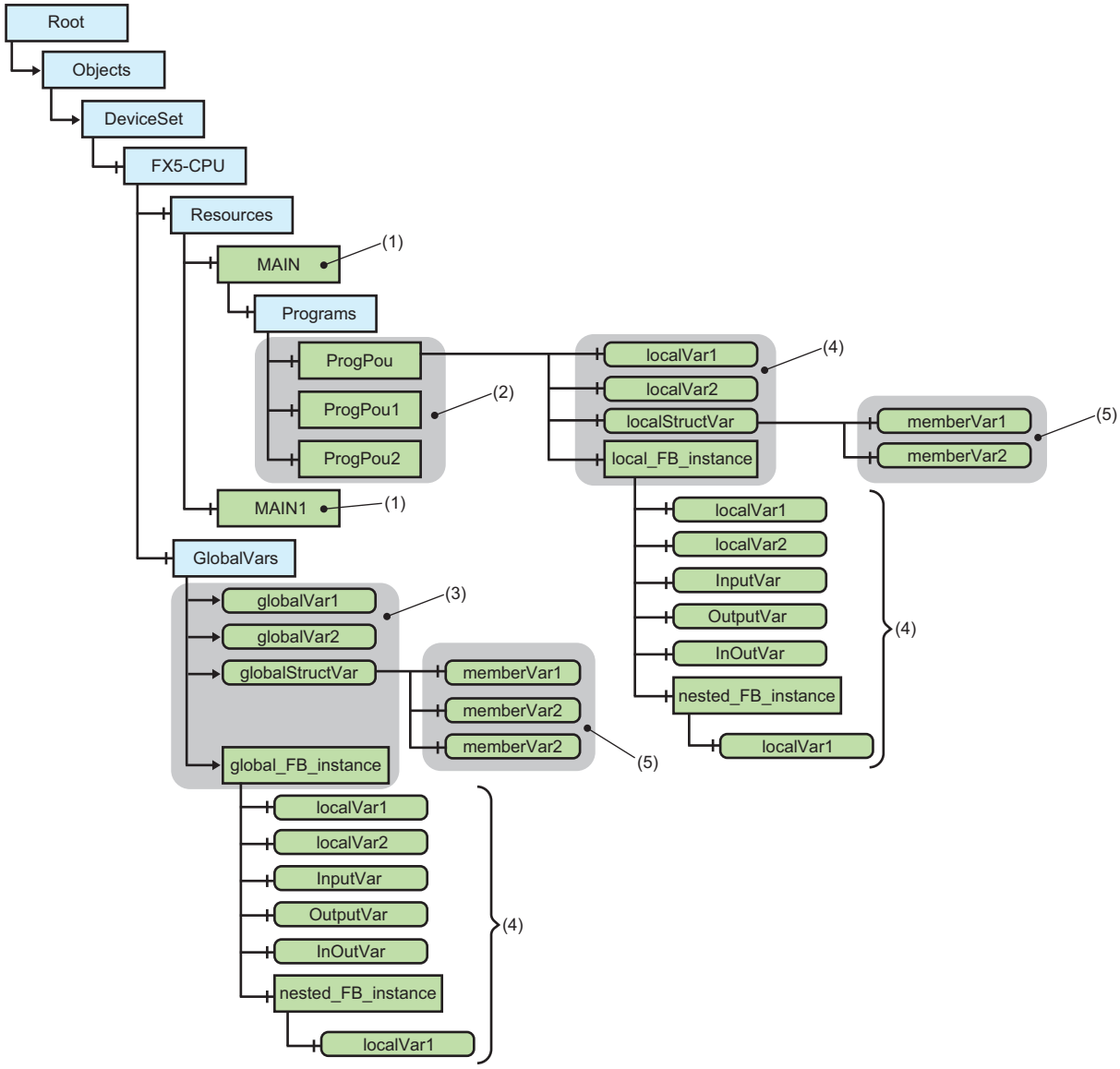


The following table shows the components of the server object.

Component name	Description	Remarks
Auditing	A status whether a server is generating an audit event.	Fixed to false. Audit events are not supported.
NamespaceArray	An array of namespace URIs used by a server.	☞ Page 19 Address space specifications
ServerArray	An array of server URIs.	Only one entry is used for a local server URI.
ServiceLevel	Ability of a server to provide data to an OPC UA client.	Fixed to 255.
ServerStatus	Information on a server status. (Example) product name, manufacturer, software version, etc.	—
ServerCapabilities	Information on server capabilities. (Example) operation limits, supported profiles, software certificate list, etc.	—
ServerDiagnostics	Diagnostic information on a server.	Diagnostic information is not supported. The EnabledFlag variable is set to FALSE; therefore, all nodes in this component cannot be read.
ServerRedundancy	Redundancy capabilities provided by a server.	An FX5-OPC does not support redundancy. The value of RedundancySupport property is fixed to 'none.'
VendorServerInfo	Vendor specific information on a server.	Empty.

User nodes

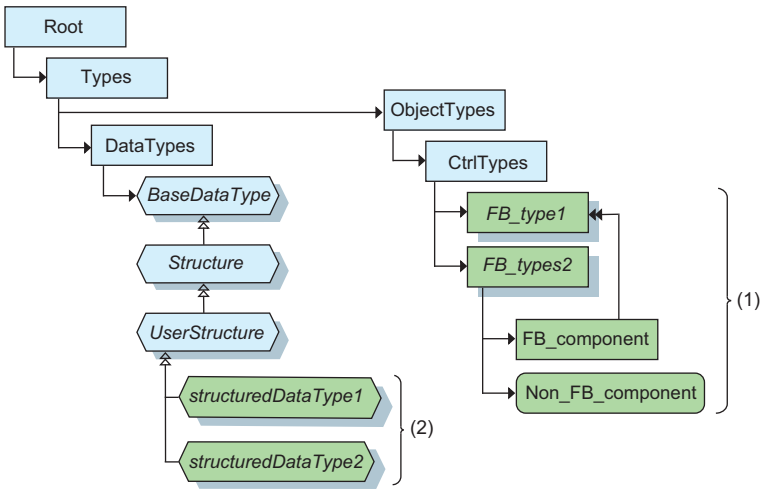
The following shows a part of the address space in which instances of user-defined project elements exist.
The structure of this part is defined by the PLCopen information model; it follows the structure of resources in a programmable controller.



The elements (1) to (5) correspond to elements in a GX Works3 project as shown below:

No.	Element	Corresponding element in a GX Works3 project	Remarks
(1)	Ctrl Resources	Program files	—
(2)	Ctrl Programs	Program blocks	—
(3)	Ctrl Variables (global)	Global labels	Unlike in GX Works3, having multiple groups of global labels is not available. All global variables are stored under a single "GlobalVars" object.
(4)	Ctrl Variables (local)	Local labels of a program block or function block	—
(5)	Members of Ctrl Variables of structured data types	Members of a structure label	These components are exposed only when the setting of "Expose structure members as components" is enabled.

The following shows a part of the address space in which user-defined data types and FB definitions exist.



The elements (1) and (2) correspond to elements in a GX Works3 project as shown below:

No.	Element	Corresponding element in a GX Works3 project	Remarks
(1)	CtrlTypes child components	FB definitions	—
(2)	UserStructure subtypes	Structure definitions	—

4.3 Factory Reset

An FX5-OPC can be restored to its initial state by erasing each setting item stored in the module.
Follow the procedure below:

Operating procedure

1. Unselect the checkboxes of all items in the "Address Space Parameter" screen of GX Works3, and write the parameters to an FX5-OPC.
2. Click the [Delete] button in "Online Operations" in the [Security Parameter] tab of OPC UA Module Configuration Tool to delete the security parameters.
3. Click the [Delete] button in the [IP Address Settings] tab of OPC UA Module Configuration Tool to delete the IP address.
4. Click the [Delete] button in the [Server Certificate] tab of OPC UA Module Configuration Tool to delete the currently used server certificate.

4.4 IP Filter

Unauthorized access can be prevented by identifying the IP address of an access source.
Rules used for identifying an IP address can be set in module parameters of GX Works3. (☞ Page 58 Security settings)
For more details on this function, refer to the following:
📖MELSEC iQ-F FX5 User's Manual (Communication)

Behavior when denying an IP address

When an IP address is denied by rules set in GX Works3, an FX5-OPC discards the packets from the IP address.
When the access destination IP address of the discarded IP packets satisfies both of the following conditions, an event (0810H) is notified with detailed information containing the access source address. (☞ Page 86 Event List)

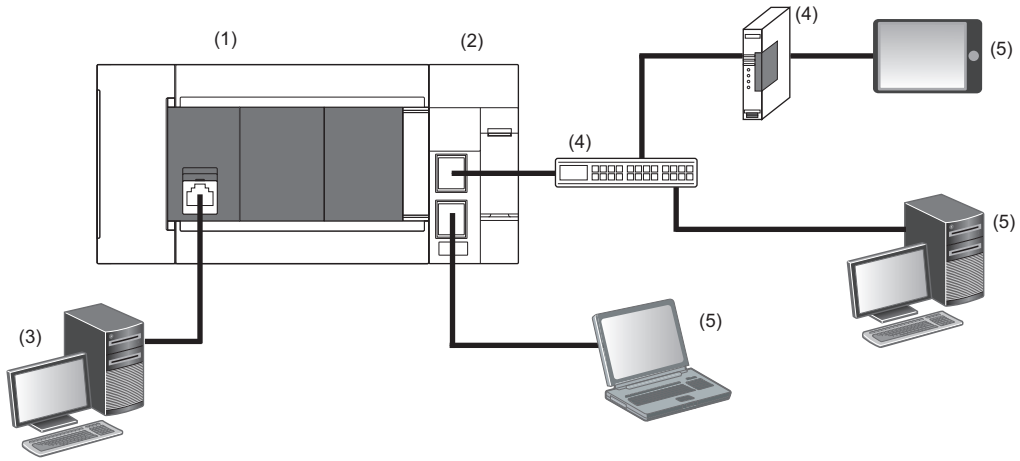
- It is the own address of the FX5-OPC.
- It is not a broadcast address or multicast address.

If a series of discarded IP packets are sent from a single IP address, only the first event is notified.
The notified event can be checked with the diagnostic function of GX Works3. (☞ Page 78 Module diagnostics)

5 SYSTEM CONFIGURATION

5.1 Overall System Configuration

This section shows the overall system configuration when using an FX5-OPC.



(1) FX5U CPU module/FX5UC CPU module
(2) FX5-OPC (OPC UA server)
(3) Personal computer in which GX Works3 or OPC UA Module Configuration Tool is installed
(4) Ethernet switch/router (optional)
(5) OPC UA client

5.2 Supported CPU Modules and Engineering Tools

This section shows the CPU modules and engineering tools supported by an FX5-OPC.

CPU modules

Module name	Firmware version
FX5U CPU module	1.245 or later
FX5UC CPU module*1	

*1 FX5-CNV-IFC or FX5-C1PS-5V is necessary to connect an FX5-OPC to an FX5UC CPU module.

Engineering tools

Engineering tool name	Software version
GX Works3	1.077F or later
OPC UA Module Configuration Tool	1.00A or later

System requirements

■GX Works3

For details, refer to the following:

GX Works3 Installation Instructions

■OPC UA Module Configuration Tool

Item		Description
Personal computer	CPU	Intel® Core™ 2 Duo or more
	Required memory	2 GB or more recommended
Hard disk free space		500 MB or more
Display		Resolution 1024 × 768 pixels or higher
Operating system (English version)*1		• Windows® 10 (Home, Pro, Enterprise, Education) • Windows 8.1 (Core, Pro, Enterprise) • Windows 7 (Starter SP1, Home Basic SP1, Home Premium SP1, Professional SP1, Enterprise SP1)
Interface for communication		Ethernet port: 10BASE-T or more

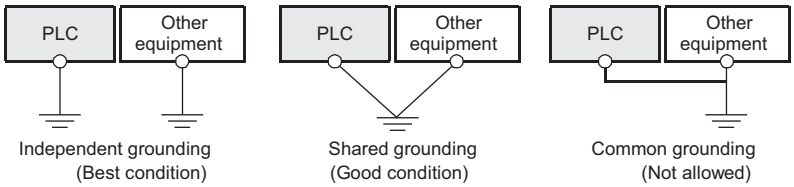
*1 32 bit and 64 bit editions are supported.

6 WIRING

6.1 Grounding

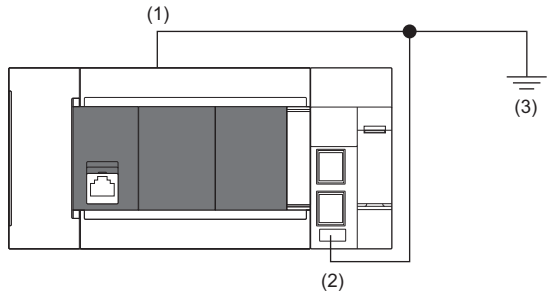
Perform the following.

- Perform class D grounding (Grounding resistance: 100Ω or less).
- Ground the PLC independently when possible.
- If the PLC cannot be grounded independently, perform the "Shared grounding" shown below.



- Bring the grounding point close to the PLC as much as possible so that the ground cable can be shortened.

Grounding of an FX5-OPC



(1) Ground terminal of CPU module
(2) FG terminal of FX5-OPC
(3) D grounding (Grounding resistance: 100Ω or less)

Terminal name	Content
⏚ FG (Ground terminal)	Perform class D grounding. (Grounding resistance: 100Ω or less)

The connection destination for the FG terminal of an FX5-OPC is a spring clamp terminal block.
To connect to the terminal block, there are two ways: by using single wires/strand wires or by using ferrules. Make sure to properly connect in accordance with the following specifications.

■Ferrule

The following table shows wire ferrules and its associated tools compatible with the terminal block.

The shape of the wire ferrule differs depending on the crimp tool to be used, use the reference product.

If the product other than referenced products is used, the wire ferrule cannot be removed. Sufficiently confirm that the wire ferrule can be removed before use.

<Reference product>

Manufacturer	Sleeve	Ferrules model	Suitable wiring size	Crimp tool
PHOENIX CONTACT GmbH & Co. KG	Ferrules with insulation sleeve	AI 0.25-8 YE	0.25mm²	CRIMPFOX 6
		AI 0.34-8 TQ	0.3, 0.34mm²	
		AI 0.5-8 WH	0.5mm²	
		AI 0.75-8 GY	0.75mm²	
	Ferrules without insulation sleeve	A 0.25-7	0.25mm²	
		A 0.34-7	0.3, 0.34mm²	
		A 0.5-8	0.5mm²	
		A 0.75-8	0.75mm²	
		AI 1.0-8	1.0mm²	
		AI 1.5-7	1.25, 1.5mm²	

The wires to connect the spring clamp terminal block are described below.

No. of wire per terminal	Wire size		
	Single wire, strand wire	Ferrule with insulation sleeve	Ferrule without insulation sleeve
Single wiring	AWG 24 to 16 (0.2 to 1.5mm²)	AWG 23 to 19 (0.25 to 0.75mm²)	AWG 23 to 16 (0.25 to 1.5mm²)

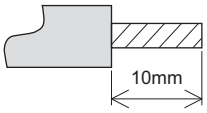
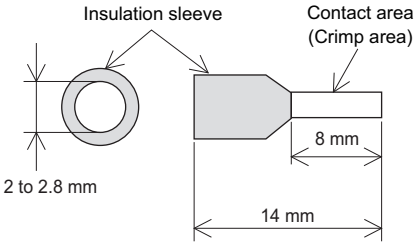
■Wire end treatment

Strip the cable about 10 mm from the tip to connect a wire ferrule at the stripped area.

Failure to do so may result in electric shock due to the conductive part.

If the wire strip length is too short, it may result in the poor contact to the spring clamp terminal part.

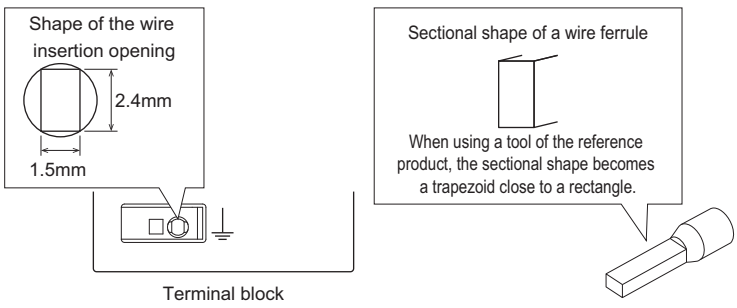
Depending on the thickness of the sheath, it may be difficult to insert into the insulation sleeve, so select the wires by referring to the appearance diagram.

Strand wire/single wire	Ferrule with insulation sleeve
	

Check the shape of the wire insertion opening with the following chart, and use the smaller wire ferrule than the described size.

Also, insert the wire with care so that the wire ferrule is in proper orientation.

Failure to do so may cause the bite of the terminal and the damage of the terminal block.



■Connection and disconnection of the cable

• Connection of the cable

Fully insert a cable whose end has been properly processed into the wire insertion opening.

If the cable cannot be inserted with this procedure, fully insert the cable while pushing the open/close button with a flathead screwdriver having a tip width of 2.0 to 2.5 mm.

After fully inserting the cable, remove the screwdriver.

<Reference>

Manufacturer	Model
PHOENIX CONTACT GmbH & Co. KG	SZS 0.4×2.5 VDE

Precautions

Pull the cable or wire ferrule slightly to check that the cable is securely clamped.

• Disconnection of the cable

Push the open/close button of the wire to be disconnected with a flathead screwdriver.

Pull out the wire with the open/close button pushed.

