FA SYSTEM SECURITY GUIDELINE

- SEPARATE VOLUME [MELSEC] -

MITSUBISHI ELECTRIC CORPORATION

Revision history

Date	Document number	Notes
Sep, 2021	BCN-P5999-1474	First edition
Jun, 2022	BCN-P5999-1474-A	Title is changed, and an example of security measures is revised
Dec, 2024	BCN-P5999-1474-B	MELSEC MX Controller (MX-R model) is supported.

Contents

Terms and Definitions

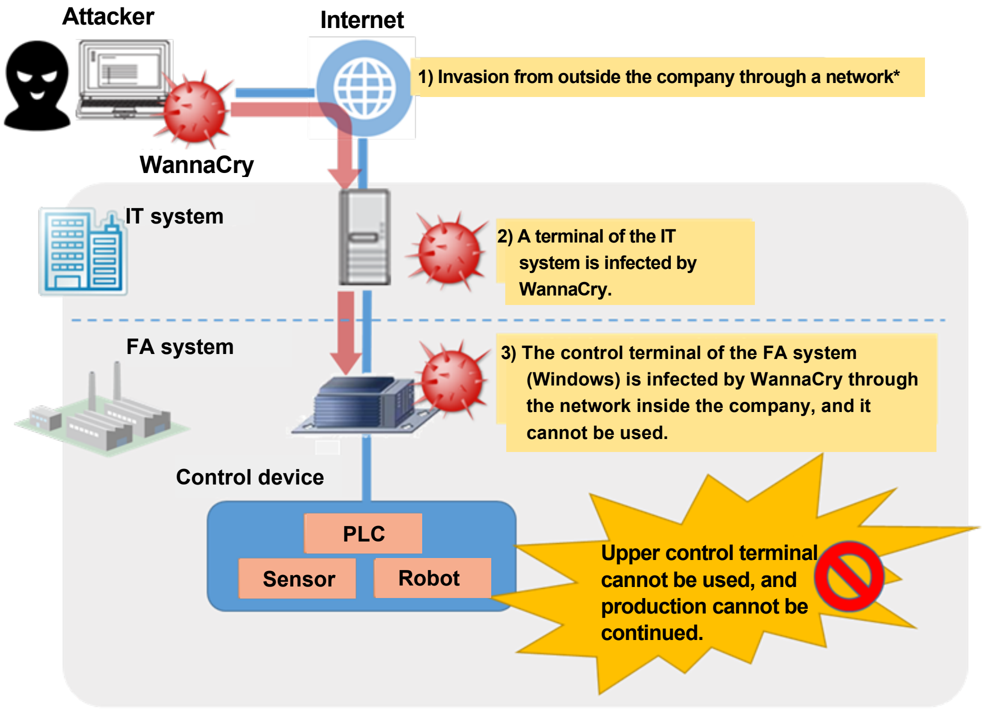
Term	Description
FA[1]	Factory Automation. The use of computer control technologies to automate factories. It also refers to devices used for automation. It is also referred to as Industrial Automation.
IEC 62443[2]	Series of the international standards, which provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs), developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC).
Confidentiality[3]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity[4]	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Availability[5]	The state that exists when data can be accessed, or a requested service provided within an acceptable period of time.
Supply chain[6]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Vulnerability[7]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Security key authentication	A function implemented in the PLC CPU to prevent unauthorized browsing and execution of programs. The project data locked with a security key can be viewed only with the engineering tool registered with the same security key. In addition, a program locked with a security key can be executed only with a module to which the same security key is registered.
File password	A function that prevents unauthorized reading/wiring of files using a password.
Remote password	A password that prevents unauthorized access to the PLC CPU from remote users.
Block password	A function that prevents unauthorized browsing of programs using a password.
Service setting function	A function that sets Enable/Disable for services on an FA product such as C controller. This function requires security password therefore unauthorized access can be prevented.

[1] Mitsubishi Electric FA Terminology Dictionary, https://www.mitsubishielectric.com/fa/assist/fa_reference/pdf/k-027-k1209.pdf
[2] International Society of Automation (ISA), https://www.isa.org/intech/201810standards/
[3] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/confidentiality
[4] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/integrity
[5] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/availability
[6] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/supply_chain
[7] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/vulnerability

1. Introduction

1.1. Background

With the rapid development of the Internet and IT/IoT technologies, IT utilization in FA systems is increasing to improve the productivity of factories. As the IT utilization in FA systems advances, conventional thinking that FA systems cannot be infected by malware or exposed to cyberattacks because they are “dedicated systems” or “closed” is no longer valid, and the security risks on FA systems are increasing. In fact, in 2017, a malware called WannaCry, which targeted IT systems, caused significant damage, including the shutdown of factories. (Figure 1)


Attacker
Internet
1) Invasion from outside the company through a network*
WannaCry
IT system
2) A terminal of the IT system is infected by WannaCry.
FA system
3) The control terminal of the FA system (Windows) is infected by WannaCry through the network inside the company, and it cannot be used.
Control device
PLC
Sensor
Robot
Upper control terminal cannot be used, and production cannot be continued.

* The TCP 445 port is directly attacked. It is infected by WannaCry without opening an e-mail.

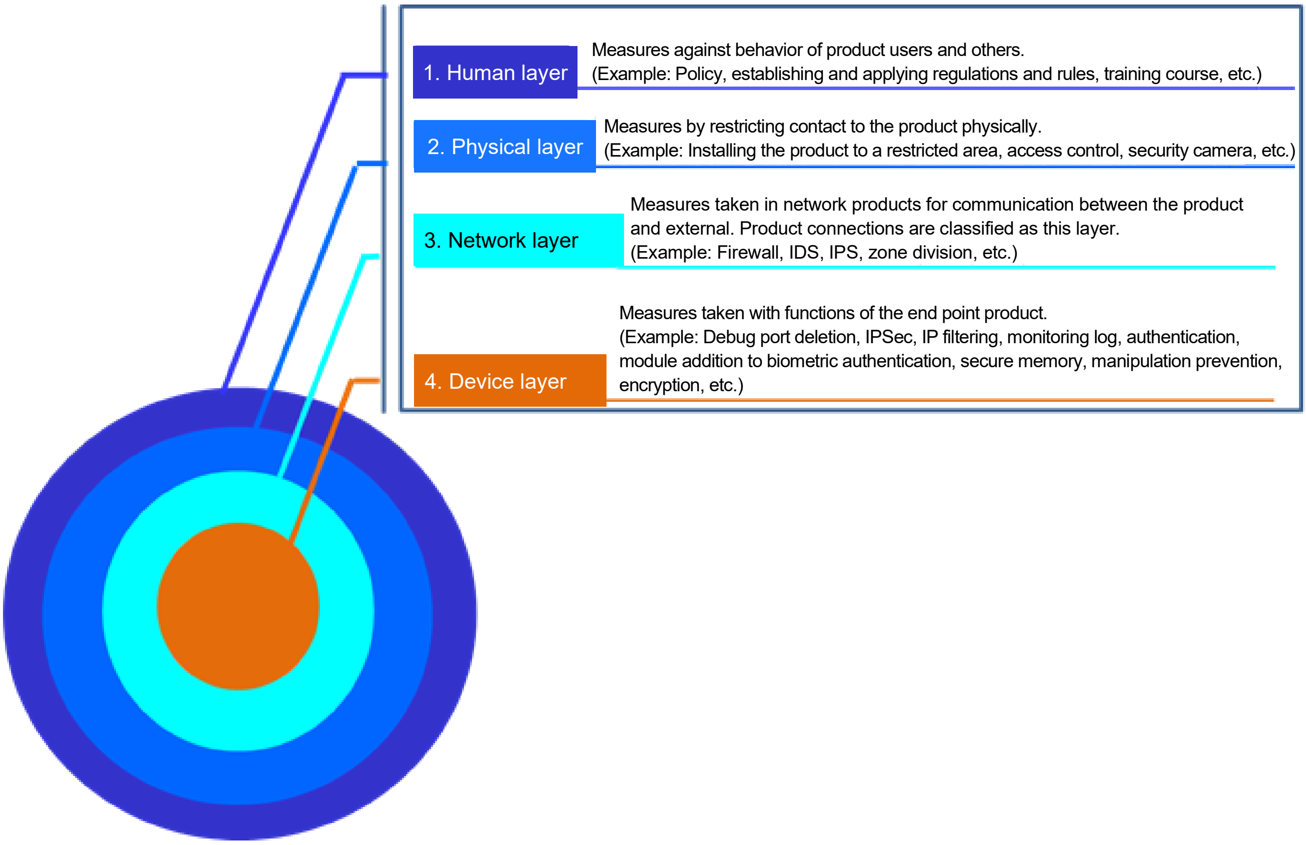
Figure 1 Example of WannaCry infection route and damage to FA system

To protect FA systems from such threats, it is important to combine multiple security measures hierarchically, ranging from physical security measures for factories such as access control, human security measures such as rules and education applied to users who handle products, to security measures on networks and FA devices in factories. This improves security and reduces the impact of attacks by “raising the costs of attack for the attacker and raising the bar to attack” and “enhancing detection and prevention capabilities in the event of an attack”. Such a concept of security measures is called “defense in depth” and is recommended in the international standard IEC 62443[8]. As a manufacturer and seller of FA devices, Mitsubishi Electric Corporation (hereinafter referred to as “Mitsubishi Electric”) is developing PLCs that are compliant with IEC 62443 for realizing and maintaining safe and secure FA systems for our customers.

[8] For IEC 62443, refer to “FA SYSTEM SECURITY GUIDELINE”.

1.2. Defense in depth for protecting FA products

Defense in depth in security measures refers to the concept of taking countermeasures from different perspectives, such as “human operations”, “use of device and facility”, “network access”, “data access”, and “application execution”. Mitsubishi Electric divides this perspective into two defense-in-depth measures, one related to the environment (outside the product) and the other related to inside the product, and defines them as the “human layer”, “physical layer”, “network layer”, and “device layer” (Figure 2). Defense in depth reduces the impact of attacks by raising the costs of attack for the attacker and enhancing detection and prevention capabilities in the event of an attack.
The security function of the Mitsubishi Electric products is one of the defense-in-depth measures in the device layer or network layer. To protect the FA system from cyberattacks, measures need to be taken in each of the human layer, physical layer, network layer, and device layer. For example, we recommend that you install a firewall for the purpose of protection from cyberattacks, install anti-virus software into the personal computer, and consider introducing the entry and exit control in the factory.



1. Human layer
Measures against behavior of product users and others.
(Example: Policy, establishing and applying regulations and rules, training course, etc.)

2. Physical layer
Measures by restricting contact to the product physically.
(Example: Installing the product to a restricted area, access control, security camera, etc.)

3. Network layer
Measures taken in network products for communication between the product and external. Product connections are classified as this layer.
(Example: Firewall, IDS, IPS, zone division, etc.)

4. Device layer
Measures taken with functions of the end point product.
(Example: Debug port deletion, IPSec, IP filtering, monitoring log, authentication, module addition to biometric authentication, secure memory, manipulation prevention, encryption, etc.)

Figure 2 Concept of defense in depth

2. Security of the MELSEC MX Controller (MX-R model)

2.1. Purpose of this chapter

This chapter provides the following information to explain our approach to the security of the MELSEC MX Controller (MX-R model) so that it can be used safely and securely in customers' FA systems.

- Policy on security measures for the MELSEC MX Controller (MX-R model) (Section 2.2):
  This section describes the policy on security measures against threats by identifying possible threats to the MELSEC MX Controller (MX-R model). Some countermeasures are performed by the MELSEC MX Controller (MX-R model) alone while others are performed in combination with other products.
- Introduction method of the MELSEC MX Controller (MX-R model) (Section 2.3 and 2.4):
  These sections describe the security functions of the MELSEC MX Controller (MX-R model), how to set them, and how to install the MELSEC MX Controller (MX-R model) in an FA system.
- Operation and maintenance method of the MELSEC MX Controller (MX-R model) (Section 2.5):
  This section describes recommendations on how to manage users and passwords for operating the MELSEC MX Controller (MX-R model).
- Removal and disposal method of the MELSEC MX Controller (MX-R model) (Section 2.6):
  This section describes the recommended methods (e.g., product data deletion functions) for removing and disposing of the MELSEC MX Controller (MX-R model).