6.2 Wiring Method

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

Connecting the cable

1. Turn the power supply of an FX5-OPC (CPU module) and external device off.
2. Push the Ethernet cable connector into the FX5-OPC until it clicks. Pay attention to the orientation of the connector.
3. Lightly pull the connector to check that the connector is securely connected.
4. Turn the power supply of the FX5-OPC (CPU module) and external device on.
5. Check whether the SPEED LED of the port connected with an Ethernet cable is on.*1

*1 The time between the cable connection and the turning on of the SPEED LED may vary. The SPEED LED usually turns after a few seconds. Note, however, that the time may be extended further if the link-up processing is repeated depending on the status of the device on the line.

Disconnecting the cable

1. Turn the power supply of the FX5-OPC (CPU module) off.
2. Unplug the Ethernet cable while pressing the latch connector down.

Precautions

- Place the Ethernet cable in a duct or clamp it. Failure to do so may lead to swinging or inadvertent pulling of dangling cable, resulting in damage to the module or the cable or malfunction due to poor contact.
- Do not touch the core of the cable-side or module-side connector, and protect them from dirt or dust. If oil on your hands, dirt, or dust adheres to the core, transmission loss may increase, causing communication problems.
- Check that the Ethernet cable is not disconnected or not shorted and check that the cable is connected properly.
- Do not use Ethernet cables with broken latch connectors. Doing so may cause the Ethernet cables to be disconnected or the module to malfunction.
- Hold the connector part of the Ethernet cable when connecting and disconnecting it. Pulling the cable connected to the module may result in damage to the module or the cable or malfunction due to poor contact.
- For connectors without Ethernet cable, attached connector cover should be placed to prevent foreign matter such as dirt or dust.
- The maximum station-to-station distance of the Ethernet cable is 100 m. However, the acceptable length may be shorter depending on the environment where the cable is used. For details, contact the cable manufacturer.
- The bending radius of the Ethernet cable is limited. For details, check the specifications of the Ethernet cable to be used.

6.3 Wiring Products

This section describes the devices used to comprise a network.

Ethernet cable

Use Ethernet cables that meet the following standards.

Communication speed	Specifications	Connector	Ethernet standard
100Mbps	Ethernet cable: Category 5 or higher (STP cable*1)	RJ45 connector	100BASE-TX
10Mbps	Ethernet cable: Category 3 or higher (STP/UTP cable*1)	RJ45 connector	10BASE-T

*1 Shielded twisted pair cable

A straight/cross cable can be used.

Point

Depending on the connection environment, communication errors may occur due to high-frequency noise from devices other than programmable controllers. The following describes precautionary measures to be taken on FX5-OPC to avoid the influence of high-frequency noise.

[Wiring]

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

Hub

Use hubs which satisfy all the following conditions.

If hubs not satisfying the conditions are used, operation is not guaranteed.

- IEEE802.3 (100BASE-TX) compliant
- The auto MDI/MDI-X function equipped
- The auto-negotiation function equipped
- Switching hub (layer 2 switch)*1

*1 A repeater hub cannot be used.

7 PARAMETER SETTINGS

Set parameters of an FX5-OPC in GX Works3 or OPC UA Module Configuration Tool.

7.1 Parameter List

The following table shows parameters for an FX5-OPC.

Setting tool	Parameter	Description	Reference
GX Works3	Module parameters	General parameters for an intelligent function module such as settings of IP address and whether to enable unsecured connections.	Page 56 Module parameters
	Address space parameters	Information about labels of GX Works3 to be exposed in the FX5-OPC address space.	Page 60 Address space parameters
OPC UA Module Configuration Tool	IP address settings	IP address settings for an FX5-OPC.	Page 65 IP address settings
	Security parameters	Information for establishing connections between an OPC UA server and OPC UA clients.	Page 66 Security parameters
	Server certificate*1	Certificate of an OPC UA server for establishing connections between the server and OPC UA clients.	Page 71 Server certificate

*1 A server certificate has a unique expiration date to prevent encrypted information from being decrypted or disclosed.
Once a server certificate expires, its expiration date cannot be extended.
If the server certificate that is stored in an OPC UA server or OPC UA client expires, communication may be rejected.
Therefore, check the expiration date regularly and renew the server certificate before it expires. (An FX5-OPC notifies an event (0902H) if 80% of the validity period of a server certificate has passed while the OPC UA server is running.)

Point

When an IP address or the enable/disable setting for unsecured connections is specified in both GX Works3 and OPC UA Module Configuration Tool, the setting in OPC UA Module Configuration Tool takes priority.

7.2 Setting Tools

This section explains tools used for setting parameters.

GX Works3

GX Works3 is an engineering tool for setting, programming, debugging, and maintaining programmable controllers.
Module parameters and address space parameters for an FX5-OPC can be set with this tool.
For details on GX Works3, refer to the following:
GX Works3 Operating Manual

Restriction

Address space parameters and security parameters cannot be verified or deleted in GX Works3.

OPC UA Module Configuration Tool

OPC UA Module Configuration Tool is a tool for setting an IP address and security parameters, managing a server certificate, and checking/changing the server status of an FX5-OPC.

Display language

The display language of OPC UA Module Configuration Tool follows the one set in GX Works3.*1
However, it follows the display language of the operating system if GX Works3 is not installed.
For the method to switch the display language of GX Works3, refer to the following:
GX Works3 Operating Manual

*1 If a language other than Japanese or English is set in GX Works3, the display language of OPC UA Module Configuration Tool will be set to English.

Screen display

OPC UA Module Configuration Tool can be started either from GX Works3 or directly.
The menu configuration in the main window differ between when starting the tool from GX Works3 and when starting it directly.
The display contents when starting the tool with each method are shown below:

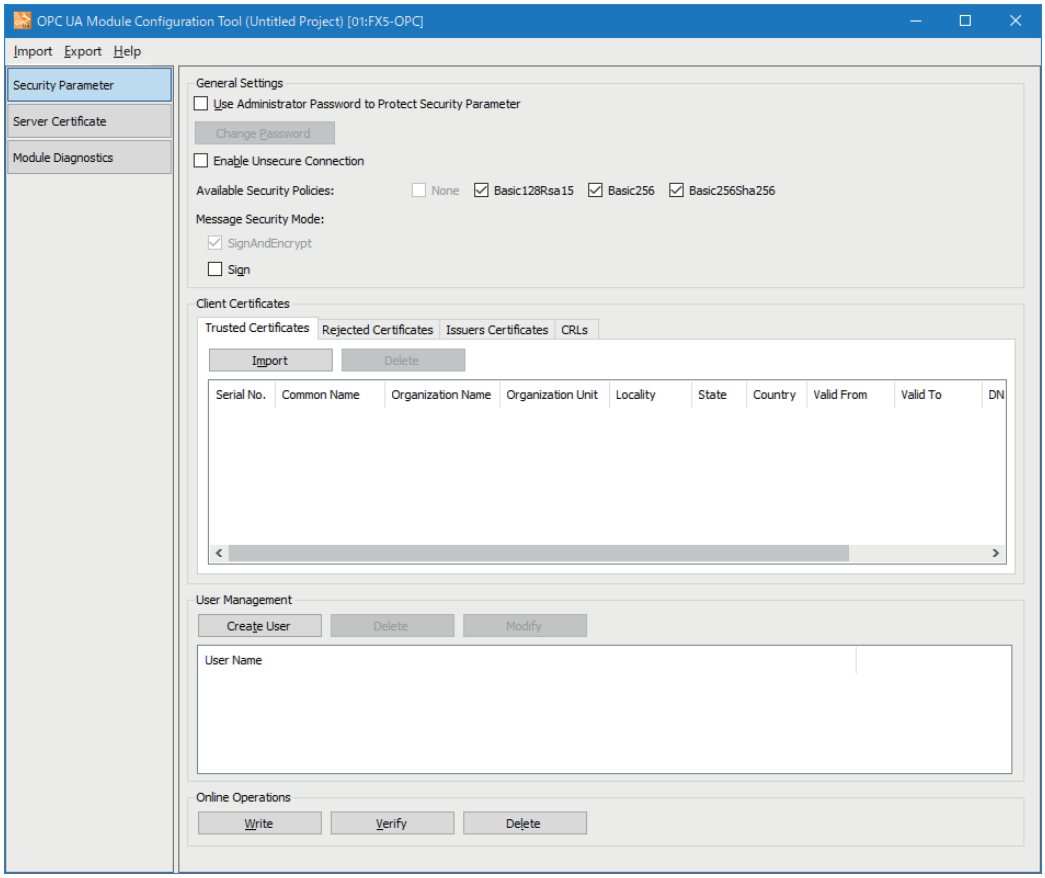
■Starting from GX Works3

The following explains the method to start OPC UA Module Configuration Tool from GX Works3 and the menu items displayed in the main window.

Settings are saved in a GX Works3 project file when saving the project.

Window

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [FX5-OPC] ⇨ [Security Parameter]



Displayed items

Menu item		Description
Import		To import settings from an OPC UA Module Configuration Tool project file to a current project. The [Security parameter] tab opens automatically after the settings are imported.
Export		To export settings of a current project to an OPC UA Module Configuration Tool project file.
Help	Help Contents	To start e-Manual Viewer and display this manual.
	About	To display information of OPC UA Module Configuration Tool such as its version.

Point

When starting OPC UA Module Configuration Tool from GX Works3, setting a connection destination is not required since the setting of GX Works3 is utilized.

■Starting directly

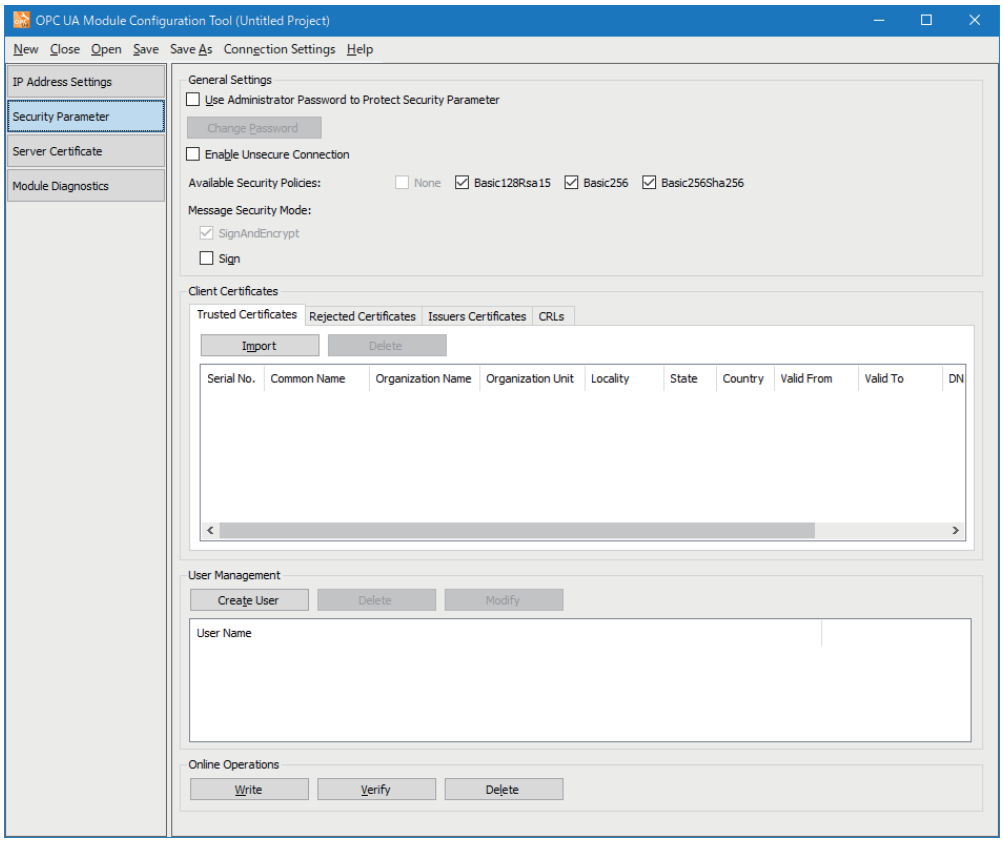
The following explains the method to start OPC UA Module Configuration Tool directly and the menu items displayed in the main window.

Settings are saved as a OPC UA Module Configuration Tool project file (*.mopc).

Window

Select [MELSOFT] ⇨ [OPC UA Module Configuration Tool] from Windows® Start*1.

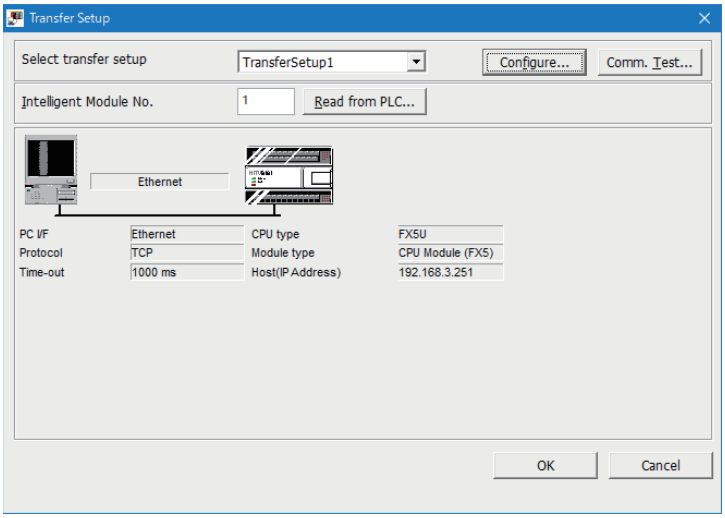
*1 Select [All apps] in the Start screen or [Start] ⇨ [All Programs]/[All apps].



Displayed items

Menu item		Description
New		To create a new project. The [Security parameter] tab opens automatically when the project is created.
Close		To close a current project.
Open		To open an existing project. The [Security parameter] tab opens automatically when the project is opened.
Save		To save a current project.
Save As		To save a current project as a new project.
Connection Settings		To open the "Transfer Setup" screen. Configure settings to connect to a CPU module in that screen.
Help	Help Contents	To start e-Manual Viewer and display this manual.
	About	To display information of OPC UA Module Configuration Tool such as its version.

• "Transfer Setup" screen



Displayed items

Item	Description
Select transfer setup	Select a connection destination to be used.
[Configure] button	Click this to open the "Transfer Setup Wizard" screen. In that screen, set details on the connection destination selected in "Select transfer setup."
[Comm.Test] button	Click this to perform the communication test between OPC UA Module Configuration Tool and a CPU module.
Intelligent Module No.	Enter the intelligent module number of an FX5-OPC.
[Read from PLC] button	Click this to read a list of intelligent function modules attached to a CPU module. Select an FX5-OPC from the list.
Selected transfer setup display	An image which shows detailed setting information of a selected connection destination is displayed.

Point

If a remote password is set on a CPU module, the password is required when connecting to the CPU module for the first time; however, the password will be required again in either of the following cases:

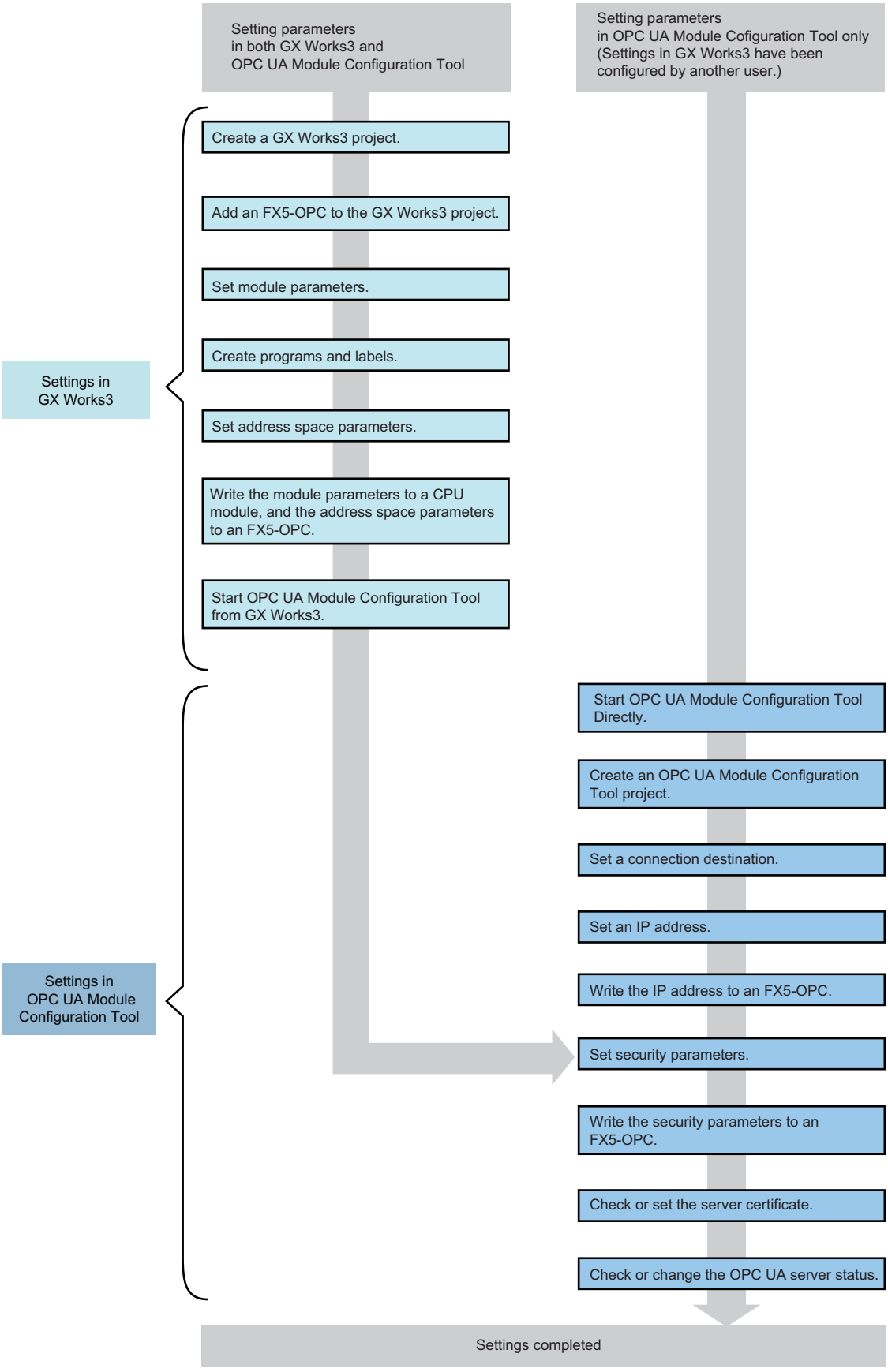
• A remote password is changed.