In addition, refer to the following manual for the detailed specifications and operation methods for each function of the MELSEC MX Controller (MX-R model) as necessary.

- MELSEC MX Controller (MX-R model) User's Manual

Read this guideline and the above related manual carefully to fully understand the security of the MELSEC MX Controller (MX-R model), and use it to realize and maintain safe and secure FA systems.

In addition, refer to the following document for the basic security policy for Mitsubishi Electric FA products including the MELSEC MX Controller (MX-R model), product life cycle initiatives, and examples of FA system construction.

- FA SYSTEM SECURITY GUIDELINE

2.2. Policy on security measures for the MELSEC MX Controller (MX-R model)

This section describes the following policy on security measures for the MELSEC MX Controller (MX-R model).

- Expected usage environment (installation environment, network, operation and maintenance, etc.) of the MELSEC MX Controller (MX-R model)
- Threats to the MELSEC MX Controller (MX-R model)
- Policy on countermeasures against threats
- Security functions in the MELSEC MX Controller (MX-R model)
- Security measures to be taken outside the product

2.2.1. Expected usage environment of the MELSEC MX Controller (MX-R model)

Figure 3 shows the environment where the MELSEC MX Controller (MX-R model) is expected to be installed. Table 1 shows the prerequisites for ensuring security in the installation environment shown in Figure 3. These installation environment and usage environment including prerequisites are the premise for the policy on security measures described in the subsequent sections.

The MELSEC MX Controller (MX-R model) is intended for use in equipment to be installed on a production site in a factory. In this equipment, devices to be connected to the CC-Link IE TSN network are also installed in addition to the MELSEC MX Controller (MX-R model), which means that this equipment is the trust boundary[9]. SD cards and maintenance personal computers are connected to the MELSEC MX Controller (MX-R model) for use, however, they are located outside the trust boundary because they are portable and used outside the equipment. In addition, there is a server room in the factory, where production monitoring personal computers and various servers are installed. It is assumed that the network in the factory where the MELSEC MX Controllers (MX-R model) are installed will be connected to the Internet via firewalls and routers.

[9] It is the boundary that separates the area that assumes trust from the other areas. As an example, the trust boundary is often equipped with security functions such as an authentication function, and users who are successfully authenticated can enter the trust boundary. Also, users who failed authentication cannot access anything within the trust boundary.

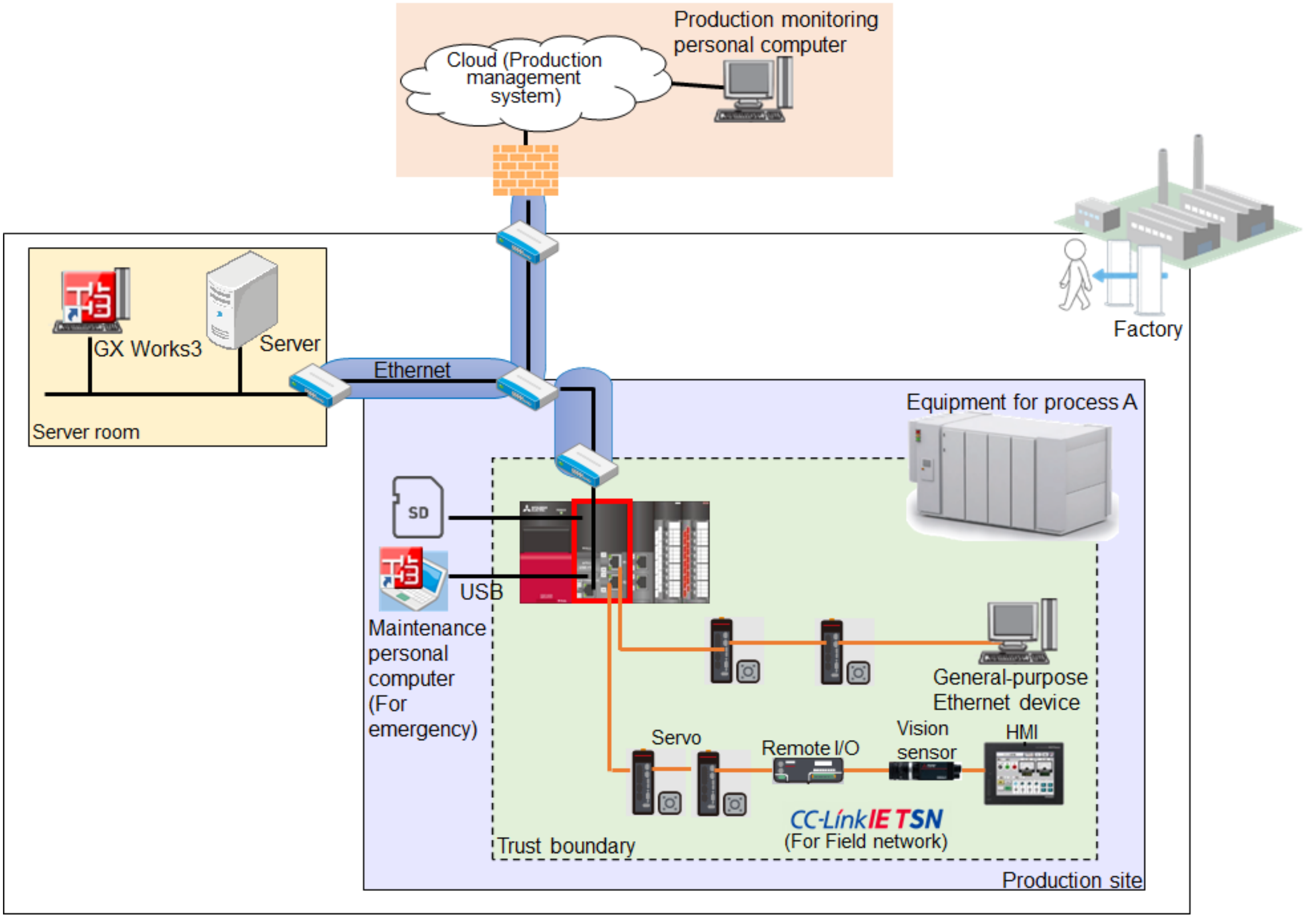


Figure 3 Environment where the MELSEC MX Controller (MX-R model) is expected to be installed

Table 1 Prerequisite in the installation environment

No.	Prerequisite	Description
1	Access control	Access control is used to restrict who can enter the factory.
2	Lock of the equipment in which the MELSEC MX Controller (MX-R model) is installed	The equipment in which the MELSEC MX Controller (MX-R model) is installed is locked, and the devices in the equipment cannot be operated or changed without the permission of the administrator.
3	Management of an SD card	An SD card is used in the locked equipment and cannot be inserted or removed without the permission of the administrator.
4	Physical protection of JTAG I/F	JTAG I/F is inside the case of the MELSEC MX Controller (MX-R model) and is not directly accessible physically.
5	Education for users	Users are adequately educated and trained to properly set, manage, and operate the MELSEC MX Controller (MX-R model).
6	Selection of an appropriate administrator	A person who will carry out the administration properly without malicious intent is selected as the administrator.
7	Installation of a firewall	Network switches and firewalls are installed between the network to which the MELSEC MX Controller (MX-R model) is connected and the external network, blocking unnecessary communications from the external network.
8	Security on the personal computer which communicates with the MELSEC MX Controller (MX-R model)	The personal computers which communicate with the MELSEC MX Controller (MX-R model) (maintenance personal computers and production monitoring personal computers) have anti-virus software to ensure security.

Table 2 describes the devices and networks in Figure 3.

Table 2 Device/application/network in the environment

No.	Term	Description
1	HMI	A device connected to the MELSEC MX Controller (MX-R model) to operate it and display information. Example of Mitsubishi Electric HMI: GOT3000 series
2	Production monitoring personal computer	A device with software for monitoring the status of the control system installed.
3	Maintenance personal computer	A device with an engineering tool necessary for maintaining the MELSEC MX Controller (MX-R model) installed. Example of Mitsubishi Electric engineering tool: GX Works3
4	Field network	A network used for communication between the MELSEC MX Controller (MX-R model) and field devices.
5	Control information network	A network that is inside a firewall and used for communication between a production monitoring personal computer or other devices and the MELSEC MX Controller (MX-R model). Example of control information network: Ethernet
6	Firewall	A device equipped with filtering functions such as packet filtering, communication restriction functions such as bandwidth limitation, and address translation functions such as NAT (Network Address Translation) and NAPT (Network Address Port Translation).
7	Network switch	A device that uses network layer information in the OSI reference protocol to separate networks with a virtual router or VLAN (Virtual Local Area Network). The network switch can also be used together with the network router.
8	External network	A network that is outside the firewall and beyond the factory's authority to manage the network. Example of external network: Internet
9	Field device	A device that generates values to be input to the MELSEC MX Controller (MX-R model) and outputs the values generated by the MELSEC MX Controller (MX-R model). Example of field device: Servo

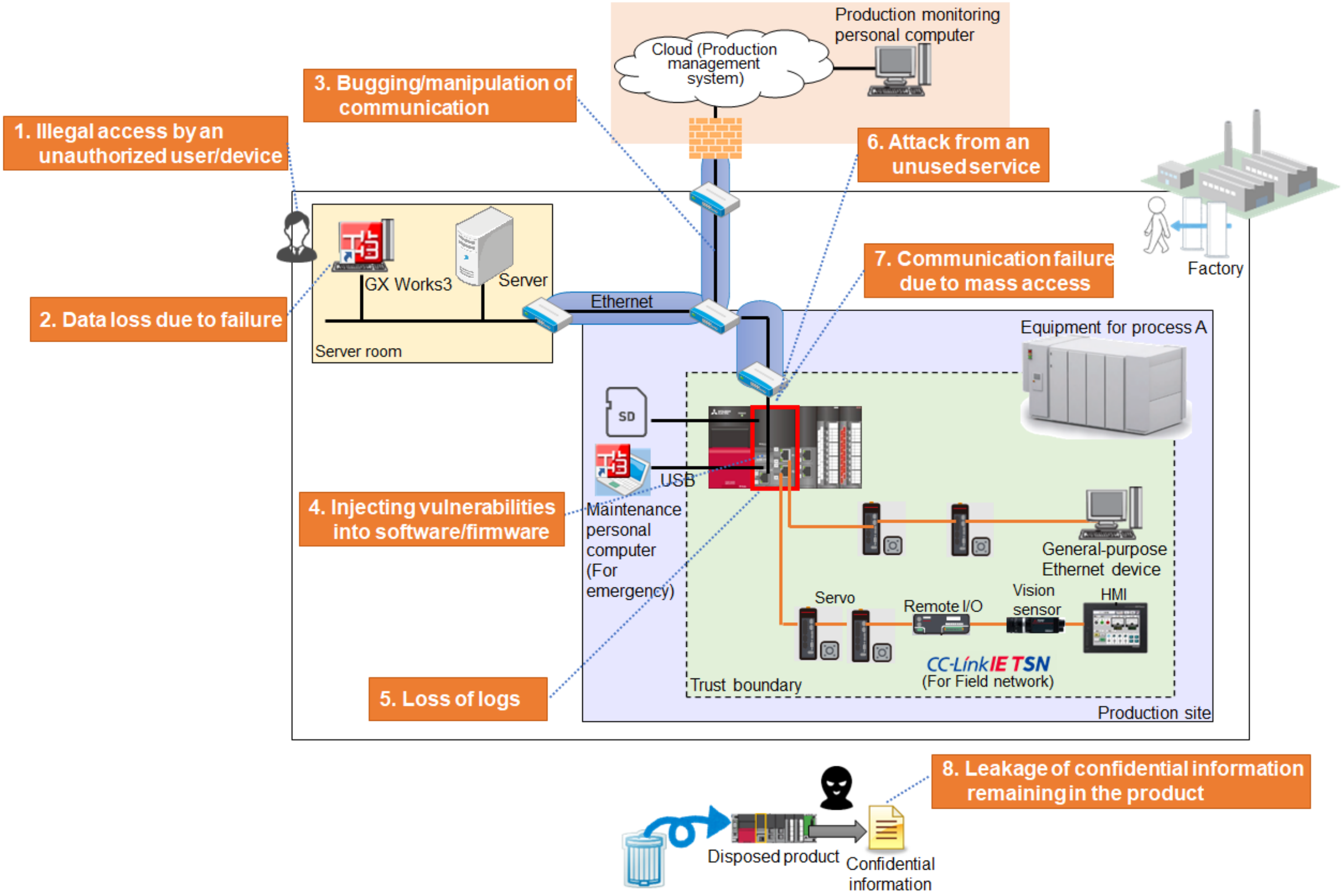
Access to devices can be physically controlled by restricting entry to individual areas of the factory or by applying physical locks to the device storage areas. These physical access controls are also important security elements. For the use of the MELSEC MX Controller (MX-R model), the area classification shown in Table 3 is assumed from a security perspective.

Table 3 Area classification and operation method

No.	Term	Description
1	Server room	A room that stores devices critical to continue the operation of the control system, such as a device that manages the network. To protect against unauthorized access and vandalism, measures are taken so that only specific people can enter and exit the room (e.g., entry and exit management).
2	Equipment area of each process	Equipment in which the MELSEC MX Controller (MX-R model) is stored. To protect against unauthorized access and vandalism, measures are taken so that only specific people out of those who are allowed to enter the production site can operate the equipment (e.g., entry and exit management).
3	Production site	An area where only the users of the control system can enter.
4	Factory	An area with both an accessible area and a server room.

2.2.2. Threats to the MELSEC MX Controller (MX-R model)

We assume the threats shown in Figure 4 and Table 4 in the usage environment of the MELSEC MX Controller (MX-R model) shown in Figure 3 of 2.1.1 based on the risk assessment of the module and knowledge of publicly known attack cases.



Production monitoring personal computer
Cloud (Production management system)
3. Bugging/manipulation of communication
1. Illegal access by an unauthorized user/device
6. Attack from an unused service
Factory
7. Communication failure due to mass access
GX Works3
Server
Ethernet
2. Data loss due to failure
Server room
Equipment for process A
SD
USB
Maintenance personal computer (For emergency)
4. Injecting vulnerabilities into software/firmware
General-purpose Ethernet device
Servo
Remote I/O
Vision sensor
HMI
CC-Link IE TSN
(For Field network)
Trust boundary
5. Loss of logs
Production site
8. Leakage of confidential information remaining in the product
Disposed product
Confidential information

Figure 4 Threats to the MELSEC MX Controller (MX-R model)

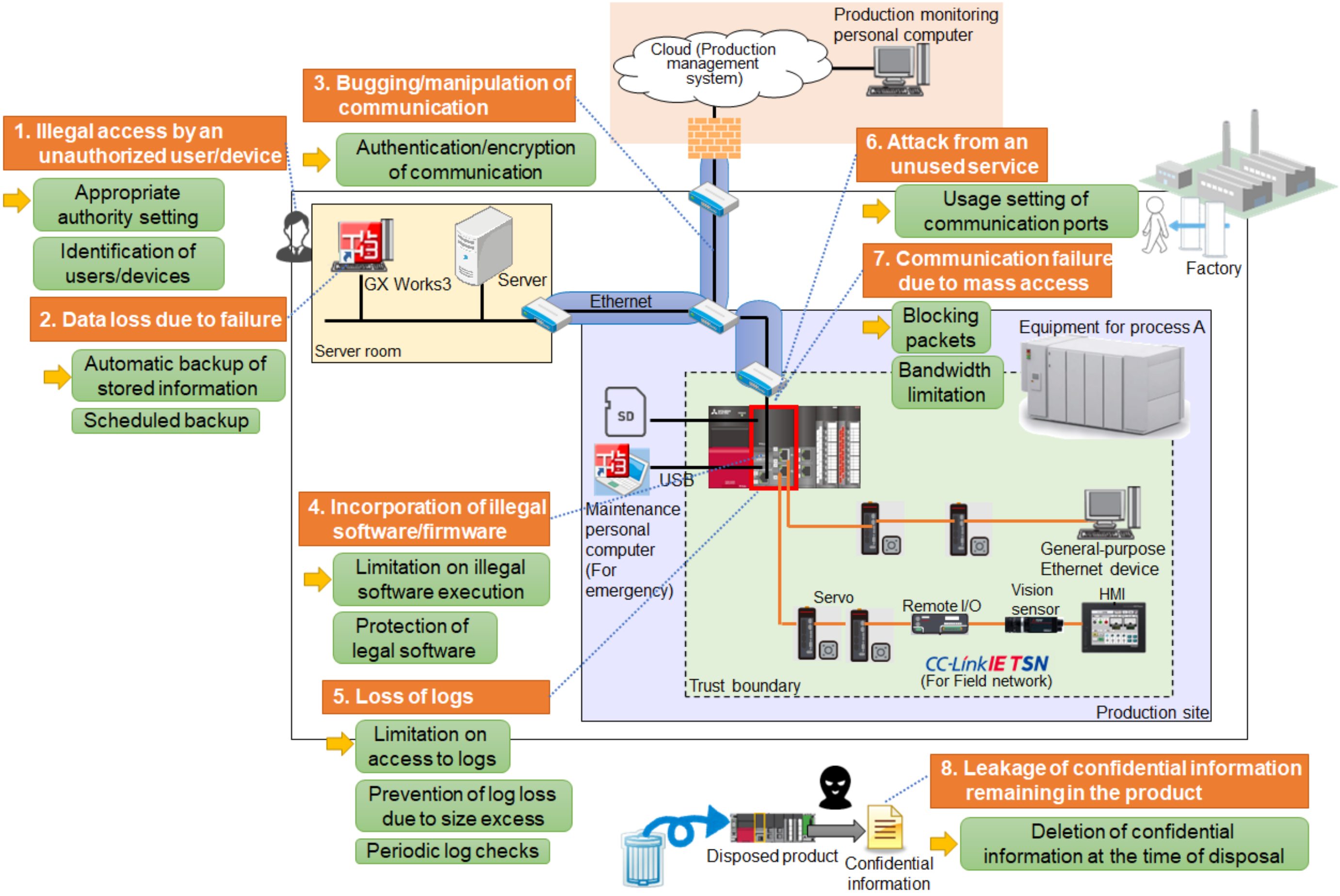
Table 4 Description of threats

No.	Threat name	Description
1	Illegal access by an unauthorized user	Illegal access is made by a user unauthorized by the administrator.
2	Data loss due to failure	Information stored in the MELSEC MX Controller (MX-R model) is lost or becomes unavailable due to a device failure caused by a disaster or other reasons.
3	Eavesdropping/manipulation of communication	Communication between the MELSEC MX Controller (MX-R model) and an external device is eavesdropped or manipulated.
4	Introduction of vulnerabilities to software/firmware	If a vulnerability is introduced in the software or firmware of the MELSEC MX Controller (MX-R model), it will be vulnerable to attack.
5	Loss of logs	Loss of logs caused by user operation errors prevents the occurrence of incidents from being traced.
6	Attack from an unused service	Illegal access is made from an unused communication port or protocol.
7	Communication failure due to mass access	Increased communication traffic in the network prevents necessary communication.
8	Leakage of confidential information remaining in the product	Information leakage occurs through the extraction of confidential information remaining in the discarded products or others.

2.2.3. Policy on countermeasures against threats

Figure 5 and Table 5 show the policy on countermeasures against threats to the MELSEC MX Controller (MX-R model). The policy includes not only the countermeasures to be taken in the MELSEC MX Controller (MX-R model), but also the ones to be taken in the customer's environment.

To realize the defense in depth described in 1.2, security measures need to be taken in the human, physical, and network layers, which are difficult to be taken in the MELSEC MX Controller (MX-R model). Therefore, it is necessary to maintain security measures not only for the MELSEC MX Controller (MX-R model) but also for the entire FA system.



Production monitoring personal computer
Cloud (Production management system)
3. Bugging/manipulation of communication
Authentication/encryption of communication
1. Illegal access by an unauthorized user/device
Appropriate authority setting
Identification of users/devices
6. Attack from an unused service
Usage setting of communication ports
Factory
GX Works3
Server
Server room
Ethernet
7. Communication failure due to mass access
Blocking packets
Bandwidth limitation
Equipment for process A
2. Data loss due to failure
Automatic backup of stored information
Scheduled backup
SD
USB
Maintenance personal computer (For emergency)
4. Incorporation of illegal software/firmware
Limitation on illegal software execution
Protection of legal software
General-purpose Ethernet device
Servo
Remote I/O
Vision sensor
HMI
CC-Link IE TSN
(For Field network)
Trust boundary
Production site
5. Loss of logs
Limitation on access to logs
Prevention of log loss due to size excess
Periodic log checks
8. Leakage of confidential information remaining in the product
Deletion of confidential information at the time of disposal
Disposed product
Confidential information

Figure 5 Policy on countermeasures against threat to the MELSEC MX Controller (MX-R model)

Table 5 Policy on countermeasures against threat to the MELSEC MX Controller (MX-R model)

No.	Threat name	Policy on countermeasures	Related functions/measures	Related security functions of the MELSEC MX Controller (MX-R model)
1	Illegal access by an unauthorized user	● Appropriate authority setting ● User identification	● User authentication function ● Physical access restriction ● Selection of the administrator ● Installation of a firewall ● Security on the personal computer	2.4.4. User authentication function
2	Data loss due to failure	● Automatic backup of the saved information ● Scheduled backup ● System restoration using backup data	● Backup/restoration function ● Scheduled backup	2.4.6. Backup/restoration function of the controller
3	Eavesdropping/manipulation of communication	● Authentication/encryption of communication	● Encrypted communication function ● Physical access restriction ● Installation of a firewall ● Security on the personal computer	2.4.7. Encrypted communication function
4	Introduction of vulnerabilities to software/firmware	● Limitation on illegal software execution ● Protection of legal software	● Firmware update function ● Add-on install function	2.4.2. Firmware update function 2.4.3. Add-on install function
5	Loss of logs	● Limitation on access to logs ● Prevention of log loss due to size excess ● Periodic log checks	● Event history function ● Log audit ● Security on the personal computer	2.4.5. Event history function
6	Attack from an unused service	● Usage setting of communication ports	● Usage setting function of default open port ● Education for users	2.4.9. Usage setting function of default open port
7	Communication failure due to mass access	● Blocking packets ● Bandwidth limitation	● IP filter function ● Bandwidth limitation function against DoS attack	2.4.8. IP filter function 2.4.10. Bandwidth limitation function against DoS attack
8	Leakage of confidential information remaining in the product	● Deletion of confidential information at the time of disposal	● Initialization of all controller information	2.4.1. Initialization function of all information in the controller

2.2.4. Security functions in the MELSEC MX Controller (MX-R model)

The MELSEC MX Controller (MX-R model) implements the security functions as described in Table 6 to realize the policy on countermeasures against threat described in 2.2.3.

Table 6 Security functions in the MELSEC MX Controller (MX-R model)

Function name	Description	Corresponding threat
User authentication function	Authenticates the user who can access.	1. Illegal access by an unauthorized user/device
Firmware update function	Checks that the firmware is not manipulated, and updates it.	4. Introduction of vulnerabilities to software/firmware
Add-on install function	Checks that the add-on is not manipulated, and updates it.	4. Introduction of vulnerabilities to software/firmware
Usage setting function of default open port	Closes the unused default open ports.	6. Attack from an unused service
Initialization of all controller information	Deletes the data memory (non-volatile data) at once. Deletes the device (volatile data).	8. Leakage of confidential information remaining in the product
Encrypted communication function	Prevents eavesdropping by encrypted communication. Prevents impersonation by using a certificate.	3. Eavesdropping/manipulation of communication
IP filter function	Communicates with only devices to which authorized IP addresses have been assigned.	7. Communication failure due to mass access
Event history function	Displays and saves the generated event logs.	5. Loss of logs
Bandwidth limitation function against DoS attack	Maintains the execution of essential functions by limiting the communication bandwidth in the event of a DoS attack.	7. Communication failure due to mass access
Backup/restoration function	Backs up the user programs, parameters, and device values in the SD memory card and restores them to the CPU module.	2. Data loss due to failure

2.2.5. Security measures to be taken outside the product

Figure 6 and Table 7 show the security measures recommended to be taken in the usage environment of the customer with the prerequisites (Table 1) in the usage environment (Figure 3) of the MELSEC MX Controller (MX-R model) and policy on countermeasures against threat (2.2.3).