• The "Transfer Setup" screen is closed by clicking the [OK] button.

For details on a remote password, refer to the following:

MELSEC iQ-F FX5 User's Manual (Communication)

7.3 Setting Procedure



For details on each setting, refer to the following:

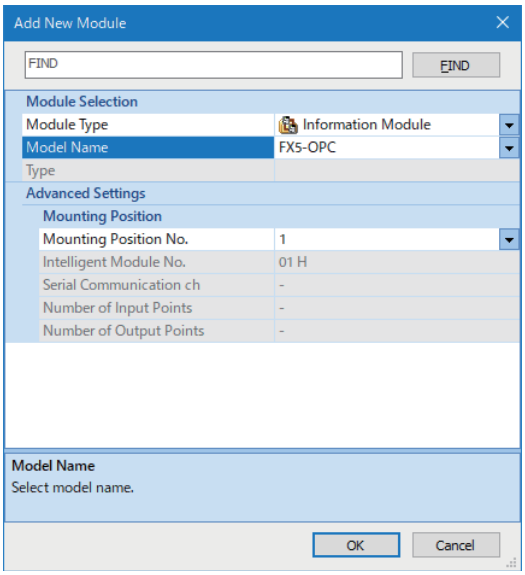
Item	Reference
Creating a GX Works3 project	GX Works3 Operating Manual
Adding an FX5-OPC to the GX Works3 project	Page 55 Adding an FX5-OPC
Setting module parameters	Page 56 Module parameters
Creating programs and labels	GX Works3 Operating Manual
Setting address space parameters	Page 60 Address space parameters
Writing the module parameters to an CPU module, and the address space parameters to an FX5-OPC	Page 64 Online operations
Starting OPC UA Module Configuration Tool from GX Works3	Page 50 Starting from GX Works3
Starting OPC UA Module Configuration Tool directly	Page 51 Starting directly
Creating an OPC UA Module Configuration Tool project	
Setting a connection destination	
Setting an IP address	Page 65 IP address settings
Writing the IP address to an FX5-OPC	
Setting security parameters	Page 66 Security parameters
Writing the security parameters to an FX5-OPC	
Checking/setting a server certificate	Page 71 Server certificate
Checking/changing the OPC UA server status	Page 74 Module diagnostics

Adding an FX5-OPC

The following explains the procedure to add an FX5-OPC to a GX Works3 project.

Operating procedure

1. Select "Parameter" ⇨ "Module Information" in the Navigation window.
2. Right-click it and select [Add New Module] from the shortcut menu.
   The "Add New Module" screen appears.
3. Set the following items and click the [OK] button.
   Module Type: Information Module
   Model Name: FX5-OPC



Module parameters

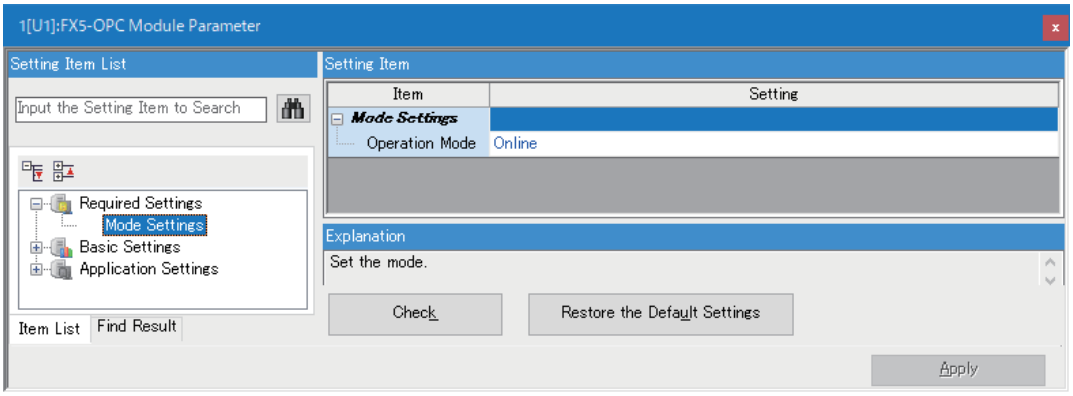
Module parameters can be set in GX Works3.

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [FX5-OPC] ⇨ [Module Parameter]

Required settings

■Mode settings

Set the operation mode of an FX5-OPC.



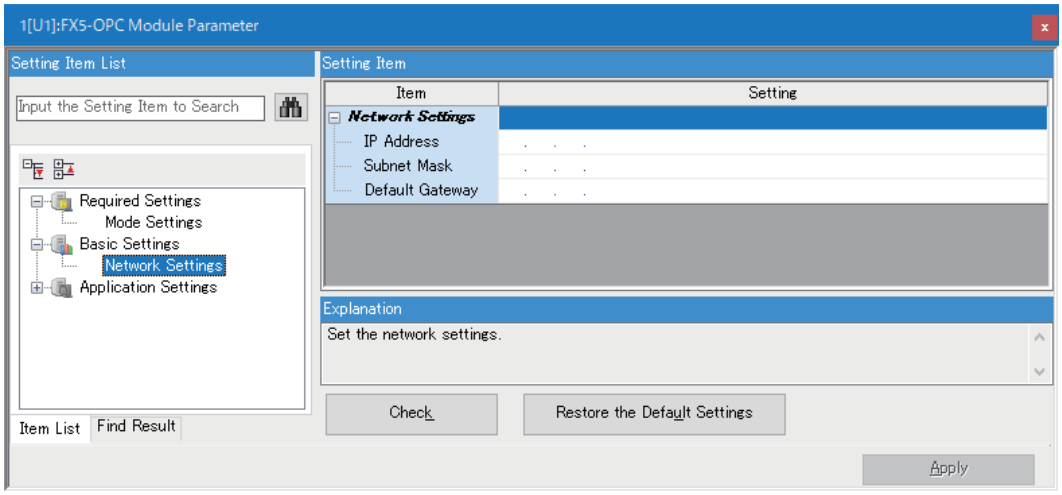
Displayed items

Item	Description	Setting range
Operation Mode	Set the operation mode of an FX5-OPC. • Online: Normal operation mode • Hardware test: Mode in which the module performs a self-diagnostics test. Select this mode when checking the operation of the module due to an error or similar problem.(☞ Page 81 Hardware Test)	• Online • Hardware test

Basic settings

■Network settings

Set the IP address of an FX5-OPC.



Displayed items

Item	Description	Setting range
IP Address*1*2	Set the IP address of an FX5-OPC. Set the class and subnet address of the FX5-OPC to the same settings as those of the external devices that communicate with the FX5-OPC. Contact the network administrator before setting the IP address.	• Blank • 1.0.0.1 to 223.255.255.254
Subnet Mask*1	Set the subnet mask of an FX5-OPC. When setting the IP address of the default gateway and performing communication with an external device in another network through a router, set the subnet mask pattern of the default gateway. All the devices in the same subnet should have a common subnet mask. The subnet mask setting is not required for communication in a single network.	• Blank • 192.0.0.0 to 255.255.255.252
Default Gateway*2	Set the default gateway of an FX5-OPC. Set the IP address of the relay device (default gateway) to access the external device in another network. Set a value that satisfies the following conditions as the IP address of the default gateway. • The class of the IP address is A, B, or C. • The subnet address of the default gateway is the same as that of the FX5-OPC.	• Blank • 1.0.0.1 to 223.255.255.254

*1 When the parameters are written to a CPU module without setting both the IP address and subnet mask, each address is set as follows:
IP address: 192.168.3.251
Subnet mask: 255.255.255.0

*2 Do not set a value that results in all bits of the host address being "0" or "1."

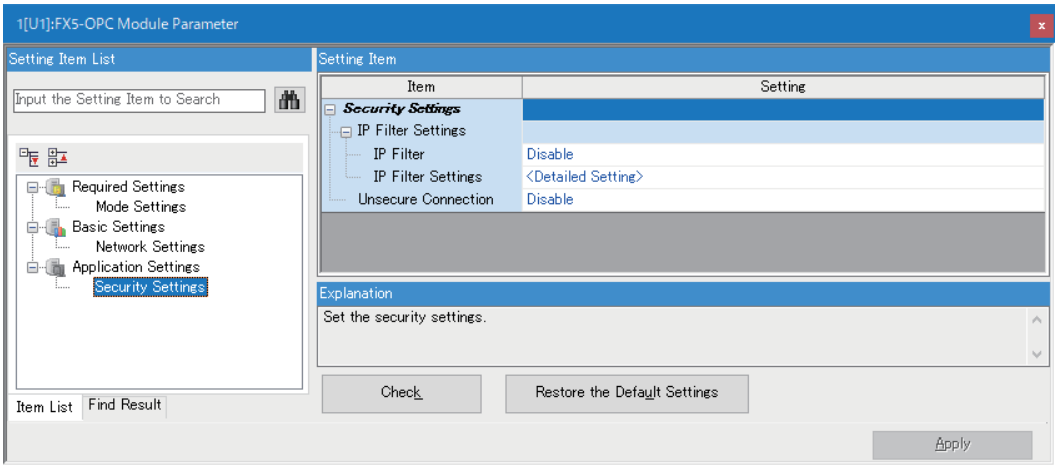
Point

When an IP address is specified in both GX Works3 and OPC UA Module Configuration Tool, the setting in OPC UA Module Configuration Tool takes priority.

Application settings

■Security settings

Set the security function.



Displayed items

Item		Description	Setting range
IP Filter Settings	IP Filter	Set whether to enable the IP filter function.	• Disable • Enable
	IP Filter Settings	Set the IP address to be allowed or denied.	—
Unsecure Connection		Select whether to enable unsecured connections from OPC UA clients.	• Disable • Enable

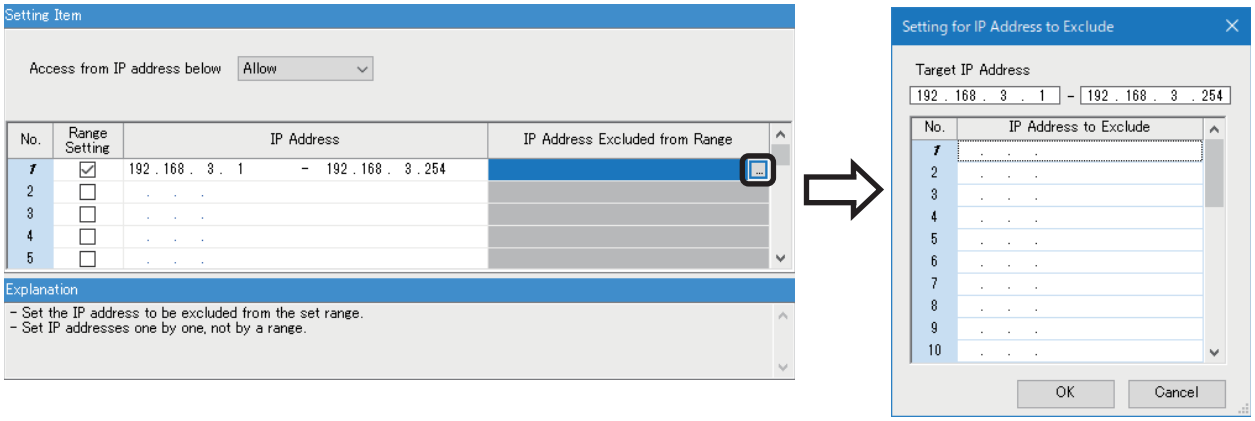
Point

When the enable/disable setting for unsecured connections is specified in both GX Works3 and OPC UA Module Configuration Tool, the setting in OPC UA Module Configuration Tool takes priority.(☞ Page 75 Enabling Unsecured Connections)

• IP filter settings

Set the IP address for which the IP filter function will be used.

Double-click <Detailed Setting> of "IP Filter Settings."



Displayed items

Item	Description	Setting range
Access from IP address below	Select whether to allow or deny the access from the specified IP addresses.	• Allow • Deny
Range Setting	Select the checkbox when specifying the IP addresses by range.	—
IP Address	Set the IP address to be allowed or denied. When selecting the checkbox of "Range Setting", enter the start IP address (left field) and end IP address (right field) of the range.	• Blank • 0.0.0.1 to 223.255.255.254
IP Address Excluded from Range	Set the IP address to be excluded from the set range when selecting the checkbox of "Range Setting." Up to 32 IP addresses can be set.	• Blank • 0.0.0.1 to 223.255.255.254

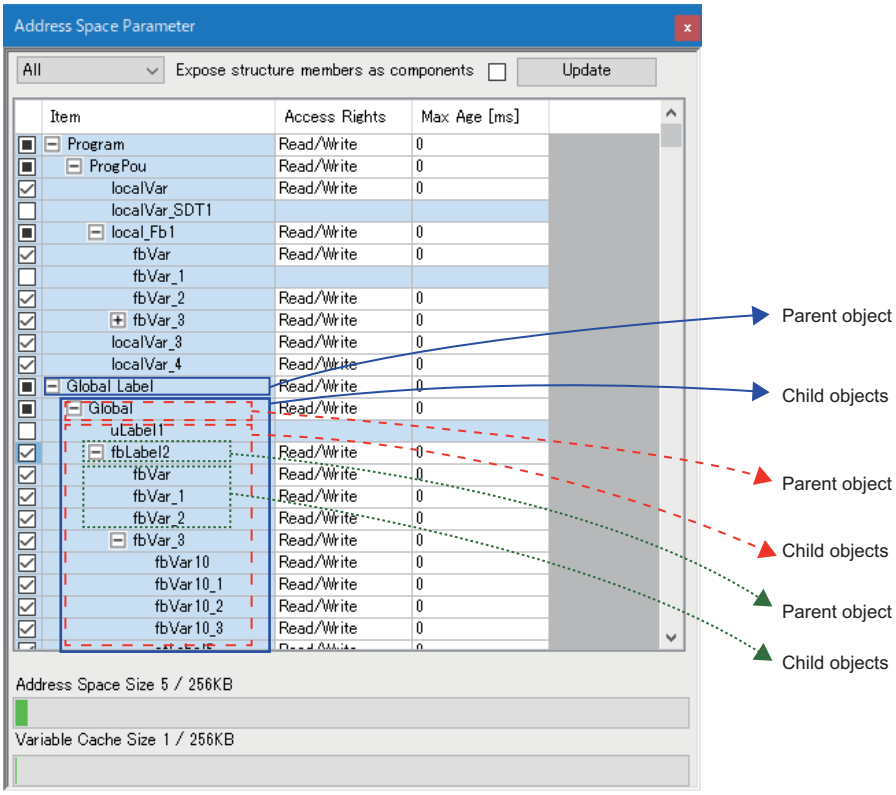
Address space parameters

Labels to be exposed in the address space can be selected in the "Address Space Parameter" screen of GX Works3.

"Address Space Parameter" screen

Window

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [FX5-OPC] ⇨ [Address Space Parameter]



Displayed items

Name	Description	Setting range
Drop-down list	Select labels to be displayed in the list.	• All • Checked • Unchecked
Expose structure members as components	Select the checkbox to expose structure members in the address space as components. An OPC UA client can access each member of a structure by selecting this checkbox. If the checkbox is not selected, a client can access the structure only as a single value, but cannot access individual members. For details, refer to the following: ☞ Page 20 User-defined structure Note that structure members are not displayed in this screen regardless of the selection status of this item.	• Enabled • Disabled
[Update] button	Click this to read information of labels set in the label editor of GX Works3 again and update the display to the latest information.*1 When data needs to be updated, such as when data related to address space parameters in a project is changed, ⚠ is displayed on the button.	—
Item	Names of labels and their parent objects in a GX Works3 project are displayed.	• Item name • Label name
Checkbox	Select labels to be exposed in the address space.*2	• No label selected • Some labels selected • All labels selected
Access Rights	Set the access right to the value of each label.*2, *3 When "Read/Write" is set, the label value can be read and written; however, the value can be only read when "Read" is set. For a constant label, "Read" is set and cannot be edited.	• Read/Write • Read

Name	Description	Setting range
Max. Age [ms]	For a variable label, set maximum elapsed time since the variable was read in milliseconds.*2, *3 For a constant label, this cell is blank and cannot be edited.	• Variable label: 0 to 10000 • Constant label: blank
Address Space Size	Size of the address space parameters calculated based on the types of the selected labels is displayed.*4	0 to 256KB
Variable Cache Size	Size of a variable cache calculated based on the data types of the selected labels is displayed.*4	0 to 256KB

*1 The state of the tree (expanded or collapsed) is not changed by updating data.

*2 For details on settings of access rights, maximum elapsed time, and labels to be exposed when a parent and child objects exist, refer to the following:
☞ Page 62 Parent object and child object

*3 Values of constant labels cannot be edited. If the checkbox of a constant label is selected, "Read" is set in "Access Rights" and the "Max Age [ms]" cell is left blank.

*4 The color turns from green to red when the size exceeds the setting range.

Restriction

A tree of structure labels cannot be expanded.

In addition, the following labels cannot be used.

- Label of which the data type is not supported by OPC UA (☞ Page 19 Simple data types)
- Label to which a device that is not supported by OPC UA is assigned (☞ Page 19 Simple data types)
- Structure array type label
- Array type label with more than 1024 elements
- Label of which data type is a macro type function block
- Local label of a function

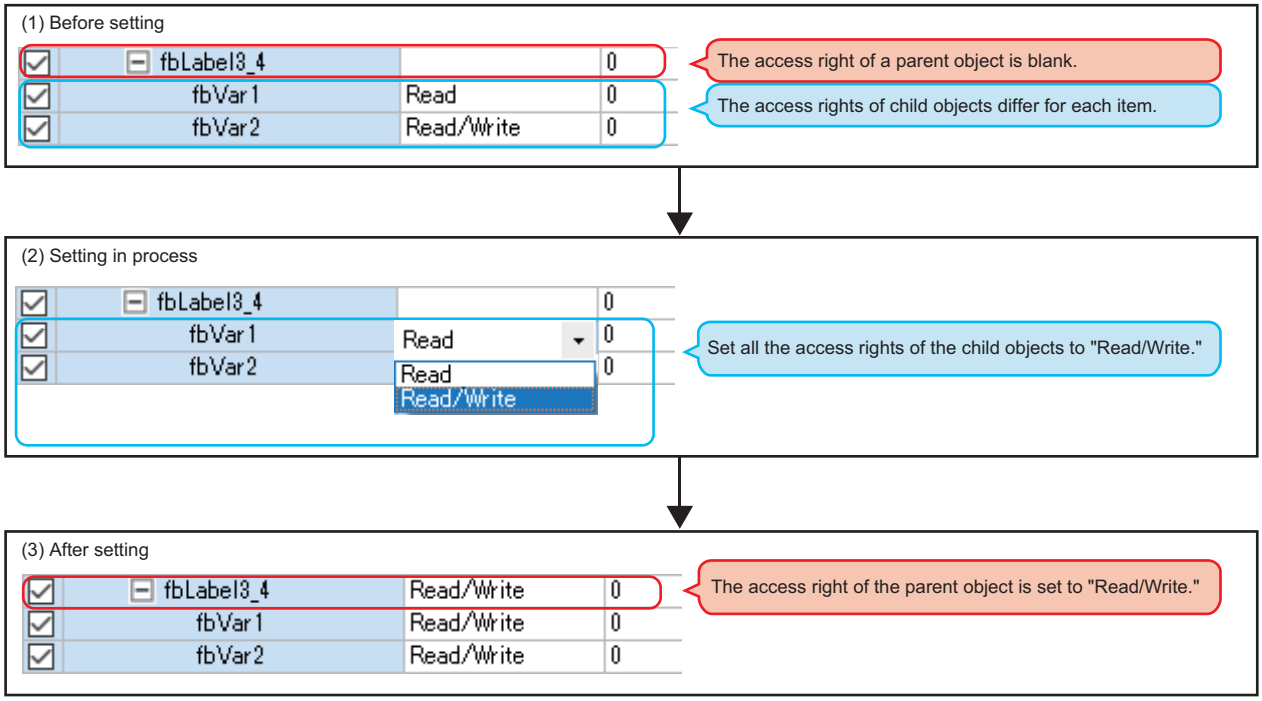
Point

- EN and ENO of a function block can be displayed in the list by selecting "Yes" for "Use EN/ENO" in the "Properties" screen for the function block.
- When closing the "Address Space Parameter" screen, the selection status of the labels and checkbox of "Expose structure members as components" is automatically saved.

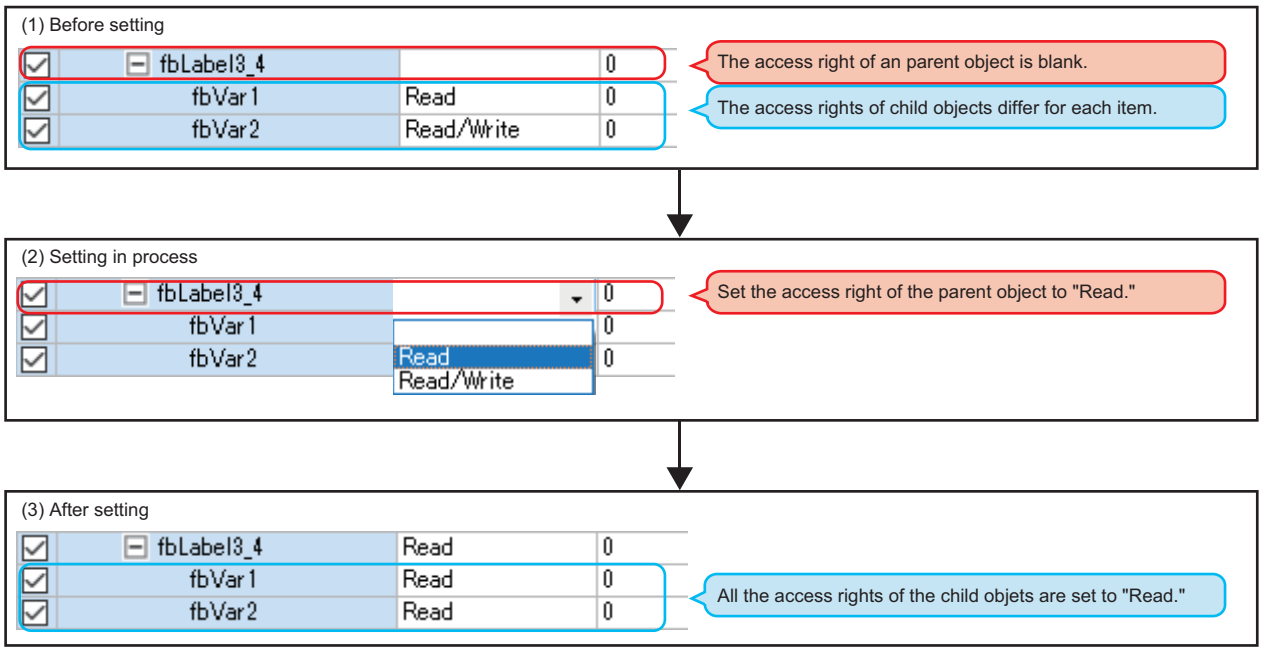
■Parent object and child object

Items displayed in the "Address Space Parameter" screen are classified into two types: parent object and child object.
Labels in a GX Works3 project are called child objects, and the items which include child objects, such as label lists, program blocks, and programs, are called parent objects.
Values of parent objects or child objects may be set automatically depending on setting content of the checkbox, access right column, or maximum elapsed time column of each item.

- When setting a same value for the access rights or maximum elapsed time of all selected child objects, the value is also displayed for their parent object.



- When setting a value for the access right or maximum elapsed time of a parent object, the same value is set for all its child objects.
  However, those values of constant labels are not changed since they are fixed.



■Updating address space parameter data

When performing any of the following operations in GX Works3, data of the address space parameters needs to be updated by clicking the [Update] button so that the data matches with GX Works3 project data.

- Any of the following data is newly created in the navigation window:
  - · Program block
  - · Function block
  - · Global label
- Any of the following data is pasted, renamed, or deleted in the navigation window:
  - · Program block
  - · Function block
  - · Structure
  - · Global label
- Any of the following labels is added, renamed, or deleted in an editor:
  - · Global label
  - · Local label of a program or function block
  - · Structure member
- A data type, array size, or assigned device of any of the following labels is changed in an editor:
  - · Global label
  - · Local label of a program or function block
  - · Structure member
- The status of "Use EN/ENO" is changed in the "Properties" screen for a function block.
- "FB type" of an FB file is changed.

Precautions

If a selected label becomes unsupported due to any changes mentioned in above, the label is removed from the "Address Space Parameter" screen.

Online operations

Module parameters can be written to a CPU module, and address space parameters to an FX5-OPC in the "Online Data Operation" screen of GX Works3.
For details on the online operations of GX Works3, refer to the following:
GX Works3 Operating Manual

Point

- In the "Online Data Operation" screen, module parameters stored in a CPU module can be read, verified, or deleted.
- Address space parameters in an FX5-OPC cannot be verified or deleted in the "Online Data Operation" screen of GX Works3.
  To delete the parameters, unselect all the checkboxes in the "Address Space Parameter" screen and write the parameters to the module again.

Online operations while an OPC UA server is running

Some online operations require stopping the OPC UA server function before the operation.
In that case, GX Works3 or OPC UA Module Configuration Tool displays a confirmation message.
Confirm the message, and decide either to stop the OPC UA server function and execute an online operation, or to abort the operation.
After the operation is finished, another confirmation message appears and asks if restarting the OPC UA server function.
If not restarting the OPC UA server function immediately, the function can be restarted at any timing by either of the following operations:

- Resetting a CPU module.
- Click the [Start Server] button in the [Module Diagnostics] tab of OPC UA Module Configuration Tool.

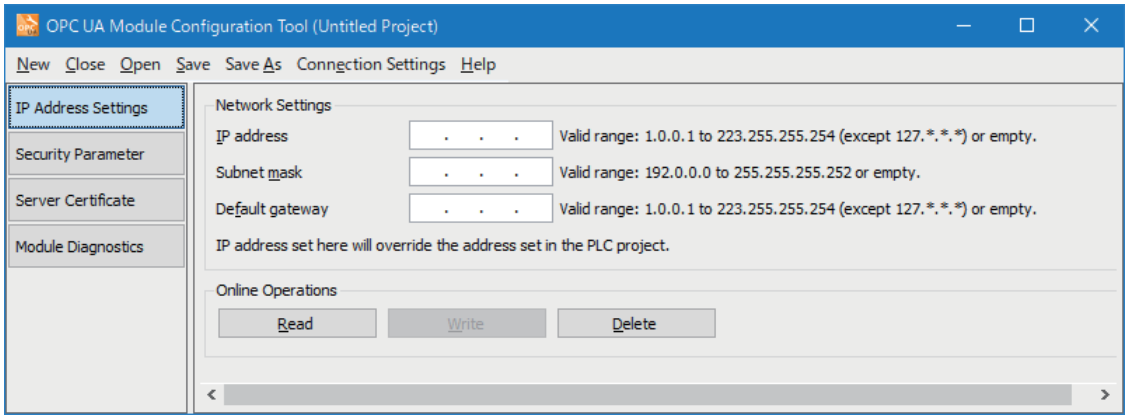
Some online operations require resetting a CPU module to apply changes after the operation.
The following table lists all online operations with their corresponding requirements.

Parameter	Online operation	Stopping the OPC UA server function before operation	Resetting a CPU module after operation
Module parameters	Read	Not required	Not required
	Write		Required
	Verify		Not required
	Delete		Required
Address space parameters	Write	Required	Not required
IP address settings	Read	Not required	Not required
	Write		Required
	Delete		
Security parameters	Write	Required	Not required
	Verify	Not required	
	Delete	Required	
Server certificate	Refresh	Not required	Not required
	Generate a New Self-Signed Certificate	Required	
	Write (Replace)		
	Delete		

IP address settings

An IP address, subnet mask, and default gateway can be set in the [IP Address Settings] tab of OPC UA Module Configuration Tool.

This tab is displayed only when OPC UA Module Configuration Tool is started directly, not from GX Works3.



Displayed items

Item		Description
Network Settings	IP address	Set an IP address to be used for communications with OPC UA clients. Any address from Class A, B, or C is available.
	Subnet mask	Set a subnet mask to be used for communications with OPC UA clients. If an IP address is specified before this item, the subnet mask is set automatically based on the IP address class. • Class A: 255.0.0.0 • Class B: 255.255.0.0 • Class C: 255.255.255.0
	Default gateway	Set a default gateway to be used for communications with OPC UA clients.
Online Operations	[Read] button	Click this to read the values of IP address, subnet mask, and default gateway from an FX5-OPC.
	[Write] button	Click this to write the values of IP address, subnet mask, and default gateway to an FX5-OPC. The values can be written only when any of the following conditions is satisfied: • Values entered for the IP address, subnet mask, and default gateway are valid. • Values entered for the IP address and subnet mask are valid, and the default gateway is blank.
	[Delete] button	Click this to delete the IP address, subnet mask, and default gateway set in an FX5-OPC.

Point

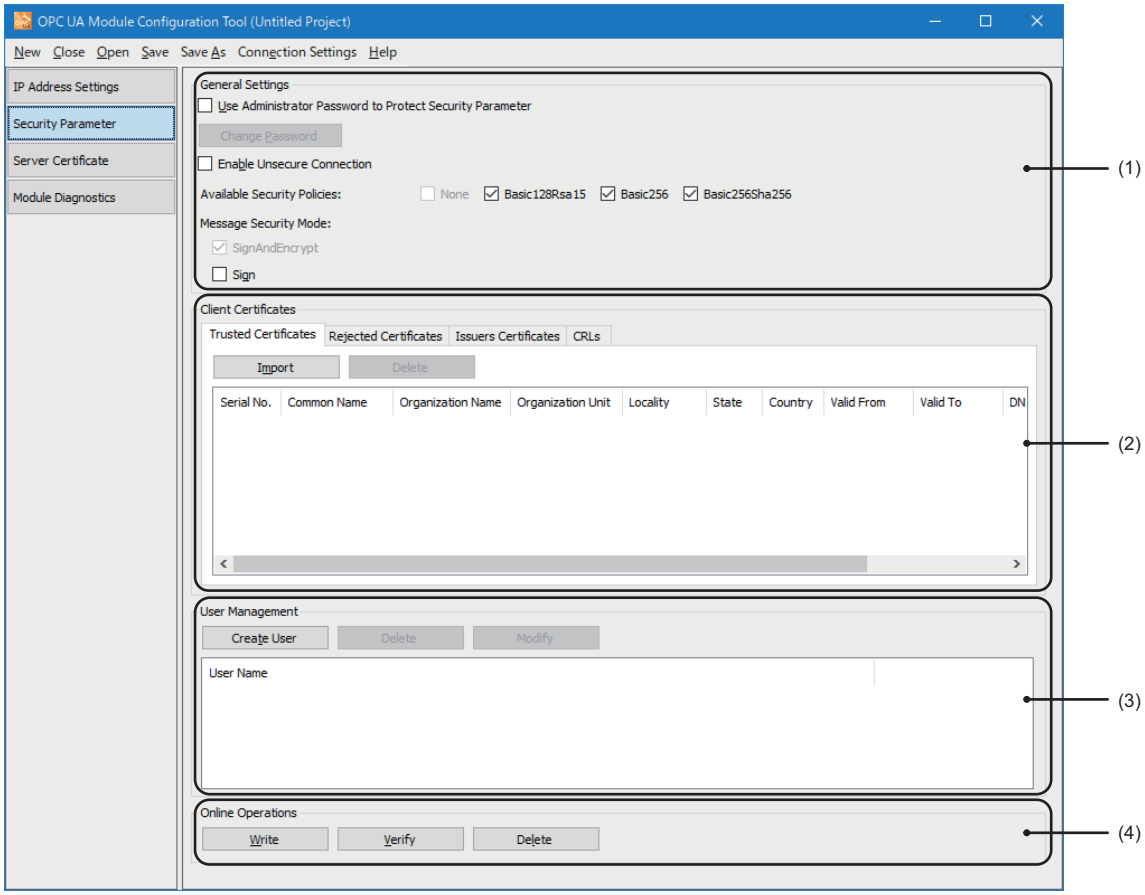
After writing or deleting an IP address, reset a CPU module to apply the changes.

For details, refer to the following:

☞ Page 64 Online operations while an OPC UA server is running

Security parameters

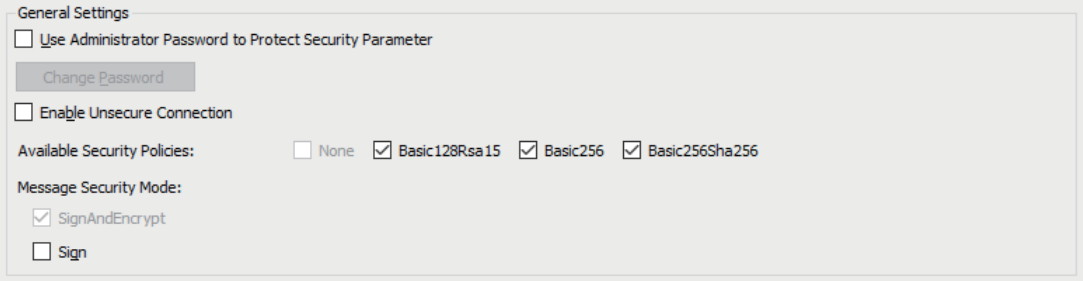
Security parameters can be set in the [Security parameter] tab of OPC UA Module Configuration Tool.