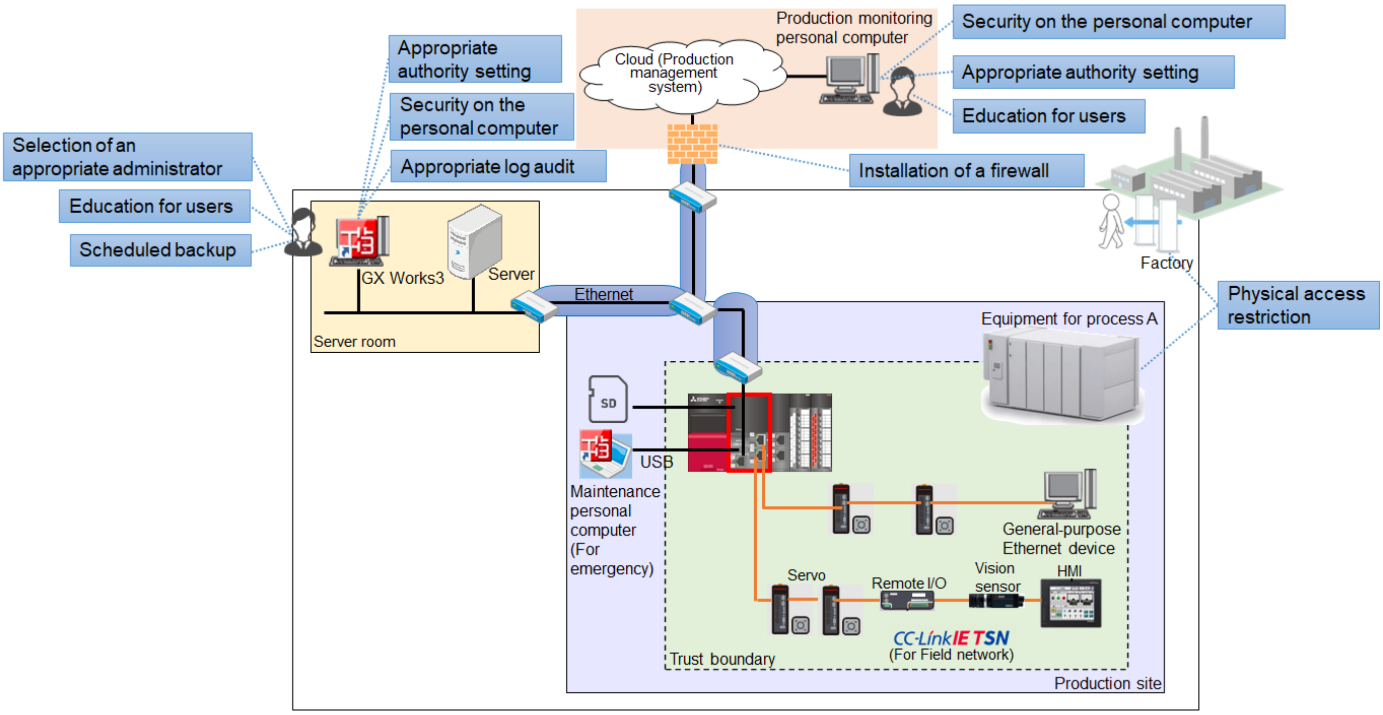

Appropriate authority setting
Security on the personal computer
Appropriate log audit
Cloud (Production management system)
Production monitoring personal computer
Security on the personal computer
Appropriate authority setting
Education for users
Installation of a firewall
Selection of an appropriate administrator
Education for users
Scheduled backup
GX Works3
Server
Server room
Ethernet
Factory
Physical access restriction
Equipment for process A
SD
USB
Maintenance personal computer (For emergency)
General-purpose Ethernet device
Servo
Remote I/O
Vision sensor
HMI
CC-Link IE TSN
(For Field network)
Trust boundary
Production site

Figure 6 Security measures to be taken in the usage environment

Table 7 Description of the security measures in the usage environment

Layer of defense in depth	Measure name	Description	Target threat
Physical layer	Physical access restriction	Physical access to the MELSEC MX Controller (MX-R model) is restricted by using it in equipment or storing it in a locked cabinet so that outsiders cannot touch it.	1. Illegal access by an unauthorized user/device 3. Eavesdropping/manipulation of communication
Human layer	Education for users	Users are educated so that they use the MELSEC MX Controller (MX-R model) securely. For example, they are educated on the following items. • Setting of the communication ports and protocols that can be used • Backup/restoration setting	1. Illegal access by an unauthorized user/device 2. Data loss due to failure
Human layer	Selection of the administrator	For the administrator, an appropriate person who will not abuse his/her authority shall be selected.	1. Illegal access by an unauthorized user/device
Human layer	Log audit	The administrator shall audit the audit logs at appropriate time intervals according to the operating regulations and operating manual. Also, he/she shall periodically check the logs for damage.	5. Loss of logs
Human layer	Scheduled backup	Scheduled backup prevents forgetting to take backups.	2. Data loss due to failure

Layer of defense in depth	Measure name	Description	Target threat
Network layer	Installation of a firewall	Installation of firewalls or others blocks illegal access from external networks.	1. Illegal access by an unauthorized user/device 3. Eavesdropping/manipulation of communication
Device layer	Security on the personal computer	Appropriate security measures such as installation of anti-virus software shall be taken on the personal computers that communicate with the MELSEC MX Controller (MX-R model) (maintenance personal computers and production management personal computers).	1. Illegal access by an unauthorized user/device 3. Eavesdropping/manipulation of communication 5. Loss of logs

2.3. Introduction of the MELSEC MX Controller (MX-R model)

This section describes how to introduce the MELSEC MX Controller (MX-R model) in a system and how to set and use the security functions of the MELSEC MX Controller (MX-R model).

2.3.1. Setting and introduction procedures of the MELSEC MX Controller (MX-R model)

To use the MELSEC MX Controller (MX-R model) in a system (Figure 7) in compliance with IEC 62443-4-2 (security enhancement settings enabled), it is recommended that the MELSEC MX Controller (MX-R model) be operated according to the procedure described in Figure 8.

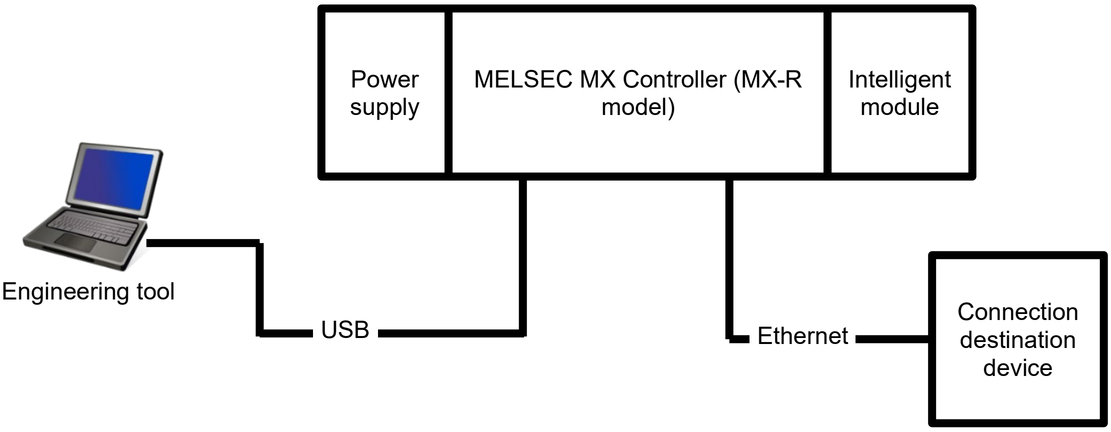

Power supply
MELSEC MX Controller (MX-R model)
Intelligent module
Engineering tool
USB
Ethernet
Connection destination device

Figure 7 System configuration example

Connect the computer with the engineering tool installed to the MELSEC MX Controller (MX-R model) and perform the settings. The following engineering tool is compatible with the MELSEC MX Controller (MX-R model).

Table 8 The engineering tool for the MELSEC MX Controller (MX-R model)

Name	Version
MELSOFT GX Works3 Version1	1.115V or later

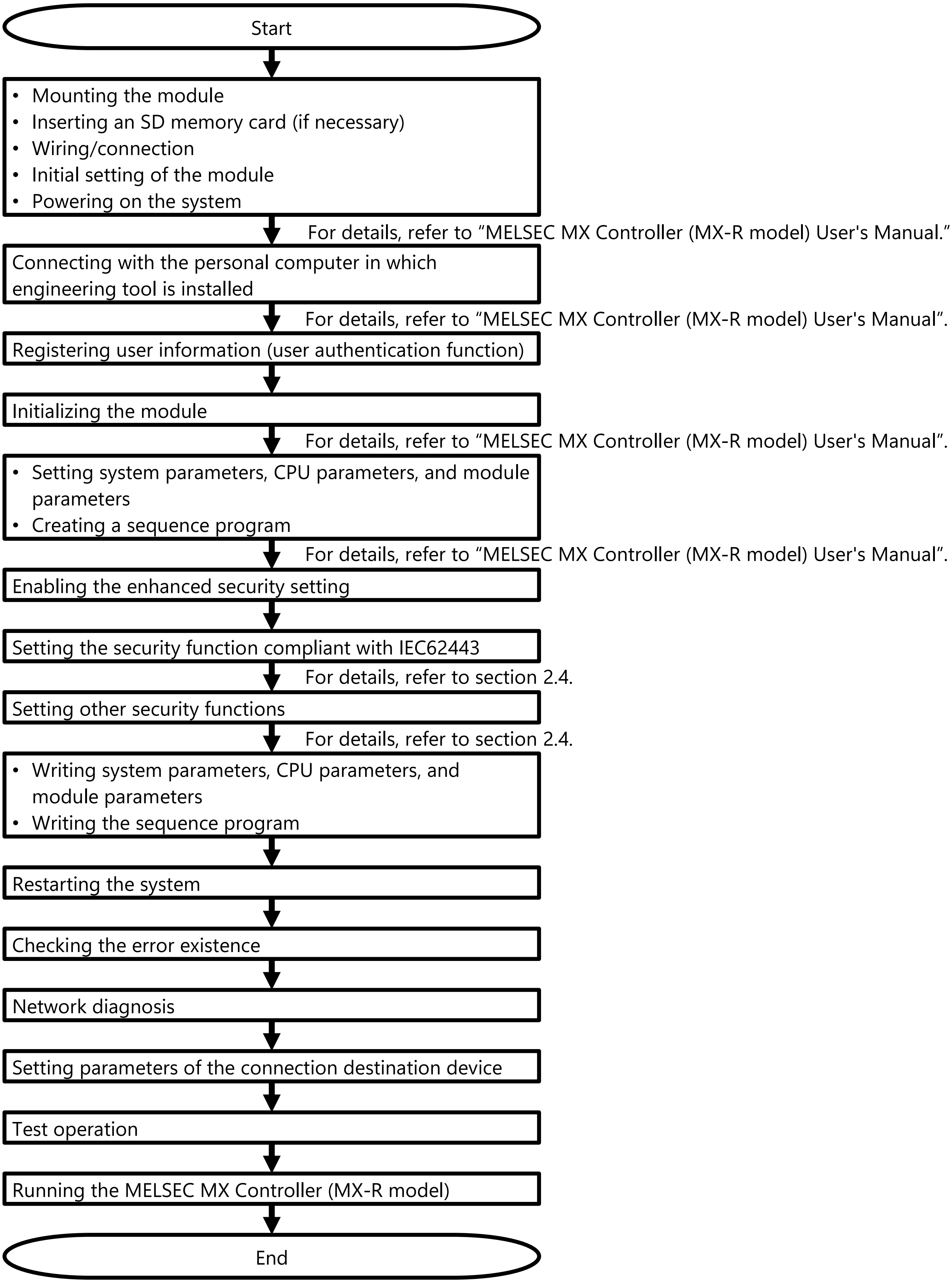

Start
• Mounting the module
• Inserting an SD memory card (if necessary)
• Wiring/connection
• Initial setting of the module
• Powering on the system
For details, refer to "MELSEC MX Controller (MX-R model) User's Manual."
Connecting with the personal computer in which engineering tool is installed
For details, refer to "MELSEC MX Controller (MX-R model) User's Manual".
Registering user information (user authentication function)
Initializing the module
For details, refer to "MELSEC MX Controller (MX-R model) User's Manual".
• Setting system parameters, CPU parameters, and module parameters
• Creating a sequence program
For details, refer to "MELSEC MX Controller (MX-R model) User's Manual".
Enabling the enhanced security setting
Setting the security function compliant with IEC62443
For details, refer to section 2.4.
Setting other security functions
For details, refer to section 2.4.
• Writing system parameters, CPU parameters, and module parameters
• Writing the sequence program
Restarting the system
Checking the error existence
Network diagnosis
Setting parameters of the connection destination device
Test operation
Running the MELSEC MX Controller (MX-R model)
End

Figure 8 Procedure before operation

• Setting the security function compliant with IEC 62443 and the security policy

Perform the following items (Table 9) as the settings for the security functions compliant with IEC 62443. In addition, when operating, please follow the implementation details described in Table 10.

Table 9 Setting for the security function compliant with IEC 62443

No.	Item	Setting for the security function	Reference
1	User authentication	User authentication shall be enabled before setting and operating the encrypted communication, IP filter, usage setting function of default open port, bandwidth limitation function against DoS attack, and time setting.	2.4.4.2
2		Operation authority for each user group shall be set properly.	2.4.4.1
3		Passwords shall be periodically changed. (It is recommended that you enable the password expiration date setting.)	2.4.4
4		Each password shall be difficult to guess. (It is recommended that you set the password strength setting to “Strong”.)	2.4.4.2
5		Appropriate lockout time and the number of lockouts shall be set.	2.4.4
6		Appropriate usage notification messages giving warning to the logged on users shall be set.	2.4.4
7		Since communication requests via a module other than a controller are out of the user authentication targets, a network to which a module other than a controller is connected shall be protected by the security functions of the module (e.g., IP filter) or by an external device (e.g., firewall).	2.4.4.2
8	User authentication function Ethernet communication function FTP server function	Appropriate timers for connection and session shall be set.	2.4.4
9	Event history	The event history function shall be enabled.	2.4.5
10		Appropriate storage size of the event history shall be set.	2.4.5
11		Event history shall be periodically backed up to a personal computer since oldest entries will be overwritten when the storage size is exceeded.	2.4.5
12		Correct time shall be set so that the time stamps are recorded correctly.	2.4.5
13		The manipulation check function for event history shall be enabled.	2.4.5
14	Backup/restoration function	Encryption setting of backup data shall be performed.	2.4.6.1
15	Encrypted communication	Communications with external devices beyond the trust boundary shall be encrypted.	2.4.7
16		Communications that require encryption shall be performed in the network ports built in the MELSEC MX Controller (MX-R model).	2.4.7.1
17		The expiration date of the certificate used for encrypted communications shall be set to one year (default setting).	2.4.7.2
18	IP filter	Accesses from external devices shall be restricted with the IP filter.	2.4.8
19	Usage setting function of default open port	Unused ports shall be set as closed.	2.4.9.1
20		Communications with the outside of the trust boundary shall be performed using the network ports built in the MELSEC MX Controller (MX-R model).	2.4.9

No.	Item	Setting for the security function	Reference
21	Bandwidth limitation function against DoS attack	The bandwidth limitation function against DoS attack shall be set.	2.4.10
22	Bandwidth limitation function against DoS attack, IP filter, and usage setting function of default open port	Use the countermeasures against DoS attacks with other examples of countermeasures against illegal access as well as the IP filter, usage setting function of default open port, and bandwidth limitation function against DoS attack.	2.4.10.1

Table 10 Implementation matters related to security policy and usage environment

No.	Item	Implementation matters	Reference
1	Precautions when removing/disposing of connected devices	When removing or disposing of a device connected to the MELSEC MX Controller (MX-R model), there is a possibility that protected assets (data) are stored in that device.	2.6
2	Connected devices	Verify prior to use that equipment connected to the MELSEC MX Controller (MX-R model) is configured and performing as intended.	-
3		Terminate the session as soon as communication with the device connected to the MELSEC MX Controller (MX-R model) is no longer required.	-
4	Use of SD card	Use the SD card only for backup/restore, and do not store any data other than backup data.	2.5.1
5	Perform and manage backups	Since there is a possibility that the protected assets (data) of the MELSEC MX Controller (MX-R model) and connected devices within the system may be lost due to a sudden disaster or failure, etc., perform regular backups and manage the backup data appropriately.	2.4.6 2.5
6	Password management	Passwords shall be properly managed to prevent leakage and shall not be reused.	2.4.4
7	Trust boundary	Use SNTP, FTP, BACnet, Modbus communications, and connections with other devices using USB ports and CC-Link IE TSN ports within a trust boundary.	2.4.7

2.4. How to set and use security functions and options

This section describes how to set and use the security functions of the controller. It also describes the important security items and precautions for setting and using each function.

For the operation procedures of the functions, refer to “MELSEC MX Controller (MX-R model) User's Manual”.

This section describes the following security functions.

- Initialization function of all information in the controller (Section 2.4.1)
- Firmware update function (Section 2.4.2)
- Add-on install function (Section 2.4.3)
- User authentication function (Section 2.4.4)
- Event history function (Section 2.4.5)
- Backup/restoration function of the controller (Section 2.4.6)
- Encrypted communication function (Section 2.4.7)
- IP filter function (Section 2.4.8)
- Usage setting function of default open port (Section 2.4.9)
- Bandwidth limitation function against DoS attack (Section 2.4.10)
- Operation setting (Section 2.4.11)

2.4.1. Initialization function of all information in the controller

Initializing all information in the controller completely deletes the data in the device/label memory, function memory, program memory, data memory, and motion data memory in the controller. The following data is the data to be deleted by initialization.

- Device/label
- File
- Setting information of security functions
- Event history
- Certificate information

2.4.2. Firmware update function

The firmware update function updates the firmware of the modules specified by an engineering tool at once.

2.4.2.1. Precautions

The following shows the precautions on using this function.

- Check that the firmware version is correctly updated using the engineering tool after the update.
- To prevent illegal firmware updates by malicious third parties, it is strongly recommended that the user authentication function of the controller be enabled. When the user authentication function is enabled, user authentication of Administrator (administrator level) is required to operate the firmware update function.
- Download the firmware update file from the MITSUBISHI ELECTRIC FA Global Website[10]. Do not use files obtained from other sources. Download the correct firmware update file according to the target model. Do not change the file name or data of the downloaded firmware update file.
- Periodically check for firmware updates and perform update as necessary.
- Since the operations of all modules cannot be guaranteed during the update, check that the controller and the system to be updated are stopped and that communication cables, wires, or others between the system and another system connected through the network are disconnected before the update.
- Check that there is no abnormality in the system operation before and after the update. If there is an abnormality after the update, restore the version before the update. To restore a version that is not published on the website, contact your local Mitsubishi Electric or our specified representatives.

[10] MITSUBISHI ELECTRIC FA Global Website, https://www.mitsubishielectric.com/fa/worldwide/

2.4.3. Add-on install function

Even if the firmware is updated using the firmware update function, add-ons installed on the controller will not be updated. Add-ons should be updated using the add-on install function. The updates are applicable to the add-on software packages provided on the MITSUBISHI ELECTRIC FA Global Website. Add-ons are updated via the add-on control screen in the engineering tool.

2.4.3.1. Precautions

- Check that the add-on version is correctly updated using the engineering tool after the update.
- To prevent illegal add-on installations by malicious third parties, it is strongly recommended that the user authentication function of the controller be enabled. When the user authentication function is enabled, user authentication of Administrator (administrator level) is required to operate the add-on install function.
- Download the add-on software package from the MITSUBISHI ELECTRIC FA Global Website. Do not use files obtained from other sources. Download the correct add-on software package according to the target model. Do not change the file name or data of the downloaded add-on software package.
- Periodically check for updates and perform update as necessary.
- Since the operations of all modules cannot be guaranteed during the installation, check that the controller and the system to be updated are stopped and that communication cables, wires, or others between the system and another system connected through the network are disconnected before the update.
- Check that there is no abnormality in the system operation before and after the update. If there is an abnormality after the update, restore the version before the update. To restore a version that is not published on the website, contact your local Mitsubishi Electric or our specified representatives.

2.4.4. User authentication function

The user authentication function restricts people (hereinafter referred to as “user”) that can access the controller. Using this function allows only the predetermined users to access the controller.

Users who need to access the controller must be authenticated with a user name and password.

Enabling the user authentication function can prevent information leakage due to access to the controller by unauthorized users and illegal operations of devices due to changes in settings.

2.4.4.1. Granting of operation authority to users

Operation authority to the controller can be granted to each authenticated user. Operation authority that can be set includes file access, memory access, device access, diagnosis, remote operation, and update, and is determined for each user group to which the user belongs. The following table shows three types of user groups. Note that the Administrators and Users groups are user groups that exist by default.

Table 11 User group

No.	User group name	Operation authority of user group
1	Administrators (Administrator group)	All the operations allowed for users can be performed. * The operation authority assigned to this group cannot be changed.
2	Users (User group)	Only data viewing such as file reading can be performed, and file writing cannot be performed. * The operation authority assigned to this group cannot be changed.
3	User-defined group	This group can be defined by a user, and the operation authority is set by the user. The user-defined group can be created by only users in the Administrators group.

Users set in the Administrators group are allowed to perform all operations on the controller. Therefore, be careful when managing users to be set in the Administrators group. When creating a user-defined group, it is recommended that minimum operation authority be granted according to the role of the group to be created.

Figure 9 shows the overview of the user authentication function. In Figure 9, user 1, user 2, and user 3 registered in the user group are correctly authenticated and allowed to access the controller. However, user 4, who is not registered in the user group, fails authentication and cannot access the controller.

Even for users who have successfully authenticated, available operations differ depending on the user group they belong to. For example, users belonging to the Administrators group can perform all operations, however, user 3, who belongs to the user-defined group that allows only the diagnosis function, can use only the diagnosis function.

If the user authentication function is not enabled, users who can connect to the controller are allowed to use all functions of the controller, which may lead to threats such as information leakage and illegal operations of devices. Enable the user authentication function and set the appropriate authority for each user.

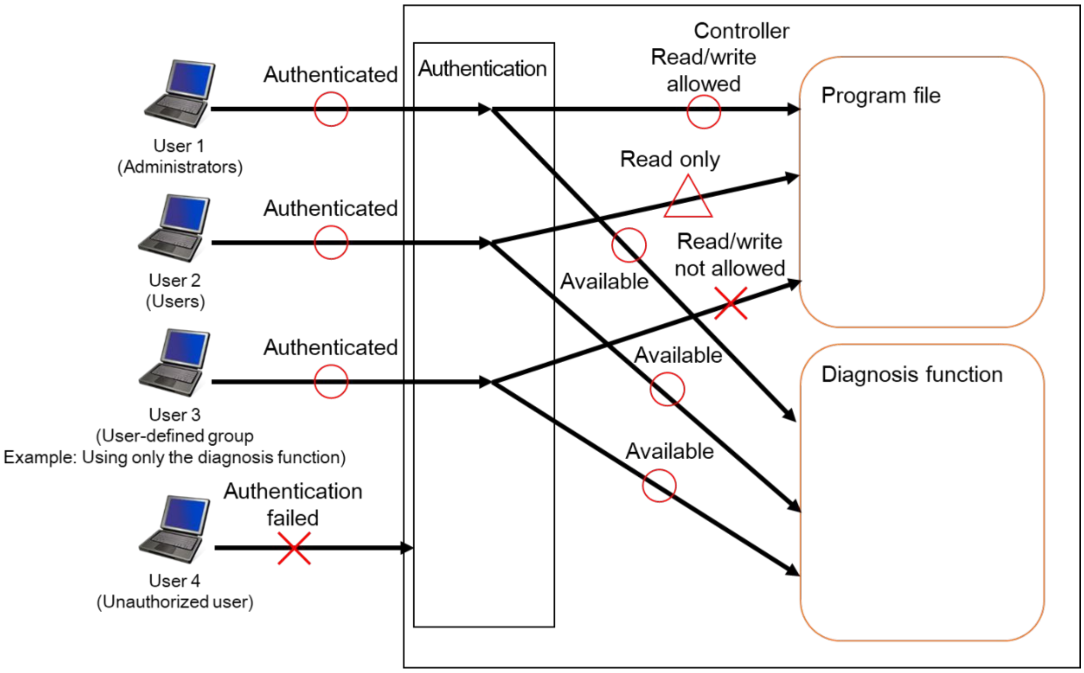


Figure 9 Overview of the user authentication function

2.4.4.2. Recommended settings

To use the controller in compliance with IEC 62443, set the user authentication function as follows.