Displayed items

No.	Item	Description	Reference
(1)	General Settings	Set general settings.	Page 67 General settings
(2)	Client Certificates	Manage client certificates.	Page 68 Client certificates
(3)	User Management	Manage users authorized to access an OPC UA server. All authorized users are displayed in the list.	Page 70 User management
(4)	Online Operations	Write security parameters to an FX5-OPC or delete the parameters stored in the module. In addition, security parameters set in OPC UA Module Configuration Tool can be checked if they match with the settings in an FX5-OPC.	Page 70 Online operations

General settings



Displayed items

Item		Description
Use Administrator Password to Protect Security Parameter		Select the checkbox to set a password to protect security parameters.*1,*2, *3 The password is used for encryption of security parameter data and authorization of an administrator. The "Password" dialog appears after selecting this checkbox. Note that the set password will be deleted once this checkbox is unselected.
[Change Password] button		Click this to change the current password.
Enable Unsecure Connection		Select the checkbox to expose the endpoint of None security policy.*4
Available Security Policies	None	This item is always disabled. The selection status depends on the status of the checkbox of "Enable Unsecure Connection."
	Basic128Rsa15	Select the checkbox to expose the endpoint of Basic128Rsa15 security policy.
	Basic256	Select the checkbox to expose the endpoint of Basic256 security policy.
	Basic256Sha256	Select the checkbox to expose the endpoint of Basic256Sha256 security policy.
Message Security Mode	SignAndEncrypt	Select the checkbox to expose the endpoint of SignAndEncrypt message security mode. This checkbox is always selected. It cannot be unselected.
	Sign	Select the checkbox to expose the endpoint of Sign message security mode.

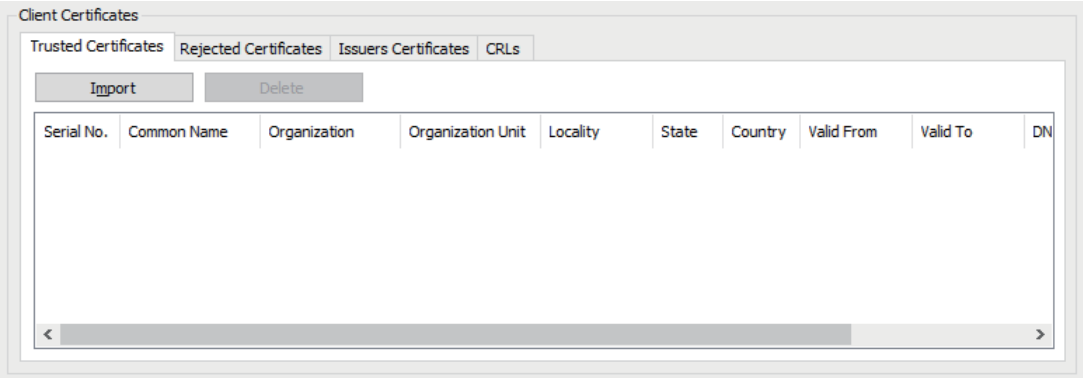
*1 A password needs to be 6 to 31 characters long.
*2 All Unicode characters are available.
*3 Characters are case-sensitive.
*4 For the considerations when enabling unsecured connections, refer to the following:
☞ Page 75 Enabling Unsecured Connections

Client certificates

■Trusted certificates

In the [Trusted Certificates] tab, trusted certificates are displayed in a list.

A certificate can be imported or deleted.



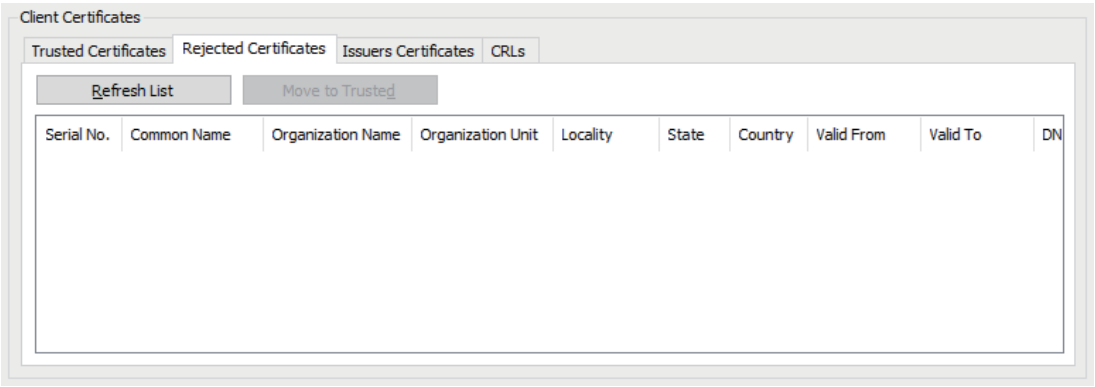
Displayed items

Item	Description
[Import] button	Click this to import a trusted certificate from a DER-format X.509 certificate file.
[Delete] button	Click this to delete a trusted certificate selected in the list.

■Rejected certificates

In the [Rejected Certificates] tab, rejected certificates are displayed in a list.

The list can be refreshed. In addition, any of the displayed certificates can be moved to the trusted certificate list.



Displayed items

Item	Description
[Refresh List] button	Click this to reload the rejected certificates from an FX5-OPC.
[Move to Trusted] button	Click this to move a rejected certificate, selected in the list, to the trusted certificate list.*1, *2, *3

*1 A rejected certificate can also be moved by dragging and dropping the certificate onto the trusted certificate list.
In that case, change tabs by placing a cursor on the [Trusted certificates] tab with the rejected certificate dragged, and drop it onto the trusted certificate list.

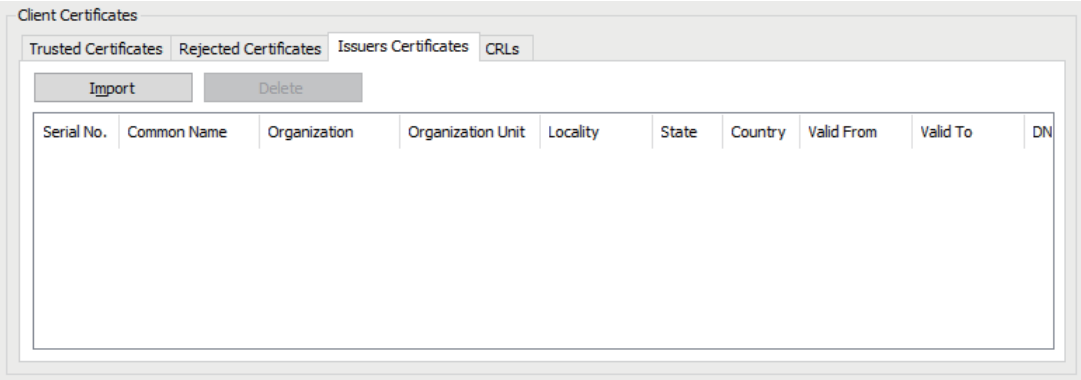
*2 Once the certificate is moved, it is immediately removed from the rejected certificate list; however, it is not deleted from data in an FX5-OPC.
To delete the certificate from data in the FX5-OPC, click the [Clear Store] button in the [Module Diagnostics] tab, or reset a CPU module. (☞ Page 74 Module diagnostics)

*3 The actual rejected certificate list is stored in an FX5-OPC and is not a part of the offline project data.
When OPC UA Module Configuration Tool is connected to an FX5-OPC, the tool reads the rejected certificate list and displays it in this tab.
A certificate, which already exists in the trusted certificate list, is not displayed (filtered).
Note that if another instance of OPC UA Module Configuration Tool is connected to the same FX5-OPC at the same time, the displayed rejected certificate list may differ, due to different contents of the trusted certificates lists in both instances.

■Issuers certificates

In the [Issuers Certificates] tab, certificates of intermediate certificate authorities are displayed in a list.

A certificate can be imported or deleted.



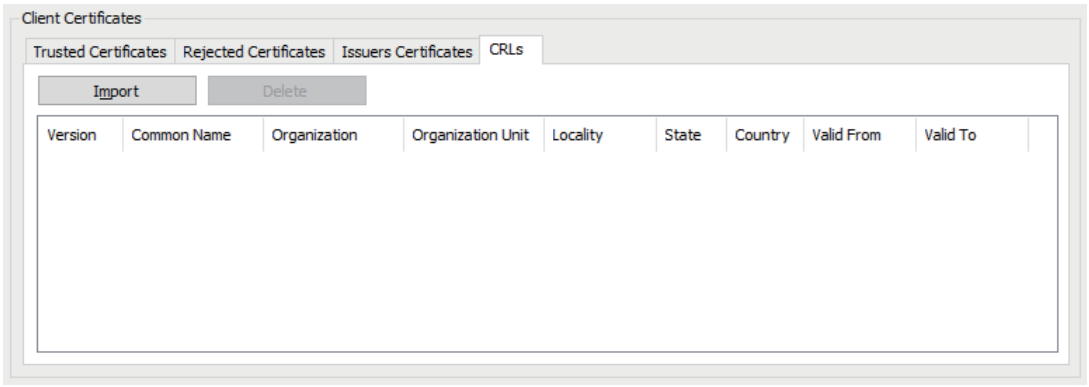
Displayed items

Item	Description
[Import] button	Click this to import a certificate of intermediate certificate authority from a DER-format X.509 certificate file.
[Delete] button	Click this to delete the certificate of an issuer selected in the list.

■CRLs (Certificate Revocation Lists)

In the [CRLs] tab, CRLs are displayed in a list.

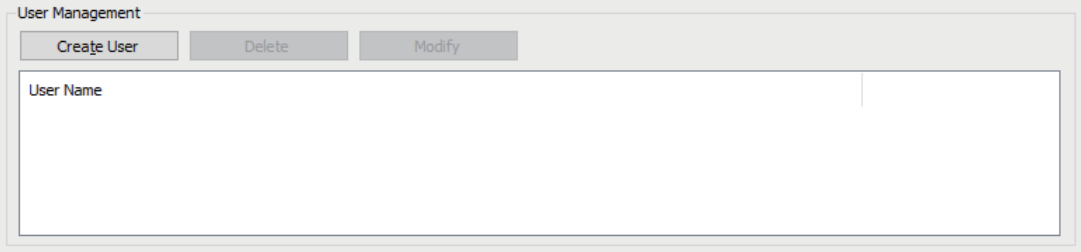
A CRL can be imported or deleted.



Displayed items

Item	Description
[Import] button	Click this to import a CRL from a DER-format X.509 certificate file.
[Delete] button	Click this to delete a CRL selected in the list.

User management

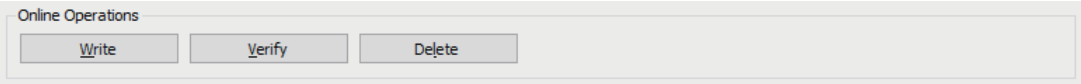


Displayed items

Item	Description
[Create User] button	Click this to open the "Create User" dialog. Set a user name and password in that screen.*1, *2, *3
[Delete] button	Click this to delete a user selected in the list.
[Modify] button	Click this to open the "Modify User" dialog for a user selected in the list. The password of the selected user can be changed in that screen.

*1 Each user name and password needs to be 6 to 31 characters long.
*2 Characters are case-sensitive.
*3 All Unicode characters are available.

Online operations



Displayed items

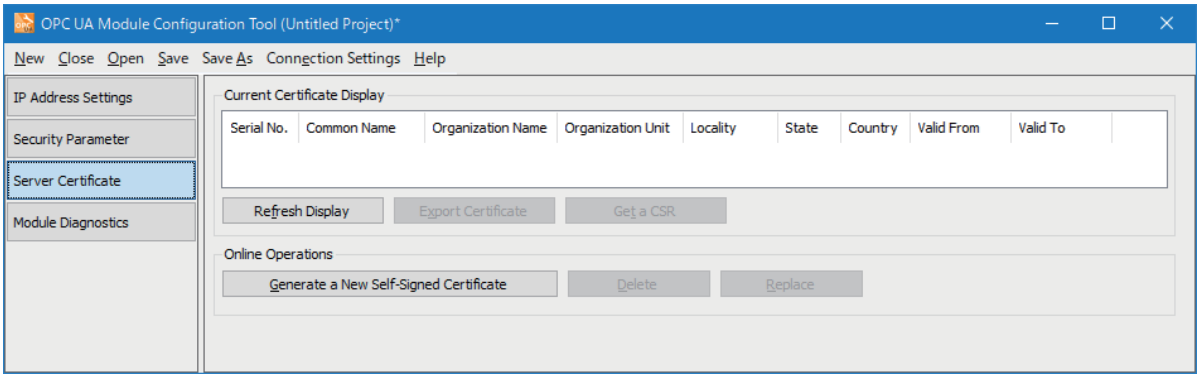
Item	Description
[Write] button	Click this to write the following security parameter settings to an FX5-OPC: • Enable Unsecure Connection • Trusted Certificates • Issuers Certificates • CRLs • User Management
[Verify] button	Click this to check whether the data in an FX5-OPC matches the current settings and display the result in a message box.
[Delete] button	Click this to delete the following security parameter settings written in an FX5-OPC: • Enable Unsecure Connection • Trusted Certificates • Issuers Certificates • CRLs • User Management

Point

Writing and deleting security parameter requires stopping the OPC UA server function before the operation.
For details, refer to the following:
☞ Page 64 Online operations while an OPC UA server is running

Server certificate

In the [Server Certificate] tab of OPC UA Module Configuration Tool, the certificate of an FX5-OPC can be checked and set.



Displayed items

Item		Description
Current Certificate Display	Certificate list	The currently used server certificate is displayed if communication with an FX5-OPC is successful after opening the [Server Certificate] tab or refreshing the display. Buttons other than the [Refresh Display] button and the [Generate a New Self-Signed Certificate] button are enabled after the server certificate is displayed.
	[Refresh Display] button	Click this to reload the server certificate from an FX5-OPC. This button is always enabled even when no server certificate is displayed.
	[Export Certificate] button	Click this button to export the currently displayed server certificate as a DER X.509 certificate format file. This button is enabled only when the server certificate is displayed in the certificate list.
	[Get a CSR] button	Click this to export a new CSR (Certificate Signing Request) for the currently used server certificate in the PEM encoded file format. A CSR is generated by an FX5-OPC. Then, it can be signed by a certificate authority. This button is enabled only when the server certificate is displayed in the certificate list.
Online Operations	[Generate a New Self-Signed Certificate] button	Click this to open the "Generate a New Self-Signed Certificate" screen. Set each item and generate a self-signed certificate in that screen.(☞ Page 72 "Generate a New Self-Signed Certificate" screen) This button is always enabled even when no server certificate is displayed.
	[Delete] button	Click this to delete the sever certificate stored in an FX5-OPC. This button is enabled only when the server certificate is displayed in the certificate list.
	[Replace] button	Click this to replace the server certificate stored in an FX5-OPC with a new one.*1 A self-signed certificate generated by the module can be replaced with a CA-signed certificate. This button is enabled only when the server certificate is displayed in the certificate list.

*1 Only DER-format X.509 certificate files are supported.

Point

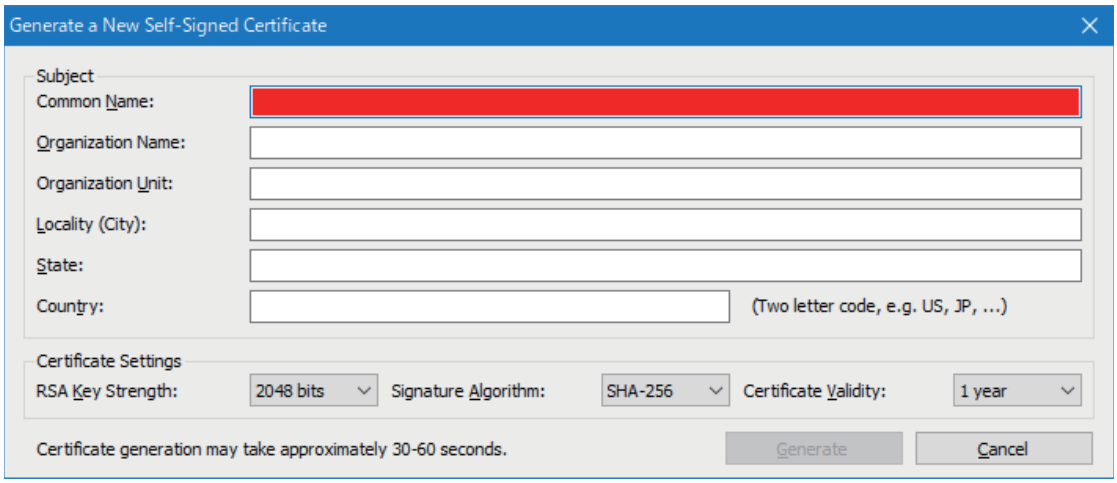
Applying a newly generated server certificate requires stopping the OPC UA server function before the operation.

For details, refer to the following:

☞ Page 64 Online operations while an OPC UA server is running

"Generate a New Self-Signed Certificate" screen

Enter information of a self-signed certificate to be generated in the "Generate a New Self-Signed Certificate" screen.



Displayed items

Item		Description	Setting range
Subject	Common Name	Enter a common name to be written in a certificate.	Up to 64 characters
	Organization Name	Enter an organization name to be written in a certificate.	• Blank • Up to 64 characters
	Organization Unit	Enter an organization unit to be written in a certificate.	• Blank • Up to 64 characters
	Locality (City)	Enter a city name to be written in a certificate.	• Blank • Up to 128 characters
	State	Enter a state name to be written in a certificate.	• Blank • Up to 128 characters
	Country	Enter a country name to be written in a certificate.	• Blank • 2 characters (upper or lower case alphabets)
Certificate Settings	RSA Key Strength	Select the strength of an RSA key.*1, *2	• 1024 bits • 2048 bits • 3072 bits • 4096 bits
	Signature Algorithm	Select a signature algorithm.*1, *2	• SHA-1 • SHA-256
	Certificate Validity	Select the validity period of a certificate.	• 1 day • 1 week • 1 month • 1 year • 2 years • 10 years

*1 "SHA-1" can be selected in "Signature Algorithm" only when "1024 bits" or "2048 bits" is set in "RSA Key Strength."
When setting "3072 bits" or "4096 bits" in "RSA Key Strength," "SHA-256" is automatically set in "Signature Algorithm."

*2 When setting "3072 bits" or "4096 bits" in "RSA Key Strength" and "SHA-1" in "Signature Algorithm," the setting in "RSA Key Strength" is automatically changed to "2048 bits."

Point

The [Generate] button is enabled only after "Common Name" is entered.

Precautions

A certificate cannot be generated depending on the total data length of the "Subject" field (excluding "Country").
The length of an RSA key varies the maximum data length.
The following table shows the maximum data length for the "Subject" field where UTF-8 encoding is used.

RSA key length	Maximum data length
1024 bits	640 bytes
2048 bits	510 bytes
3072 bits	380 bytes
4096 bits	260 bytes

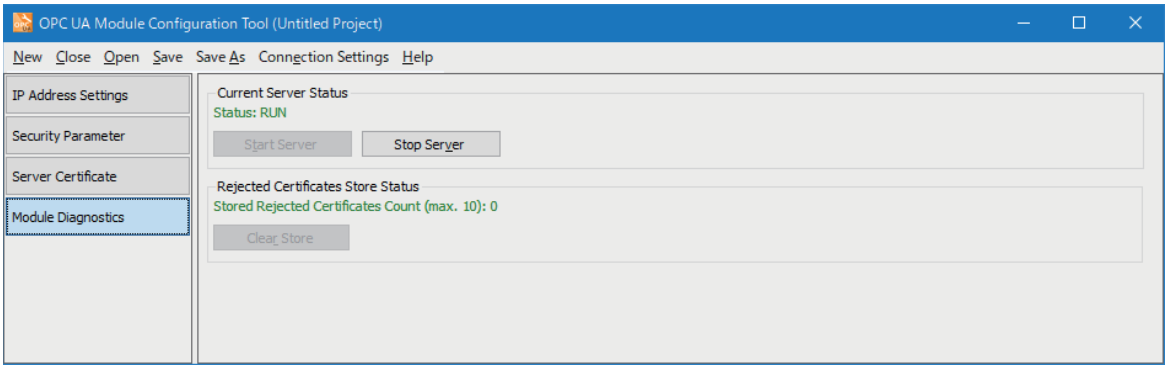
Note that with UTF-8 encoding, ASCII characters occupy one byte while the characters belonging to the Unicode Basic Multilingual Plane (BMP), such as Japanese characters, occupy three bytes.

Module diagnostics

In the [Module Diagnostics] tab of OPC UA Module Configuration Tool, the status of an OPC UA server can be checked and changed.

The displayed server status is updated every five seconds after selecting this tab or starting/stopping a server.

In addition, the number of rejected certificates stored in an FX5-OPC can be checked and they can be deleted in a batch.



Displayed items

Item		Description
Current Server Status	Status	The server status ("RUN", "STOP", or "Unknown") is displayed.
	[Start Server] button	Click this to start a server. This button is enabled while the server is in "STOP" or "Unknown" state.
	[Stop Server] button	Click this to stop a server. This button is enabled while the server is in "RUN" or "Unknown" state.
Rejected Certificates Store Status	Stored Rejected Certificates Count	The number of rejected certificates stored in an FX5-OPC is displayed ('0' to '10' or "Unknown").
	[Clear Store] button	Click this to delete all rejected certificates stored in an FX5-OPC. This button is enabled only when one or more rejected certificates are stored or the number of stored certificates is unknown.

7.4 Enabling Unsecured Connections

Unsecured connections with OPC UA clients are disabled by default.
By changing a module parameter setting in GX Works3 or security parameter setting in OPC UA Module Configuration Tool, an FX5-OPC allows unsecured connections with OPC UA clients.
However, note that it is recommended to always use secure connections in an OPC UA system.

Setting method

Unsecured connections can be enabled with either of the following methods.

- GX Works3: Select "Enable" for "Unsecure Connection" in the security settings of module parameters.(☞ Page 58 Application settings)
- OPC UA Module Configuration Tool: Select the checkbox of "Enable Unsecure Connection" in the [Security Parameter] tab.(☞ Page 67 General settings)

When both parameters are set

When the setting for unsecured connections is configured in both module parameters and security parameters, the one in the security parameters takes priority.
The following table shows the setting status of each of the parameters and whether unsecured connections are actually enabled or disabled.

■Module parameters are not stored in a CPU module:

Security parameter		Unsecured connection
Not stored in an FX5-OPC		Disabled
Stored in an FX5-OPC	Unsecured connections are disabled.	Disabled
	Unsecured connections are enabled.	Enabled

■Unsecured connections are disabled in module parameters:

Security parameter		Unsecured connection
Not stored in an FX5-OPC		Disabled
Stored in an FX5-OPC	Unsecured connections are disabled.	Disabled
	Unsecured connections are enabled.	Enabled

■Unsecured connections are enabled in module parameters:

Security parameter		Unsecured connection
Not stored in an FX5-OPC		Enabled
Stored in an FX5-OPC	Unsecured connections are disabled.	Disabled
	Unsecured connections are enabled.	Enabled

8 TROUBLESHOOTING

This chapter explains errors that may occur when using an FX5-OPC and their troubleshooting methods.

8.1 Checking Errors with LEDs

The module status can be checked with LEDs.

Point

The LED status can be checked remotely by using the diagnostic function.
In addition, when an error is detected, details of the error can be checked with the diagnostic function.
For details on the diagnostic function, refer to the following:
☞ Page 78 Module diagnostics

Module error status

The module status can be checked with the statuses of the RUN LED and ERROR LED.

RUN LED	ERROR LED	Module status*1	Description
OFF	Flashing	Major error	The module cannot operate normally due to a hardware or memory error.
ON	Flashing	Moderate error	The module has stopped operation. If the error cause is removed, the module can operate again.
ON	ON	Minor error	The module is operating though an error has occurred.
ON	OFF	No error	The module is operating normally.

*1 When multiple errors occur, the error status is displayed in the order of major, moderate, and minor.

■When the RUN LED turns OFF

When the RUN LED turns OFF after an FX5-OPC is powered ON, check the following item:

Check item	Corrective action
Is the FX5-OPC attached properly?	Attach the FX5-OPC properly to the CPU module.

If the problem cannot be solved with the above action, perform the hardware test to check if the FX5-OPC has any failure.(☞ Page 81 Hardware Test)

■When the ERROR LED turns ON or is flashing

When the ERROR LED turns ON or is flashing, check the following item:

Check item	Corrective action
Has any error occurred in the module diagnostics?	Take the corrective actions displayed in the module diagnostics.(☞ Page 78 Module diagnostics)

OPC UA server function status

The status of the OPC UA server function can be checked with the statuses of OPERATION LED, SESSION LED, and D ACCESS LED.

OPERATION LED	SESSION LED	D ACCESS LED	OPC UA server function status	Description
OFF	OFF	OFF	Stopped	An OPC UA server is not responding to a client.
ON	OFF	OFF	Running	An OPC UA server is waiting for a client to connect.
ON	ON	OFF	Running	There is an active client session; however, programmable controller data is not accessed through the session.
ON	ON	ON	Running	Programmable controller data is accessed through an active client session.

Point

An FX5-OPC automatically starts the OPC UA server function after the module startup (the OPERATION LED turns ON).
The OPC UA server function may stops (the OPERATION LED turns OFF) when performing an online operation in GX Works3 or OPC UA Module Configuration Tool.
For details on the online operations which turn OFF the OPERATION LED, refer to the following:
☞ Page 64 Online operations

Ethernet connection status

The status of Ethernet connection can be checked with the status of the SD/RD LED, which is next to each Ethernet port.

SD/RD LED	Description
OFF	Data is not being sent or received via Ethernet. Check the connections of the cables and network devices.
ON	Data is being sent or received normally via Ethernet.

■When the SD/RD LED turns OFF (data cannot be sent/received)

When the SD/RD LED turns OFF and data cannot be sent or received, check the following items:

Check item	Corrective action
Is the ERROR LED ON or flashing?	Take the corrective actions displayed in the module diagnostics.(☞ Page 78 Module diagnostics)
Is the Ethernet cable connected properly?	Connect the Ethernet cable again.
Are the parameter settings correct?	Review the settings in GX Works3.

If the problem cannot be solved with the above actions, perform the hardware test to check if the FX5-OPC has any failure.(☞ Page 81 Hardware Test)

8.2 Checking the Module Status

The status of an FX5-OPC can be checked by the following methods:

☞ Page 78 Module diagnostics

☞ Page 80 Checking with the buffer memory

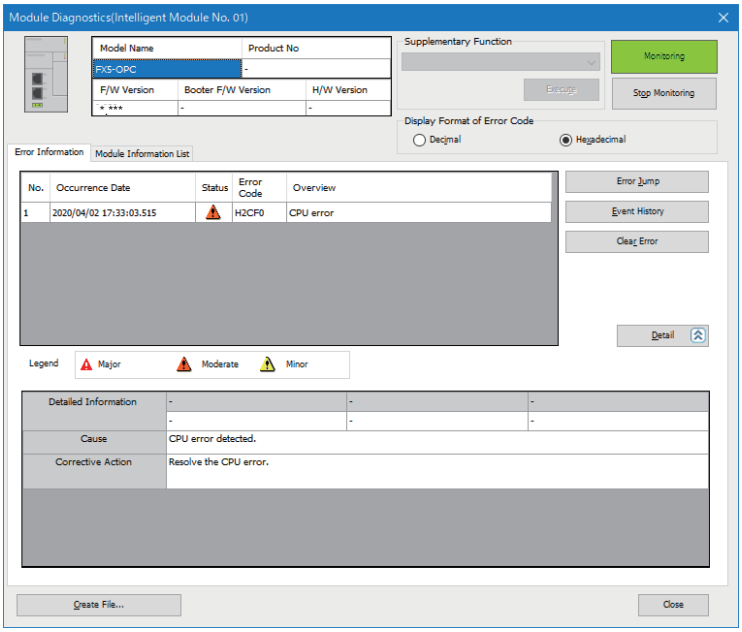
Module diagnostics

Error information and module information of an FX5-OPC can be checked in the "Module Diagnostics" screen of GX Works3. Select an FX5-OPC from the module configuration in the system monitor of GX Works3 and double-click one of the cells in the same column to display the "Module Diagnostics" screen.

Item	Purpose
Error Information	To display the details of errors occurring. Click the [Event History] button to check the history of errors that have occurred in an FX5-OPC and ones detected in each module.
Module Information List	To display the information of each status of an FX5-OPC.

Error Information

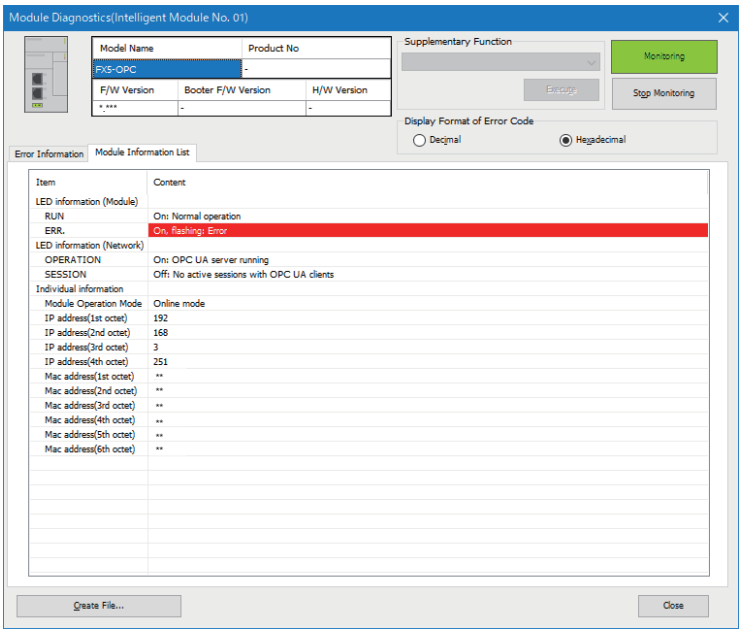
The description of an error occurring and its corrective action can be checked.



Item	Description
Status	Major: An error such as a hardware or memory error. The module stops operating.
	Moderate: An error, such as parameter error, which affects module operation. The module stops operating.
	Minor: An error such as communication failure. The module continues operating.
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.

Module Information List

The information of each status of an FX5-OPC can be checked by switching to the [Module Information List] tab.



Item		Description
LED information (Module)		The statuses of the RUN LED and ERROR LED of an FX5-OPC are displayed.
LED information (Network)*1		The statuses of the OPERATION LED and SESSION LED of an FX5-OPC are displayed.
Individual information*1	Module Operation Mode	The mode (online or hardware test mode) of an FX5-OPC is displayed.
	IP address (1st octet)	The IP address of an FX5-OPC is displayed.
	IP address (2nd octet)	
	IP address (3rd octet)	
	IP address (4th octet)	
	MAC address (1st octet)	The MAC address of an FX5-OPC is displayed.
	MAC address (2nd octet)	
	MAC address (3rd octet)	
	MAC address (4th octet)	
	MAC address (5th octet)	
	MAC address (6th octet)	

*1 An undefined value is stored during the hardware test.

Checking with the buffer memory

Errors that have occurred in an FX5-OPC can be checked in the following buffer memory addresses:

Buffer memory address	Buffer memory name	Description	Reference
Un\G29	Latest error code	The latest error code is stored.	Page 93 Latest error code (Un\G29)
Un\G34.F	Module error status	An error flag is stored.	Page 94 Input signals (Un\G34)
Un\G0	Server status	The status of an OPC UA server is stored.	Page 92 Server status (Un\G0)
Un\G2	Session status	The status of OPC UA client sessions is stored.	Page 92 Session status (Un\G2)
Un\G3	Security status	The status of security parameters is stored.	Page 93 Security status (Un\G3)

8.3 Hardware Test

The hardware test diagnoses hardware such as the ROM or RAM of an FX5-OPC.
This section explains the procedure to perform the hardware test and the operations required after the test.

Restriction

- Values in the buffer memory cannot be accessed in GX Works3 or a program during the hardware test.
- Do not change the operating status of a CPU module during the hardware test. If its operating status is changed, an major error occurs in the CPU module.

Procedure to perform the hardware test

Operating procedure

1. Set the operation mode of an FX5-OPC to "Hardware test" in GX Works3.

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [FX5-OPC] ⇨ [Module Parameter] ⇨ [Required Settings] ⇨ [Mode Settings] ⇨ [Operation Mode]

2. Disconnect a cable if it is connected to an Ethernet port of the FX5-OPC.
3. Set the CPU module to the STOP state, and write the parameters.
4. Turn the power of the CPU module OFF and ON, or reset the CPU module.
   The hardware test is automatically performed.
5. Check the hardware test result with the following LEDs:

RUN LED	ERROR LED	Status
Flashing	OFF	The hardware test is in process.
ON	OFF	The hardware test is completed normally.
ON	ON	The hardware test is completed with an error.

Operations when the hardware test is completed normally

Operating procedure

1. Set the operation mode of the FX5-OPC to "Online" in GX Works3.

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [FX5-OPC] ⇨ [Module Parameter] ⇨ [Required Settings] ⇨ [Mode Settings] ⇨ [Operation Mode]

2. Write the parameters, then turn the power of the CPU module OFF and ON or reset the CPU module.

Operations when the hardware test is completed with an error

Operating procedure

1. Check that adequate measures to reduce noise are taken for the programmable controller system and retry the hardware test.
2. If the test is completed with an error again, a hardware component of the FX5-OPC may have a failure. Please consult your local Mitsubishi representative.

8.4 Troubleshooting by Symptom

This section shows troubleshooting methods for issues other than FX5-OPC errors.

For errors occurring in an FX5-OPC, identify their causes by using LEDs or the diagnostic function of GX Works3. (☞ Page 76 Checking Errors with LEDs, Page 78 Module diagnostics)

Symptom	Check item	Corrective action
The module READY signal (buffer memory address: Un\G34.0) does not turn ON even if the power is ON.	Is the module initializing?	Wait for the module to initialize. It may take several seconds for the module READY signal (buffer memory address: Un\G34.0) to turn ON depending on the settings for the module.
Unable to connect to an FX5-OPC from an OPC UA client.	Is there any other device with the same IP address on the same network?	Review all the IP address settings on the network to avoid duplication.
	Is the OPC UA server function stopped?	The OPC UA server function may be stopped due to changes in settings for an FX5-OPC. In that case, reset a CPU module and wait for the FX5-OPC initialization to complete.
	Is the OPC UA client operating normally?	Troubleshoot the OPC UA client.
	Is the security (trusted certificates, for example) configured properly in the FX5-OPC and the OPC UA client?	Review the security configuration in the FX5-OPC and in the OPC UA client.
	Is the server certificate expired?	Generate a new server certificate. Before generating a new server certificate, check that the clock of the CPU module is set to the current time.
A variable value read by an OPC UA client does not change as expected.	Has an error occurred in the CPU module?	If an error has occurred in the CPU module, check the error details and take an appropriate corrective action.
A variable value written by an OPC UA client is not applied properly to a CPU module.	Is the value overwritten by a program, engineering tool such as GX Works3, or another OPC UA client?	Do not write data to a same memory area from multiple sources such as a program, engineering tool (GX Works3, for example), or another OPC UA client.
	Has an error occurred in the CPU module?	If an error has occurred in the CPU module, check the error details and take an appropriate corrective action.

8.5 Error Code List

When an FX5-OPC detects an error during its operation, the module stores the error code in 'latest error code' (Un\G29) of the buffer memory.

The error details and cause can be identified by checking the error code.