- Enable the user authentication function.
  - ➢ Enable the user authentication function before setting and using other functions.
- Protect the network of a path for which user authentication is invalid (*).
  - ➢ Use a firewall or others to protect the network of a path for which user authentication is invalid.
- Set the user password strength to “Strong”.
- Enable the expiration date setting of the user password.
- Set the device/label access as the user authentication target in the user authentication out-of-target operation setting.

* Path for which user authentication is invalid

Note that if the user authentication function of the destination controller is disabled, the controller is accessible even if the authentication function of the relay controller is enabled.

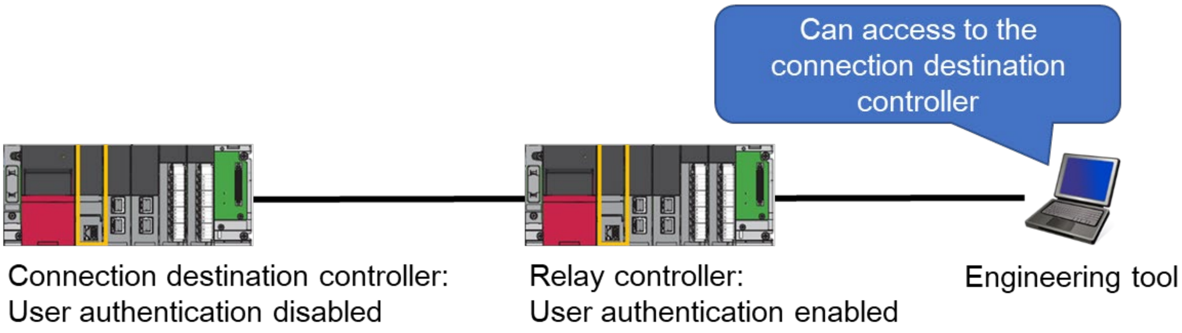

Can access to the connection destination controller
Connection destination controller: User authentication disabled
Relay controller: User authentication enabled
Engineering tool

Figure 10 Path for which user authentication is invalid

2.4.4.3. Precautions

The following shows the precautions on using this function.

- Note the following points regarding the password management.
  - Keep your password secret from others.
  - Do not use the same password repeatedly.
- Lockout of users
  - With the user authentication function, if a user fails the authentication continuously, he/she is locked out. The number of authentication failures before lockout and the lockout time can be changed from the settings.

    Users in the Administrators group can unlock other users who have been locked out. It is recommended that the lockout be released after confirming that the user who failed to log in is a legitimate user.
- Troubleshooting in case of password loss
  - If a user in a group other than the Administrators group loses the password

    Log in as a user in the Administrators group and reset the password for the user who has lost his/her password.
  - If a user in the Administrators group loses the password

    Log in as another user in the Administrators group and reset the password for the user who has lost his/her password.

    However, the password for users in the Administrators group can be reset only by themselves. If passwords for all the users in the group are lost, the user authentication function can be disabled by using the all information initialization function of the controller. Note that this operation deletes all the data saved in the controller.
- The user authentication function does not perform access control to files in an SD memory card. Therefore, do not store important data in the SD memory card.

2.4.5. Event history function

The event history function saves information, such as errors detected by a module, operations executed on a module, and errors occurred on the network, which was collected by the controller from each module, to a data memory or SD memory card. Information such as saved errors and operations can be checked with the engineering tools, and the history of occurrences can be checked in chronological order.

The event history function allows the investigation of the causes of malfunctions that have occurred in facilities/equipment and the detection of illegal access and operations.

When using the product in conformance with IEC62443-4-2, specify the data memory as the save destination for the event history.

2.4.5.1. Security events to watch for

Regarding the events obtained by the event history function, the following events are particularly useful for detecting illegal access and operations.

Table 12 Security events to watch for

No.	Event to watch for	Overview
1	Event related to user authentication	Logon failure events of users using the user authentication function and lockout events due to consecutive logon failures are useful for detecting access by unauthorized users.
2	Event related to file reading/writing	For events such as file access and file reading/writing, checking for access events in unusual patterns is useful for detecting illegal file access.
3	Event related to access control by communication path	Checking the access events from IP addresses whose access is restricted by the IP filter function is useful to detect access by unauthorized users.
4	Event history deletion event	If a deletion event in an unintended event history is recorded, the event history may be cleared for the purpose of clearing traces of the illegal access, for example.

2.4.6. Backup/restoration function of the controller

The backup function of the controller backs up all the data in the controller and device/label data including file registers to an SD memory card, file server, or folder on a personal computer.

The restoration function of the controller restores all the backed up data or device/label data, motion data, and others to the controller.

With these functions, data can be backed up at any timing and restored while the system is stopped.

It is recommended to select all target data in the setting of data to be backed up and the setting of data to be restored.

It is also recommended that the data in the controller be backed up periodically using the automatic backup function included in this function. This allows the system to be restored to the most recent state from the backup data in the event of a system malfunction.

2.4.6.1. Encryption of backup data

When this function is used, encryption of backup data can be set with an engineering tool. To use the controller in compliance with IEC 62443, perform encryption during backup.

Specify a password for encryption, and enter the password to restore encrypted data. If the password entered at the time of encryption setting is forgotten, the backup data encrypted with the password cannot be restored. Therefore, manage your password appropriately.

In addition, the encryption setting (“encrypt” or “do not encrypt”) is out of the restoration targets. To generate and encrypt backup data after restoration, set encryption again using the engineering tool.

2.4.6.2. Precautions

The following shows the precautions on using this function.

- If the restoration fails due to integrity verification failure, the backup data has been manipulated or rewritten. Do not use the backup data in question, but use other backup data.

2.4.7. Encrypted communication function

The encrypted communication function encrypts communication data when the controller communicates with an external device beyond the trust boundary.

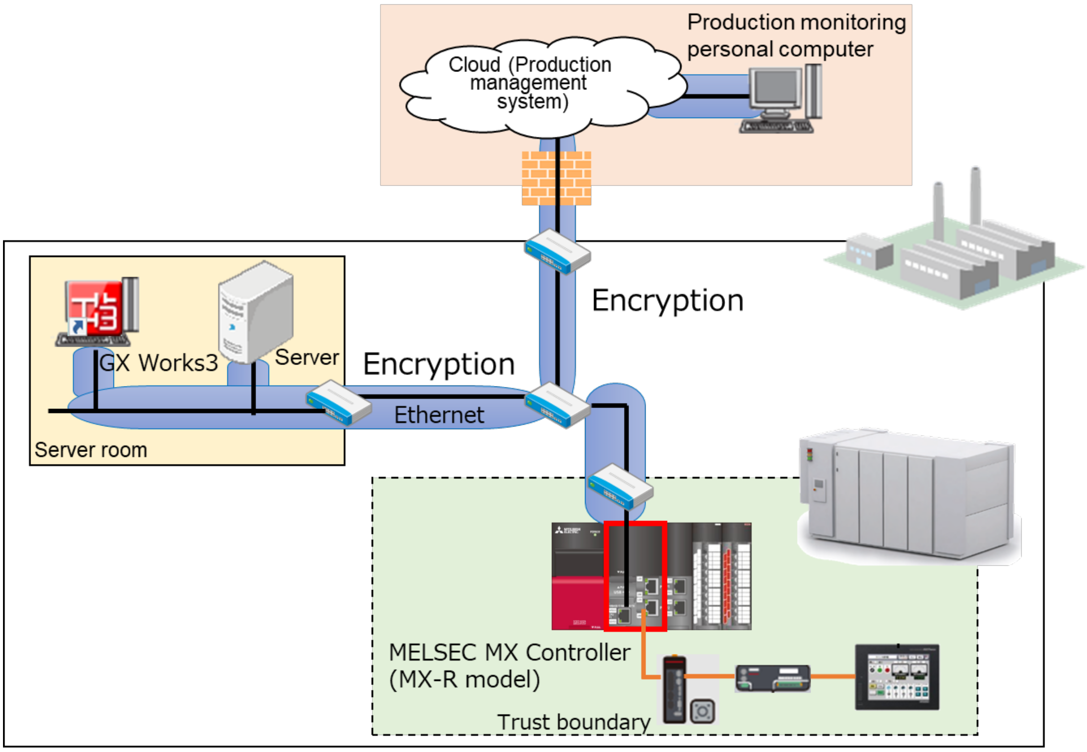

Production monitoring personal computer
Cloud (Production management system)
Encryption
GX Works3
Server
Encryption
Ethernet
Server room
MELSEC MX Controller (MX-R model)
Trust boundary

Figure 11 Overview of the encrypted communication function

2.4.7.1. Communication function to be encrypted

For the Ethernet functions built in the controller, the communication functions to be encrypted are shown in the following table.

Table 13 Communication function to be encrypted

No.	Communication function
1	Connection with MELSOFT products and GOT
2	Communication via SLMP
3	File transfer (FTPS server/client)
4	Communication via socket communication
5	OPC UA server

To use the controller in compliance with IEC 62443, encrypt the communication with external devices beyond the trust boundary. The encrypted communication can be performed only via the network ports built in the controller.

Encryption must be set with an engineering tool to perform encrypted communication. To protect the setting information of the encrypted communication, set the encrypted communication according to the connection method (USB connection or Ethernet connection) at the time of setting, as described in the procedure A below for USB connection and procedure B below for Ethernet connection. In addition, when the controller communicates with the external devices other than the engineering tool, follow the procedure C below after the settings described in A or B.

A) When connecting the controller to be set to the engineering tool via USB

- In the case of USB connection, the controller and the engineering tool are directly connected. Therefore, no threat of the setting information being eavesdropped or manipulated by an attacker is expected. Follow the steps to set the encrypted communication.

B) When connecting the controller to be set to the engineering tool via Ethernet

- In the case of communication beyond the trust boundary, the setting information may be eavesdropped or manipulated by an attacker. Therefore, set the encrypted communication between the engineering tool and the controller from inside the trust boundary.
- After completing the above settings, set the encrypted communication for other communication functions.

C) After completing the settings in A or B, set the encrypted communication with the external devices other than the engineering tool.

- The setting information of the encrypted communication is communicated in clear text to the external devices except for the engineering tool. Therefore, if the external device is this controller, it is recommended to set the encrypted communication via USB.
- If the external device is not this controller, set the encrypted communication using the method recommended by the manual of the external device.

* Communication available only within the trust boundary

When connecting the MELSEC MX Controller (MX-R model) and other devices for communication, use the communication shown below only within the trust boundary, and do not use it for communication with devices outside the trust boundary.

- Communication via USB
- Communication via CC-Link IE TSN port[11]
- Communication by FTP
- Communication by SNTP
- Communication by BACnet
- Communication by Modbus/TCP

*TLS/DTLS version

When using TLS or DTLS for encrypted communication, set the version to be the same as that of the communication partner.

[11] In this document, among the Ethernet ports mounted on the MELSEC MX Controller (MX-R model), the port with CC-Link IE TSN communication function is referred to as CC-Link IE TSN port.

2.4.7.2. Digital certificate used for encrypted communications

A digital certificate (hereinafter referred to as “certificate”) is data used to pass a key used for encrypted communications to the external device. If the certificate is not set correctly, encrypted communications with the external device cannot be performed. Perform the following procedure to create and write a certificate.