An error code can be checked by either of the following methods:

- Module diagnostics of GX Works3 (☞ Page 78 Module diagnostics)
- 'Latest error code' (Un\G29) in the buffer memory (☞ Page 93 Latest error code (Un\G29))

Error code list

The following table lists details of errors which can occur in an FX5-OPC:

Error code	Error name	Error description	Corrective action
1080H	Flash ROM write count error	Exceeded the maximum number of write operations allowed for the external flash ROM.	Correct operation of the module cannot be guaranteed. Replace the module with a new one.
1810H	Failed to write IP address	Failed to write IP address to flash memory.	Try again to write the IP address with OPC UA Configurator. If the error occurs again, contact your local Mitsubishi representative.
1900H	Hardware error	Flash ROM memory test has failed during initialization.	Reset FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
1D00H	Parameter error	General parameter error.	Write parameters to the module again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.
1D02H	Parameter error	Address space parameter error.	Write Address Space Parameters from GX Works3 to the module again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.
1D03H	Parameter error	Address space parameter error.	A possible reason for this error is, that Address Space representation in memory exceeded the maximum size. Even if the Address Space Size displayed by GX Works3 appeared in range, this could happen when all of the following cases are met: close to maximum value, publishing user-defined structured data types to the Address Space, and setting "Expose structure members as components". Try reducing the Address Space Size by GX Works3 until the error stops occurring, and write Address Space Parameters from GX Works3 to the module again and reset the PLC. If the error still occurs, contact your local Mitsubishi representative.
1D05H to 1D06H	Parameter error	Security parameter error.	Write Security Parameters from OPC UA Configurator to the module again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.
1D07H to 1D08H	Parameter error	Extended Parameter file handling error.	Write parameters to the module again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.
1E00H	CPU data access error	General error of the CPU data access task.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
1E01H	CPU data access error	Failed to read/write data from CPU due to the internal timeout.	Check if the error also happens when the CPU is in STOP mode. It no, try to decrease the scan time of the PLC program. If yes, confirm the status of the FX5-CPU. If the error occurs again although there are no errors in the CPU, contact your local Mitsubishi representative.
1E02H	CPU data access error	Failed to read/write data from CPU.	Write parameters to the module again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.

Error code	Error name	Error description	Corrective action
1E03H	CPU data access error	Failed to read/write data from CPU due to the internal timeout.	Check if the error also happens when the CPU is in STOP mode. It no, try to decrease the scan time of the PLC program. If yes, confirm the status of the FX5-CPU. If the error occurs again although there are no errors in the CPU, contact your local Mitsubishi representative.
1E04H	CPU data access error	Failed to read/write data from CPU.	Write parameters to the module again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.
1E05H	OPC UA subscription processing overloaded	FX5-OPC is overloaded and cannot process subscriptions in timely manner.	Increase the Max. Age setting for variables in the address space. Decrease the number of sessions, subscriptions or monitored items created by all clients. Decrease the scan time of the PLC program.
1E06H	Data access processing overloaded	Accessing a single variable data in the PLC takes excessive amount of time.	Decrease the scan time of the PLC program. Avoid using array data types with big number of elements.
1E07H	TCP listener timeout	The TCP session has timed-out due to 60s inactivity.	Make sure that the OPC UA client sends a request to FX5-OPC in intervals shorter than 60s.
1E08H	TCP connection closed due to error	An invalid or unexpected request was made by an OPC UA client or there was a failure in processing a request by FX5-OPC.	• Use certified OPC UA clients. • In case the load on FX5-OPC is high e.g. CPU scan time is high, number of monitored items is high etc., try to reduce the load. • Configure the OPC UA client to reduce the amount of data sent by the server at one time. (e.g., reduce the maximum number of notifications sent in a single Publish, reduce subscriptions, reduce monitor items, etc.) • Make sure the network condition is stable i.e. there are no frequent connections/disconnections. • Detailed information of this error contains a standard OPC UA status code, which gives a hint about the cause of the error.
1F00H	OPC UA server error	General error of the OPC UA server task.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
2160H	IP address conflict detected	IP address conflict detected.	Set the IP address, which is unique in the local network.
2C80H to 2C82H	Parameter error	Processing Module Parameter file failed.	Write the Module Parameter from GX Works3 to CPU again and reset the PLC. If the error occurs again, contact your local Mitsubishi representative.
2CF0H	CPU error	CPU error detected.	Resolve the CPU error.
3040H	Update error	Firmware update file version error	For this update, a PLC applicable to the new version is required. Please consult your local Mitsubishi representative.
3041H	Update error	Failed to verify the integrity of the firmware update file.	Replace the update file in the SD memory card with the correct file, and perform update again.
3042H	Update error	Failed to acquire the firmware update file.	Replace the update file in the SD memory card with the correct file, and perform update again.
306EH	Parameter error	Invalid IP address set in GX Works3.	In GX Works3, set the IP address in a range which is supported by FX5-OPC.
306FH	Parameter error	Invalid subnet mask set in GX Works3.	In GX Works3, set the subnet mask in a range which is supported by FX5-OPC.
3073H	Parameter error	Invalid gateway address set in GX Works3.	In GX Works3, set the default gateway in a range which is supported by FX5-OPC.
3095H to 309CH	Parameter error	IP Filter Settings invalid.	Rewrite the Module Parameter file in the CPU and restart the system. If the error occurs again, contact your local Mitsubishi representative.
30A1H	Parameter error	Module Parameter file invalid.	Rewrite the Module Parameter file in the CPU and restart the system. If the error occurs again, contact your local Mitsubishi representative.
3C00H	Hardware error	WDT interrupt.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E00H	Hardware error	Failed to initialize the TCP/IP stack.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.

Error code	Error name	Error description	Corrective action
3E01H	Hardware error	Failed to initialize the OPC UA toolkit.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E02H	Hardware error	Failed to start the OPC UA server.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E03H	Hardware error	Failed to stop the OPC UA server.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E04H	Hardware error	An internal error occurred.	As the error may be caused by the module overload, try to reduce the load on the module by decreasing the frequency of incoming requests from all clients.
3E30H to 3E43H	Hardware error	Hardware error detected.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E50H	Hardware error	RAM check error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E51H	Hardware error	Sum check code error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E52H	Hardware error	Flash memory test access error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E53H	Hardware error	Flash memory test verification error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E54H	Hardware error	Buffer memory access error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E55H	Hardware error	BusAsic register read error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3E56H	Hardware error	Factory test mode error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3FA1H	Hardware error	Hardware error.	Restart FX5-OPC. If the error occurs again, contact your local Mitsubishi representative.
3FA2H	Flash ROM write count error	Exceeded the maximum number of write operations allowed for the on-chip flash ROM.	Correct operation of the module cannot be guaranteed. Replace the module with a new one.

8.6 Event List

Information of errors and events which an FX5-OPC detects is saved in a CPU built-in memory or SD memory card.
When an event occurs, its event code and details can be checked in the screen opened by the following operation:

- Clicking the [Event History] button in the "Module Diagnostics" screen of GX Works3 (☞ Page 78 Module diagnostics)

Event list

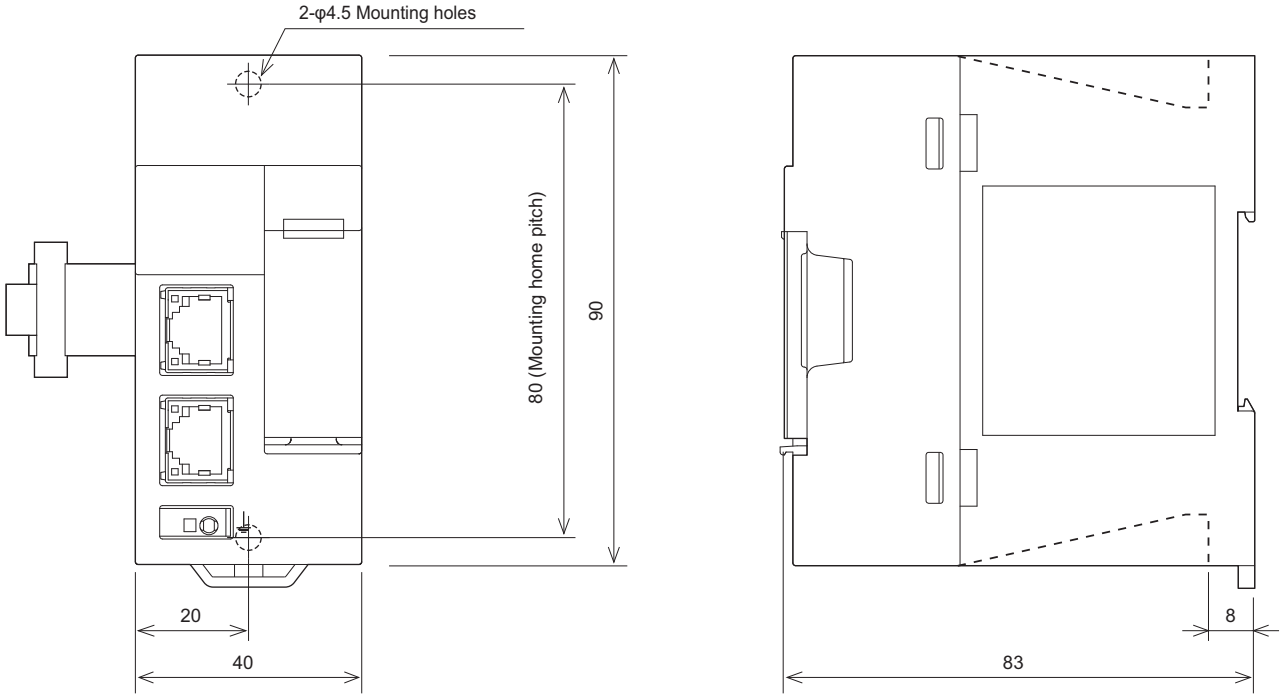
The following table lists details of events which can occur in an FX5-OPC:

Event code	Event type	Event category	Detected event	Description
0801H	System	Warning	Parameter file	Address space configuration stored.
0802H	System	Warning	Parameter file	Address space configuration deleted.
0803H	System	Warning	Parameter file	Security configuration stored.
0804H	System	Warning	Parameter file	Security configuration deleted.
0805H	System	Warning	Server certificate	Server certificate and private key generated.
0806H	System	Warning	Server certificate	Server certificate replaced.
0807H	System	Warning	Server certificate	Server certificate and private key deleted.
0808H	System	Warning	IP address	IP address configuration stored.
0809H	System	Warning	IP address	IP address configuration deleted.
080AH	System	Warning	OPC UA server	OPC UA server started.
080BH	System	Warning	OPC UA server	OPC UA server stopped.
080CH	System	Warning	OPC UA server	Session created.
080EH	System	Warning	OPC UA server	Session closed.
0810H	System	Warning	IP filter	Denied connection based on the IP filter rules.
0820H	System	Warning	Clock time change	PLC clock time has been changed backwards by more than 10ms while OPC UA server was running.
0900H	System	Warning	OPC UA server	Client certificate rejected.
0901H	System	Warning	OPC UA server	User validation failed.
0902H	System	Warning	Server certificate	More than 80% of the certificate's lifetime has already passed.
0903H	System	Warning	Rejected certificates	Rejected certificates storage became full.
1080H to 3FFFH	System	Error	When an error occurs, the error information is stored as an event.	

APPENDIX

Appendix 1 External Dimensions

The following figure shows the external dimensions of an FX5-OPC.



(Unit: mm)

- MASS (Weight): approx. 0.2 kg

A

Appendix 2 Standards

Certification of UL, cUL standards

An FX5-OPC supports UL (UL, cUL) standards.
For the models that support UL standards, refer to the following file number.
UL, cUL file number: E95239

Compliance with EC directive (CE marking)

This product complies with EC directive, however, this document does not guarantee that a mechanical system including this product will comply with EC directive.
Compliance to EMC directive and the low voltage directive (LVD) of the entire mechanical module should be checked by the manufacturer. For more details, please contact your local Mitsubishi Electric sales office.

Requirement for compliance with EMC directive

The following products have shown compliance through direct testing (of the identified standards below) and design analysis (through the creation of a technical construction file) to the European Directive for Electromagnetic Compatibility (2014/30/EU) when used as directed by the appropriate documentation.

Considerations

This product is designed for use in industrial applications.

Product compatibility

Type: Programmable controller (open type equipment)
Models: FX5 manufactured after the following date

from July 1st, 2021	FX5-OPC

Electromagnetic compatibility (EMC) directive	Remarks
EN61131-2:2007 programmable controllers - Equipment requirements and tests	Compliance with all relevant aspects of the standard. EMI • Radiated emission • Conducted emission EMS • Radiated electromagnetic field • Fast transient burst • Electrostatic discharge • High-energy surge • Voltage drops and interruptions • Conducted RF • Power frequency magnetic field

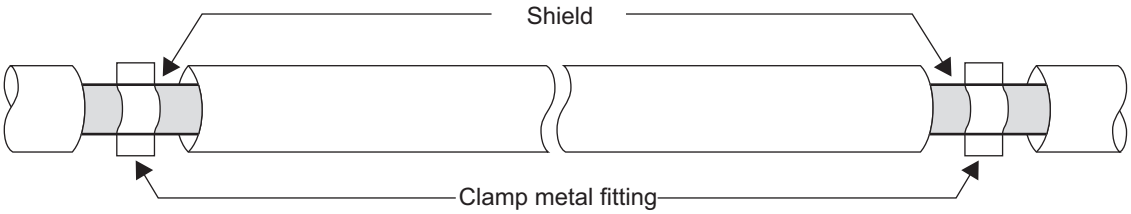
Caution for compliance with EC directive

Caution for when an FX5-OPC is used

When an FX5-OPC is used, attach a ferrite core to the power supplies of the CPU module. Make 2 turns around the ferrite core and attach within approximately 200 mm from the terminal block and connectors of the power cable. (Ferrite core used in Mitsubishi Electric's test: E04SR401938 manufactured by SEIWA ELECTRIC MFG. CO., LTD.)

Caution for when the Ethernet port is used

Use a shielded twisted pair cable for the 10BASE-T or 100BASE-TX cable.
Strip a part of the jacket of the shielded twisted pair cable as shown below and ground as much of the exposed shield as possible to both sides of the cable.



A

Appendix 3 Module Labels

The buffer memory of an FX5-OPC can be set using module labels.

Structure of a module label

The module label name is defined with the following structure.

- "Instance name"_"data format""label name"_D

■Instance name

The following is the instance name of an FX5-OPC.

Model	Instance name
FX5-OPC	FX5OPC

Ex.

FX5OPC_uServerStatus_D

■Data format

The data format indicates the size of a buffer memory area. The following shows the classification.

Data format	Description
b	Bit
u	Word [Unsigned]/Bit String [16-bit]
ud	Double word [Unsigned]/Bit String [32-bit]
un	Word of multiple buffer memories [Unsigned]/Bit String [16-bit]

■Label name

A label name unique to the module.

■_D

This symbol indicates that the module label is for direct access. Value update timing is shown below.

Type	Description	Access timing
Direct access	The values read/written from/to the module labels are reflected to the module immediately.	At writing to or reading from the module label

Appendix 4 Buffer Memory

The buffer memory is used to exchange data between an FX5-OPC and a CPU module.
Buffer memory values are set to their defaults (initial values) when the system is powered off or the CPU module is reset.

Buffer memory list

The following lists the buffer memory of an FX5-OPC.

Buffer memory address		Name	Initial value	Read/Write	Reference
Decimal	Hexadecimal				
0	0H	Server status	0	Read	Page 92 Server status (Un\G0)
2	2H	Session status	0	Read	Page 92 Session status (Un\G2)
3	3H	Security status	0	Read	Page 93 Security status (Un\G3)
4	4H	Rejected certificates count	0	Read	Page 93 Rejected certificates count (Un\G4)
29	1DH	Latest error code	0	Read	Page 93 Latest error code (Un\G29)
30	1EH	Module information	69C2H	Read	Page 93 Module information (Un\G30)
31	1FH	Firmware version	*1	Read	Page 93 Firmware version (Un\G31)
34	22H	Input signals	0	Read	Page 94 Input signals (Un\G34)
36	24H	Output signals	0	Read/Write	Page 94 Output signals (Un\G36)
63	3FH	IP address source	0	Read	Page 94 IP address source (Un\G63)
64 to 65	40H to 41H	IP address	192.168.3.251	Read	Page 94 IP address (Un\G64 to Un\G65)
74 to 75	4AH to 4BH	Subnet mask	255.255.255.0	Read	Page 95 Subnet mask (Un\G74 to Un\G75)
76 to 77	4CH to 4DH	Default gateway	0.0.0.0	Read	Page 95 Default gateway (Un\G76 to Un\G77)
102 to 104	66H to 68H	MAC address	MAC address written before shipment	Read	Page 95 Ethernet address (MAC address) (Un\G102 to Un\G104)
200 to 283	C8H to 11BH	Session details	0	Read	Page 96 Session details (Un\G200 to Un\G283)

*1 The firmware version of the FX5-OPC is stored. For Ver. 1.000, 1000 is stored.

A

Buffer memory details

The following shows the details on the buffer memory of an FX5-OPC.

Server status (Un\G0)

The status of an OPC UA server is stored.

Value	Description
0 or 2	Stopped
1	Running

Session status (Un\G2)

The status of OPC UA client sessions is stored.

Address	Bit	Value	Description
Un\G2	b0 to b2	0	Initial value
		1	First session free, available to create a new session
		2	First session created, but not activated yet
		4	First session active
	b3 to b5	0	Initial value
		1	Second session free, available to create a new session
		2	Second session created, but not activated yet
		4	Second session active
	b6 to b8	0	Initial value
		1	Third session free, available to create a new session
		2	Third session created, but not activated yet
		4	Third session active
	b9 to b11	0	Initial value
		1	Fourth session free, available to create a new session
		2	Fourth session created, but not activated yet
		4	Fourth session active

Security status (Un\G3)

The status of security parameters is stored.