1) Creating a certificate
   - Create a certificate with an engineering tool. From the certificate management screen, select the controller for which the certificate is to be set, and enter the items necessary to create the certificate. The controller selected in this step is used as a server device.
   - Set the expiration date for the certificate. The expiration date is set to one year by default. To use the controller in compliance with IEC 62443, do not change the expiration date from the default setting.
2) Writing the certificate
   - From the certificate management screen of the engineering tool, select the controller to be set and write the certificate created in step 1). The controller selected in this step is used as a client device.

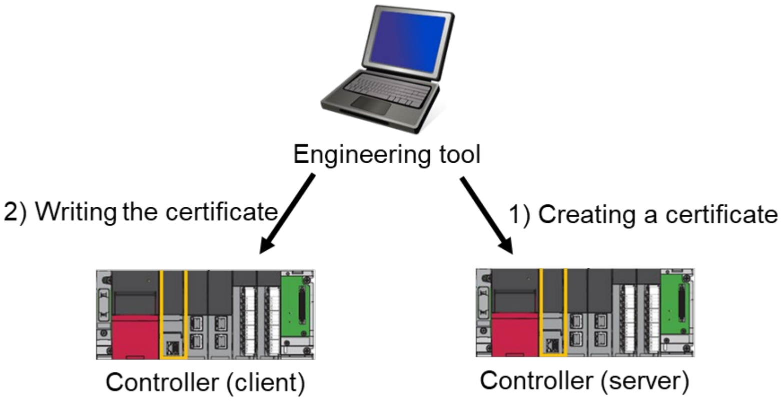


Figure 12 Setting procedure of a certificate

2.4.7.3. Precautions on a digital certificate

Note the following points regarding the certificate management.

- Set the correct time to the controller so that the expiration date setting of the certificate works correctly.
- Enable the user authentication to prevent illegal deletion or modification of certificate stored in the controller.
- If the expiration date set for the certificate expires, encrypted communications are no longer performed. Notification will be made via an error event and buffer memory when the expiration date is within 90 days and when the expiration date has expired. When a “within 90 days before certificate expiration” event occurs, renew the certificate by the day of expiration. The certificate can be renewed with the following procedure.
  1) Delete the target certificate.
  2) Create a new certificate.
  3) Set the created certificate for the client device.

2.4.8. IP filter function

An IP filter identifies the IP address of the access source, and prevents access from an illegal IP address. The IP address of the external device to be allowed or denied is set in the parameters, and access from external devices is restricted.

It is recommended that only the IP addresses of the external devices for which communication is permitted be allowed. In the following setting example, only the IP addresses of external device 1 and external device 2 are allowed.

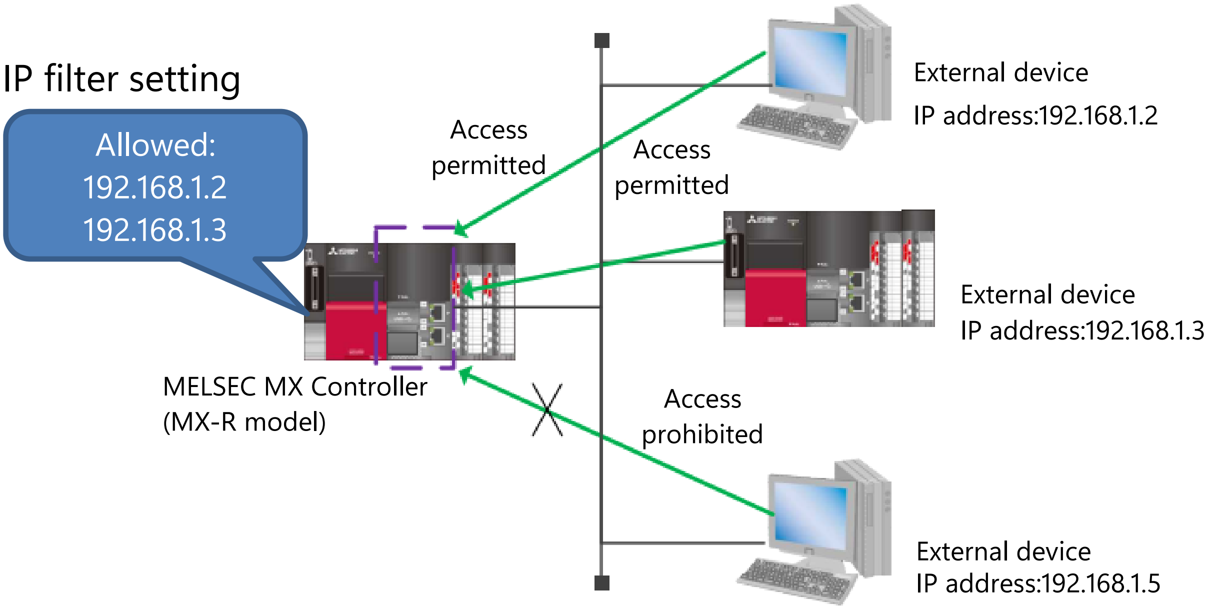


Figure 13 Access restriction by IP filter

2.4.8.1. Recommendations for using IP filters

- Use of the IP filter function is recommended when using in an environment connected to a LAN line.
- To use the controller in compliance with IEC 62443, use the IP filter function.
- If a proxy server exists on the LAN, block the IP address of the proxy server. If the IP address is allowed, access from a personal computer that has access to the proxy server cannot be prevented.
- To block access from an external device to another station, configure the IP filter settings for the connected station (the station directly connected to the external device).
- Even if communication settings such as SLMP, socket communication, or MELSOFT connection are configured, access will not be made if the target device is targeted for blocking by the IP filter.
- The IP filter function is one method of preventing illegal access from an external device. It does not completely prevent illegal access. Take measures other than the IP filter function to secure the controller and system against attacks such as illegal access from external devices in accordance with the concept of defense in depth.

2.4.9. Usage setting function of default open port

The usage setting function of default open port allows the controller to open/close the system ports that are open by default.

2.4.9.1. Concept of port open/close

Unused ports should be properly closed in accordance with the security policy. Leaving unused ports open gives attackers the information and means to attack. The following shows the examples of recommended open/close settings.

1) Communication inside the trust boundary
   - For the communication inside the trust boundary, close the unused ports.

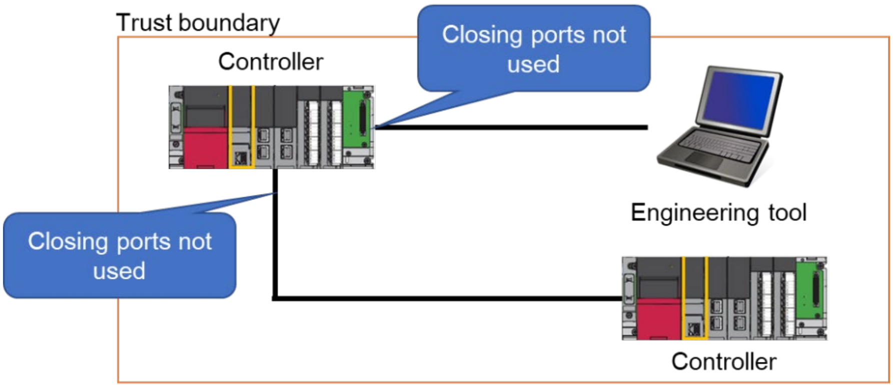


Figure 14 Example of port close setting within the trust boundary

2) Communication with the outside of the trust boundary

- For the communication with the outside of the trust boundary, use this function to close all the ports that are open by default. Perform the communication with the outside of the trust boundary using the encrypted communication function.

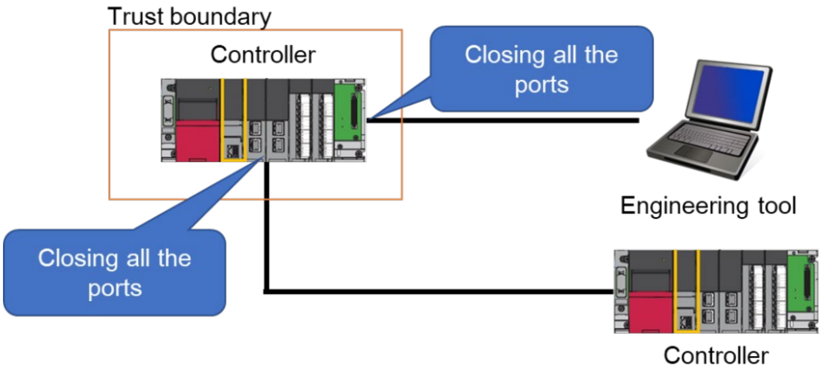


Figure 15 Example of port close setting outside the trust boundary

2.4.9.2. Precautions

The following shows the precautions on using this function.

- To use the controller in compliance with IEC 62443, set the unused ports as closed.
- To prevent illegal setting changes, enable the user authentication function before setting and operating this function.
- This function opens or closes the system ports that are open by default. Ports that the user has opened explicitly by setting parameters are out of the operation targets of this function.
- This function is one method of preventing illegal access from an external device. It does not completely prevent illegal access. Take measures other than this function to secure the controller and system against attacks such as illegal access from external devices in accordance with the concept of defense in depth.

2.4.10. Bandwidth limitation function against DoS attack

The bandwidth limitation against Dos attack limits the network bandwidth used by the controller. This function addresses “bandwidth consuming attack”, “system resource consuming attack”, and “attack that forces the security function to consume transmission bandwidth” by limiting the bandwidth used.

2.4.10.1. Recommendations for bandwidth limitation settings

When using this function, set the transmission bandwidth and reception bandwidth that can be used. Note the following items for the setting.

- To prevent illegal setting changes, enable the user authentication function before setting and operating this function.
- Regarding the determination of the bandwidth to be limited, the normal bandwidth used depends on the usage environment and system configuration. Therefore, when setting the bandwidth, check the normal communication bandwidth in the actual usage environment in advance and set an appropriate bandwidth.
- To use the controller in compliance with IEC 62443, use this function with the IP filter or usage setting function of default open port.

2.4.11. Operation setting

Operation setting is a function to set the operation of the MELSEC MX Controller (MX-R model) (stop/continue operation) when an error is detected in the module. The behavior of the MELSEC MX Controller (MX-R model) when an error is detected in each operation setting is as follows.

Table 14 Behavior of the MELSEC MX Controller (MX-R model) with operation setting

No.	Operation setting	Output	Behavior
1	Stop operation	Hold	The MELSEC MX Controller (MX-R model) stops operation when an error is detected and holds the output to the corresponding unit.
2	Continue operation	-	When the MELSEC MX Controller (MX-R model) detects an error, it executes a program other than the program (instruction) in which the error occurred.

When setting “Continue calculation”, be sure to verify the operation when an error occurs in advance and confirm that there are no problems.

2.5. Operation and maintenance of the MELSEC MX Controller (MX-R model)

2.5.1. Recommended operation example of the MELSEC MX Controller (MX-R model)

As physical security measures on the MELSEC MX Controller (MX-R model), restricting access to certain areas in the factory and installing the MELSEC MX Controller (MX-R model) in a secure location where it can be monitored (e.g., inside equipment or locked cabinet) are recommended to protect it from access by an unauthorized person and physical destruction. Applying the entry and exit management that allows only specific people to enter and exit the room is recommended by separating a room containing devices that manage the network and are critical to continue the operation of the control system from other areas.

The MELSEC MX Controller (MX-R model) communicates with a personal computer (maintenance personal computer or production management personal computer) via a network. By installing engineering software on a personal computer, the files stored in the MELSEC MX Controller (MX-R model) can be operated. To prevent these personal computers from being compromised, which causes files stored in the MELSEC MX Controller (MX-R model) to be leaked, or files that cause unintended behavior to be written to the module, taking the following security measures on personal computers that are connected to the MELSEC MX Controller (MX-R model) is recommended.