Address	Bit	Name	Value	Description	Initial value	Read/Write
Un\G3	b0	Security parameter storage status	0	A valid security parameter file is not stored in the flash ROM of an FX5-OPC.	0	Read
			1	A valid security parameter file is stored in the flash ROM of an FX5-OPC.		
	b1	Unsecured connection status	0	Unsecured connections are disabled. (☞ Page 75 Enabling Unsecured Connections)		
			1	Unsecured connections are enabled. (☞ Page 75 Enabling Unsecured Connections)		
	b2	User defined status	0	No user is created in "User Management" in the [Security Parameter] tab of OPC UA Module Configuration Tool.		
			1	A user is created in "User Management" in the [Security Parameter] tab of OPC UA Module Configuration Tool.		
	b3	"Sign" mode setting status	0	The checkbox of "Sign" is not selected in the [Security Parameter] tab of OPC UA Module Configuration Tool.		
			1	The checkbox of "Sign" is selected in the [Security Parameter] tab of OPC UA Module Configuration Tool.		

Rejected certificates count (Un\G4)

The number of rejected certificates stored in an FX5-OPC is stored.

Value	Description
0 to 9	Zero to nine certificates are stored. When a new untrusted OPC UA client is connected, its certificate is stored in the rejected certificate list.
10	10 certificates are stored. The certificates stored in the rejected certificate list has reached the maximum number. Even if a new untrusted OPC UA client is connected, its certificate will not be stored in the list. To store a new certificate, click the [Clear Store] button in the [Module Diagnostics] tab. Alternatively, reset a CPU module. (☞ Page 74 Module diagnostics)

Latest error code (Un\G29)

The latest error code occurred in an FX5-OPC is stored. ('0' is stored when the module operates normally.)

For details on error codes, refer to the following:

☞ Page 83 Error Code List

Point

Information of 'latest error code' (Un\G29) is not cleared even if the problem occurred in an FX5-OPC has been solved.

To clear the information, turn ON 'module error clear request' (bit 15) of 'output signals' (Un\G36). (☞ Page 94 Output signals (Un\G36))

Module information (Un\G30)

Module information (69C2H) of an FX5-OPC is stored.

Firmware version (Un\G31)

The firmware version of an FX5-OPC is stored.

Ex.

When the firmware version is 1.000: K1000

Input signals (Un\G34)

The communication status of an FX5-OPC can be checked with these signals.

Address	bit	Signal name	Description
Un\G34	b0	Module READY	A signal for checking whether the FX5-OPC is ready to start its operation. • ON: The module is operable. (Initialization is completed.) • OFF: The module is not operable. (Initialization is not yet completed or it failed.)
	b15	Module error status	A signal for checking whether an error has occurred in the FX5-OPC. • ON: An error has occurred. • OFF: No error When an error occurs, the error code is stored in 'latest error code' (Un\G29). (☞ Page 93 Latest error code (Un\G29))

Output signals (Un\G36)

An FX5-OPC can be controlled with these signals.

Address	bit	Signal name	Description
Un\G36	b15	Module error clear request	A signal for requesting to clear an error occurred in the FX5-OPC. To request to clear an error, turn this signal from OFF to ON, then back to OFF again. By issuing this request after removing the error cause, each buffer memory and LED status will be changed as follows. • 'Module error status' (Un\G34.b15): ON to OFF • ERROR LED: ON/flashing to OFF • 'Latest error code' (Un\G29): cleared

IP address source (Un\G63)

The status of the source of IP address, subnet mask, and default gateway set in GX Works3 or OPC UA Module Configuration Tool is stored.

Value	Description
0	An IP address is not assigned due to an error.
1	The default IP address is used.
2	The IP address set in the module parameters of GX Works3 is used.
3	The IP address set for flash ROM in OPC UA Module Configuration Tool is used.

IP address (Un\G64 to Un\G65)

The IP address of the own station set in GX Works3 or OPC UA Module Configuration Tool is stored.

Address	Description
Un\G64	Third octet, fourth octet
Un\G65	First octet, second octet

Ex.

When the IP address is 192.168.3.251: Un\G64 = 03FBH, Un\G65 = C0A8H

	3.	251		
Un\G64	03	FB	H	
	192.	168.		
Un\G65	C0	A8	H	

Subnet mask (Un\G74 to Un\G75)

The subnet mask of the own station set in GX Works3 or OPC UA Module Configuration Tool is stored.

Address	Description
Un\G74	Third octet, fourth octet
Un\G75	First octet, second octet

Ex.

When the subnet mask is 255.255.255.0: Un\G74 = FF00H, Un\G75 = FFFFH

	255.	0	
Un\G74	FF	00	H

	255.	255.	
Un\G75	FF	FF	H

Default gateway (Un\G76 to Un\G77)

The default gateway of the own station set in GX Works3 or OPC UA Module Configuration Tool is stored.

Address	Description
Un\G76	Third octet, fourth octet
Un\G77	First octet, second octet

Ex.

When the default gateway IP address is 192.168.3.254: Un\G76 = 03FEH, Un\G77 = C0A8H

	3.	254	
Un\G76	03	FE	H

	192.	168.	
Un\G77	C0	A8	H

Ethernet address (MAC address) (Un\G102 to Un\G104)

The MAC address of the own station is stored.

Address	Description
Un\G102	Serial ID
Un\G103	Lower one digit of vendor ID, model ID
Un\G104	Upper two digits of vendor ID

Ex.

When the MAC address is 2B-F8-60-71-4B-10: Un\G102 = 4B10H, Un\G103 = 6071H, Un\G104 = 2BF8H

	4B	10	
Un\G102	4B	10	H

	60	71	
Un\G103	60	71	H

	2B	F8	
Un\G104	2B	F8	H

A

Session details (Un\G200 to Un\G283)

Detailed information on available sessions is stored.

Up to four sessions are available.

Address	Session	Name	Description
Un\G200	First session	Session status	Information on the session status is stored.
Un\G201 to Un\G202		Session ID	The unique ID of the session is stored.
Un\G203 to Un\G204		IP address	The IP address of the connected OPC UA client is stored.
Un\G205 to Un\G220		Reserved	—
Un\G221	Second session	Session status	Information on the session status is stored.
Un\G222 to Un\G223		Session ID	The unique ID of the session is stored.
Un\G224 to Un\G225		IP address	The IP address of the connected OPC UA client is stored.
Un\G226 to Un\G241		Reserved	—
Un\G242	Third session	Session status	Information on the session status is stored.
Un\G243 to Un\G244		Session ID	The unique ID of the session is stored.
Un\G245 to Un\G246		IP address	The IP address of the connected OPC UA client is stored.
Un\G247 to Un\G262		Reserved	—
Un\G263	Fourth session	Session status	Information on the session status is stored.
Un\G264 to Un\G265		Session ID	The unique ID of the session is stored.
Un\G266 to Un\G267		IP address	The IP address of the connected OPC UA client is stored.
Un\G268 to Un\G283		Reserved	—

Ex.

The following shows an example of handling the first session. The operations will be the same for other sessions if their addresses are the same. For handling the second and later sessions, refer to the items with the same name as those of the first session.

■Session status (Un\G200)

The status of the first session is stored.

Value	Description
0	Session not ready yet
1	Session ready to be created
2	Session created, but not activated yet
4	Session active

■Session ID (Un\G201 to Un\G202)

The unique 4-byte ID of the first session is stored.

■IP address (Un\G203 to Un\G204)

The IP address of the OPC UA client that recently used the first session is stored.

Address	Description
Un\G203	Third octet, fourth octet
Un\G204	First octet, second octet

Ex.

When the IP address is 192.168.3.150: Un\G203 = 0396H, Un\G204 = C0A8H

	3.	150	
Un\G203	03	96	H
	192.	168.	
Un\G204	C0	A8	H

Appendix 5 Performance Considerations

This section describes the performance considerations for the OPC UA server function of an FX5-OPC and measurement results of the server processing time.

Address space size

The number of variables in an address space is limited by the memory capacity of an FX5-OPC.

For details on the factors which affect the size of an address space, refer to the following:

☞ Page 21 Considerations

Polling performance

The address space size is not equal to the number of variables that can be accessed cyclically with a defined interval.

Methods to access a variable value in OPC UA communication are as follows:

Method	Description
Using the following two services:*1 • Read • Write	By using these services in a client server system, an OPC UA client can access a variable value. Time required for an FX5-OPC to send a response depends on the number of variables included in the request and on the number of parallel requests from other clients.
Using the following two service sets:*1 • MonitoredItem • Subscription	This access method is commonly used by OPC UA clients. By using these service sets, a client selects variables and asks an OPC UA server to monitor the variables at a requested sampling interval*2. The server sends a notification to the client only when any of the monitored items changed its value. If the load on the server is high, variables may not be able to keep the requested interval. In that case, the Good_Overload status code*3 is returned to the client.

*1 For details on each service/service set, refer to the following:
☞ Page 17 Supported services

*2 Must be bigger than the minimum sampling interval of an OPC UA server, which is defined in the performance specifications. (☞ Page 15 Performance Specifications)

*3 For details on the Good_Overload status code, refer to the OPC UA standards.

■Sampling rate

The sampling rate that an FX5-OPC can actually achieve depends on the following factors:

No.	Item	Remarks
1	Number of active sessions, subscriptions, and monitored items created by all connected clients	—
2	Number of variables accessed through all channels	—
3	Data type of a monitored variable	A long array or complex structure requires more time to obtain its value than integer type data.
4	Load on a CPU module	The polling speed slows down when a scan time is long or another application such as GX Works3 is accessing a CPU module at the same time.
5	Layout of variables in the memory of a CPU module	An FX5-OPC optimizes fetching of variable values by reading memory blocks. Assigning GX Works3 labels to adjacent device addresses improves the overall performance. Note that automatically assigned devices are always assigned to consecutive addresses.

By enabling caching of variable values which are read from a CPU module, an FX5-OPC can skip the reading process when the same value or another value from the same memory block is requested within a short time.

This results in the improvement of overall polling performance and the avoidance of server overload.

Period for which a value in the cache is held can be set in "Max Age [ms]" in address space parameters of GX Works3.

(☞ Page 60 Address space parameters)

"Max Age [ms]" can be set for each variable; therefore, a smaller value can be specified for variables that change fast, and a bigger value for ones that change slowly.

Connection time

An OPC UA communication protocol is used to establish a session between an OPC UA client and OPC UA server.
Time required to establish a session with FX5-OPC depends on the security policy of an endpoint and the length of RSA keys of both a client and a server.
When connecting an endpoint whose security policy and message security policy are None, the key length does not affect speed.
In other cases, however, the key length significantly affects performance.

■Measurement example

The following shows measurement results when connecting to an OPC UA server from an OPC UA client the key length of which was 2048 bits.

OPC UA server key length	Approximate client connection time
1024 bits	1 second
2048 bits	3 seconds
3072 bits	8 seconds
4096 bits	12 seconds

Precautions

An FX5-OPC will be temporarily unresponsive to clients already connected while establishing a session with a newly connecting client.
To realize stable operations, ensure that session timeouts are set long enough in all clients.

Server certificate generation time

Time required for FX5-OPC to generate a server certificate depends mainly on the following two factors:

No.	Item	Remarks
1	Key length selected in OPC UA Module Configuration Tool	The larger a key length (bits) is, the longer it takes to generate a certificate.
2	Load on an FX5-OPC responding to OPC UA clients	Monitoring hundreds of variables through OPC UA subscriptions with small sampling rates (less than one second) results in the high load on an FX5-OPC; therefore, it takes longer to generate a certificate. For a certificate with a 4096 bit key, the generation may take approximately 12 hours. To minimize the certificate generation time, it is recommended to stop the OPC UA server function before starting the generation.

Note that due to characteristics of the RSA key generation algorithm, the generation time is not deterministic even when generating a certificate when the OPC UA server function is stopped.

■Measurement example

The following shows measurement results when generating a certificate with an FX5-OPC which was not connected to any clients.

Selected key length	Approximate certificate generation time
1024 bits	5 to 10 seconds
2048 bits	30 to 60 seconds
3072 bits	1 to 3 minutes
4096 bits	5 to 15 minutes

Appendix 6 Software Licenses and Copyrights

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

OpenSSL 1.1.1

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 double 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 (c) 1998-2019 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 (C) 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 aheared 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 rouines 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 licence 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 licence [including the GNU Public Licence.]

OPC UA Toolkit

This product includes code that was developed by Softing Industrial Automation GmbH (https://industrial.softing.com) for the The Softing uaToolkit Embedded.
Copyright© Softing Industrial Automation GmbH 2019.
The Softing uaToolkit Embedded uses the following 3rd party libraries:

■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.
The ANSI C Stack is used under the RCL license. The RCL license agreement can be found at https://opcfoundation.org/license/rcl.html.
The platform layers of the ANSI C Stack are used under the MIT license. This license agreement can be found at https://opcfoundation.org/license/mit.html.

■MemPool (https://github.com/SoftingIndustrial/MemPool)
Copyright (C) 2017 Bernd Edlinger
Released under the eCos license.
The eCos license version 2.0
The eCos license is a modified version of the well known GNU General Public License (GPL).
The eCos license is officially recognised as a GPL-compatible Free Software License and is
an OSI-approved Open Source License. An exception clause has been added which limits the
circumstances in which the license applies to other code. The exception clause is as follows:

As a special exception, if other files instantiate templates or use macros or inline
functions from this file, or you compile this file and link it with other works to produce
a work based on this file, this file does not by itself cause the resulting work to be
covered by the GNU General Public License. However the source code for this file must
still be made available in accordance with section (6) of the GNU General Public License v3.

This exception does not invalidate any other reasons why a work based on this file might
be covered by the GNU General Public License.

See here for details: http://ecos.sourceware.org/license-overview.html

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

■__VA_ARGS__ helpers (http://stackoverflow.com/questions/5588855/standard-alternative-to-gccs-va-args-trick)
Copyright (C) 2012 Richard Hansen
Released under the cc by-sa. The license agreement can be found at https://creativecommons.org/licenses/by-sa/3.0/

MD5 Message-Digest Algorithm

This product includes code that was developed by RSA Data Security, Inc.
Copyright (C) 1991-2, RSA Data Security, Inc.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

OPC UA Module Configuration Tool

OPC UA Module Configuration Tool uses the following 3rd party libraries:

■Bouncy Castle (https://www.bouncycastle.org)
Copyright (c) 2000 - 2019 The Legion of the Bouncy Castle Inc. (https://www.bouncycastle.org)
Released under the MIT license
http://opensource.org/licenses/mit-license.php

■IPAddressControlLib (https://github.com/m66n/ipaddresscontrollib)
Copyright (c) 2016 Michael Chapman
Released under the MIT license
http://opensource.org/licenses/mit-license.php

MEMO

INDEX

MEMO

REVISIONS

Revision date	Revision	Description
July 2021	A	First Edition
December 2021	B	■Added or modified parts Section 2.3, Section 4.2
June 2022	C	■Added or modified parts RELEVANT MANUALS, Section 2.1, Chapter 3
March 2023	D	■Added or modified parts Section 2.3, Appendix 2
September 2023	E	■Added or modified parts Section 4.2, Section 8.5, Appendix 6
November 2023	F	■Added or modified parts Manual name (old manual name 'MELSEC iQ-F FX5 User's Manual (OPC UA)') RELEVANT MANUALS, Section 4.1, Section 8.5
March 2024	G	■Added or modified parts Chapter 3, Section 4.2, Section 8.5, Appendix 5

Japanese manual number: SH-082249-G

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. Relay failure or output contact failure caused by usage beyond the specified life of contact (cycles).
   6. 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.
   7. Failure caused by reasons unpredictable by scientific technology standards at time of shipment from Mitsubishi.
   8. 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.

6. Product application

(1) In using the Mitsubishi MELSEC programmable controller, the usage conditions shall be that the application will not lead to a major accident even if any problem or fault should occur in the programmable controller device, and that backup and fail-safe functions are systematically provided outside of the device for any problem or fault.

(2) The Mitsubishi programmable controller has been designed and manufactured for applications in general industries, etc. Thus, applications in which the public could be affected such as in nuclear power plants and other power plants operated by respective power companies, and applications in which a special quality assurance system is required, such as for railway companies or public service purposes shall be excluded from the programmable controller applications.
In addition, applications in which human life or property that could be greatly affected, such as in aircraft, medical applications, incineration and fuel devices, manned transportation, equipment for recreation and amusement, and safety devices, shall also be excluded from the programmable controller range of applications.
However, in certain cases, some applications may be possible, providing the user consults their local Mitsubishi representative outlining the special requirements of the project, and providing that all parties concerned agree to the special circumstances, solely at the user's discretion.

(3) Mitsubishi shall have no responsibility or liability for any problems involving programmable controller trouble and system trouble caused by DoS attacks, unauthorized access, computer viruses, and other cyberattacks.

TRADEMARKS

Microsoft and Windows are trademarks of the Microsoft group of companies.
PLCopen is either a registered trademark or a trademark of the association PLCopen.
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.

Manual number: SH(NA)-082250ENG-G(2403)MEE
MODEL: FX5-U-OPC-E
MODEL CODE: 09R580

MITSUBISHI ELECTRIC CORPORATION

HEAD OFFICE: TOKYO BLDG., 2-7-3, MARUNOUCHI, CHIYODA-KU, TOKYO 100-8310, JAPAN
NAGOYA WORKS: 1-14, YADA-MINAMI 5-CHOME, HIGASHI-KU, NAGOYA 461-8670, JAPAN