- Personal computer theft prevention measures using wire locks and others
- Access control for personal computer users
  - Allowing only authorized persons to log in to the personal computer
  - Strict management of login information
  - Introduction of fingerprint authentication
- Introduction of anti-virus software

To protect trust boundary where the MELSEC MX Controller (MX-R model) is installed or the network where personal computers are installed from external unauthorized access, installing network devices such as firewalls and routers at the boundary between the Internet and the factory network or outside the trust boundary is recommended. To communicate with the MELSEC MX Controller (MX-R model) from a personal computer located outside the trust boundary, set the port numbers set by the encrypted communication function in the permission list of the packet filter of the firewall on the route.

As a part of the continuous security operations in the factory where the MELSEC MX Controller (MX-R model) is installed, performing the check items related to each function as shown in Table 15 is recommended.

Table 15 Item to be checked for continuous security operations

No.	Function name	Check item
1	Backup	Back up the user programs/parameters/device values in an SD memory card in preparation for a product failure.
2	Checking the obtained logs	To detect suspicious behavior, checking the logs obtained with the event history function is useful. For example, the possibility of illegal access can be found by checking the log of failed login attempts or the access log to the USB port. Also, check the results of the security self-diagnostic function and take appropriate measures according to the operation manual.

No.	Function name	Check item
3	Checking the certificate	Check the expiration date of the certificate used for the encrypted communication function. If the certificate expires, communications will not be performed properly. Renew the certificate.

For using the MELSEC MX Controller (MX-R model), selecting an appropriate person as the administrator is recommended. It is recommended that users of the MELSEC MX Controller (MX-R model) receive adequate education and training to properly set, manage, and operate the product. Use the MELSEC MX Controller (MX-R model) appropriately in accordance with the operation manual and this guideline.

The files (customer's resources) stored in the SD memory card may be leaked if it is stolen. In addition, if an SD memory card containing an illegal file is inserted by a malicious third party, the control of the customer's facilities may be affected. For this reason, it is recommended that SD memory cards not be used whenever possible in environments where control panels or devices are not protected from unauthorized access to SD memory card slots. The following shows the functions that use an SD memory card and recommended alternative operation methods.

Table 16 Functions that use an SD memory card and recommended alternative operation methods

No.	Function	Recommended operation method
1	Event history function	Specify data memory as the save location of event history files.
2	File operation command (SP.FREAD and SP.FWRITE commands)	· For data input, use the device/label initial values instead of files. · For data output, use the latch device/label initial values instead of files.
3	Logging function	Specify the following as the storage location of logging setting files. · Data memory Specify either of the following as the save location of logging result files. · Data memory · Function memory
4	Latch function	Specify the built-in memory in the destination memory setting.
5	Boot function	Do not use the boot function. (Specify the built-in memory when writing data to the controller.)
6	Label access function from external devices	Store the data for label communication in data memory.
7	Device station parameter automatic setting function	Store the device station parameters in data memory.
8	Communication protocol support function	Store the module extension parameters in data memory. (Including the module extension parameters of other intelligent function modules)
9	User data write	Store the general-purpose files in data memory.
10	Backup/restoration function	Specify “encrypt” in the encryption setting to ensure safe backup/restoration from/to the SD memory card.

2.5.2. Periodic maintenance

Perform security maintenance periodically (at least once a year recommended) to secure your systems and controllers. Specifically, checking the normal operations of the functions listed in Table 17 is recommended. In addition, Table 18 lists the functions where the function settings affect security. Periodically check that these settings are correct as well.

Table 17 Operation verification item of the security function

No.	Function name	Check item
1	Initialization function of all information in the controller	After logon to a controller with program files, parameter files, and user authentication settings (security information) written with the Administrator authority, the initialization of all information shall succeed, the written files shall be deleted, and access shall be permitted without logon. * When the initialization function of all information in the controller is performed for this verification, all the program files, parameter files, and user authentication settings are initialized. Therefore, back up all the files (data) before verification.
2	Firmware update function via engineering tool	Firmware update using the firmware update information file for controllers shall succeed, and result in the intended firmware version.
		Firmware update using the firmware update information file for other than controllers shall fail and firmware version is not changed from the original version.
3	User authentication function	The user shall be able to log on only when the correct combination of the user name and password is entered.
		The user shall be locked out if an incorrect combination of the user name and password is entered multiple times.
		Operations shall be allowed only within the operation authority of the user group to which the logged on user belongs.
4	Event history function	Each event for which no filter settings have been made shall be saved in the event history.
		The occurrence date and time of the event stored in the event history shall be correct.
5	Backup function of controller	With an SD memory card inserted, a backup execution request operation shall succeed and a backup file shall be generated in the SD memory card.
6	Restoration function of controller	With an SD memory card containing the backup data for which a password is set inserted, the status at the time of backup shall be restored if the correct password is set and a restoration execution request operation is performed.
		With an SD memory card containing the backup data for which a password is set inserted, a decryption failure error shall occur if an invalid password is set and a restore execution request operation is performed.
7	Encrypted communication function	When encrypted communication is performed with a client device in which a certificate created by the target controller is imported, the “TLS/DTLS connection communication start/end” event shall be saved in the event history. *It is recommended to use a packet capture tool or others to check that the communication is performed using an expected protocol (TLS/DTLS).
		If a connection close request operation is performed during encrypted communication, the communication shall be stopped.
		When encrypted communication is performed with a client device in which a certificate created by a controller other than the target one is imported, the “communication by TLS/DTLS could not be performed successfully” error shall occur.

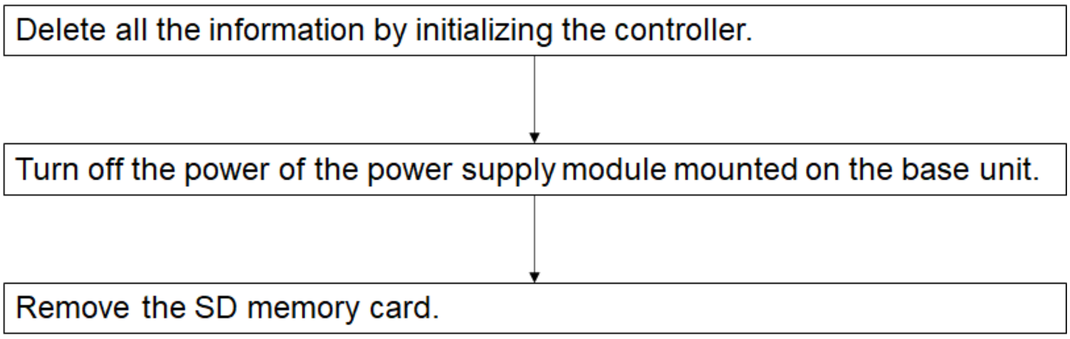
No.	Function name	Check item
8	IP filter function	When an IP address is set to be denied in the IP filter settings, communications from the set IP address shall be denied, and communications from other IP addresses shall not be denied.
		When an IP address is set to be allowed in the IP filter settings, communications from the set IP address shall not be denied, and communications from other IP addresses shall be denied.
9	Usage setting function of default open port	The port set as “closed” cannot be accessed.
10	Bandwidth limitation function against DoS attack	When packets below the threshold of the bandwidth setting are sent, no access restriction event shall occur.
		When packets above the threshold of the bandwidth setting are sent, an access restriction event shall occur.

Table 18 Setting check item of the security function

No.	Function name	Check item
1	User authentication function	Check the users who have access to the MELSEC MX Controller (MX-R model). If any unnecessary user accounts remain, delete them.
		Check the authorities granted to the account. If inappropriate authorities have been granted, remove them.
2	Usage setting function of default open port	Check which port is open. If a port which is not currently used is open, close the port.
3	IP filter function	Check the IP addresses that are allowed to communicate with the product. If access from an unintended IP address is allowed, block the access.

2.6. Removal and disposal of the MELSEC MX Controller (MX-R model)

Incorrect disposal or transfer may result in leakage of data remaining in the product. To prevent data leakage, follow the procedures below to remove and dispose of the product when you stop using it.



Delete all the information by initializing the controller.

Turn off the power of the power supply module mounted on the base unit.

Remove the SD memory card.

Figure 16 Removal method of the product

If the data needs to be backed up before deleted, use the backup function to make a backup.
The following shows the information to be deleted by the all information initialization function.

- Device/label
- File
- Setting information of security functions
- Event history
- Certificate information

Note that the contents in the SD memory card are not deleted by initialization of all controller information. When disposing of or transferring the controller, always remove the SD memory card and manage it properly. For the general precautions regarding disposal, refer to “Safety precautions” in the manual.
If the all information initialization function cannot be used due to malfunction or others, it is recommended that the product be crushed or magnetically destroyed before disposal so that confidential information cannot be read from it.

For the control stability of the entire factory and preservation of data stored in the system, shut down the MELSEC MX Controller (MX-R model) after the system is shut down with the appropriate procedures according to the operation manual.

When removing a device connected to a MELSEC MX Controller (MX-R model) in the system, the device may still have data that should be protected. Please remove it after taking measures such as deleting the data so that the information cannot be retrieved.

3. Contact information for security issues

We collect information on product vulnerabilities from external security researchers and coordinating bodies (such as domestic and foreign CERTs[12]) to improve the information security of our products. For information regarding product vulnerabilities, please contact such coordinating bodies or please contact Mitsubishi Electric through the contact form on the following website.

Mitsubishi Electric PSIRT
https://www.mitsubishielectric.com/en/psirt/contact/

[12] Computer Emergency Response Team

4. Q&A

[Q1]:

What kind of policies do the MELSEC programmable controllers of Mitsubishi Electric have for product security measures?

[A1]:

Our company adopts the following basic policies: “1) Compliance”, “2) Building organizations and systems to ensure safety and security”, “3) Promoting defense in depth in FA systems”, “4) Protection of MELSEC programmable controller in product life cycle”, and “5) Reduction of security risks in supply chain”. For details, refer to “2 Security Approaches of Mitsubishi Electric “ of “FA system security guideline”.

[Q2]:

Do the MELSEC programmable controllers of Mitsubishi Electric follow any security standards?

[A2]:

We will strive to provide products that comply with the international security standards for control systems (such as IEC 62443).

[Q3]:

How are cyber security measures taken for the MELSEC programmable controllers of Mitsubishi Electric?

[A3]:

As a company providing devices and services for promoting factory automation, we take the following measures based on the concept of international security standards (IEC 62443).

- Building organizations and systems in our company to ensure security
- Implementing security functions in products and creating security guidelines
- Protection of MELSEC programmable controllers in the production life cycle (planning, design, production, operation, and disposal)
- Security measures in the supply chain

For details of each item, refer to “3 Approaches on FA Cyber Preservation” of the “FA products security guideline”.

[Q4]:

What does Mitsubishi Electric do with the MELSEC programmable controllers to protect customers' system and data from security threats?

[A4]:

We are promoting general security measures based on four core policies described in [A3] as general for the MELSEC programmable controllers. For the MELSEC programmable controllers (programmable controllers and C controllers), we implement functions such as IP filter function, user authentication, and security key authentication to reduce the security risk of our customers. In addition, we implement measures to protect MELSEC programmable controllers from evolving attacks considering security in each phase (plan, design, manufacture, operate, and dispose) of the product life cycle.

For the security functions of MELSEC programmable controllers, refer to “2.2.4. Security functions in the MELSEC MX Controller (MX-R model) in this document. For the production life cycle, refer to "2.2.5 Implementing secure product life cycle"” of the “FA system security guideline”.

[Q5]:

How do I consider security measures for the factory?

[A5]:

The priorities of security measures vary depending on what do you need to protect and what kind of threats are possible in your factory. Refer to “3. Construction and Operation of a Secure FA System” of the “FA system security guideline” and “2.2.3. Policy on countermeasures against threats in this document to consider security measures according to your factory.

[Q6]:

What should I do with the external storage media (such as an SD card) before disposing the MELSEC programmable controller?

[A6]:

To prevent programs and recipe information from being removed, we recommend initializing the external storage media no longer needed to delete the stored information before disposal.

[Q7]:

What kind of measures does Mitsubishi Electric take for procurement of product parts and devices or the software (including updates) used in the design, development, and manufacturing processes?

[A7]:

In order to reduce risks associated with externally procured hardware and software, we raise security awareness by conducting on-site checks with our suppliers and providing guidelines, and we reduce vulnerabilities through incoming inspections. We also instruct our suppliers on how to prevent leakage of design information and programs related to our products, including security-related information.