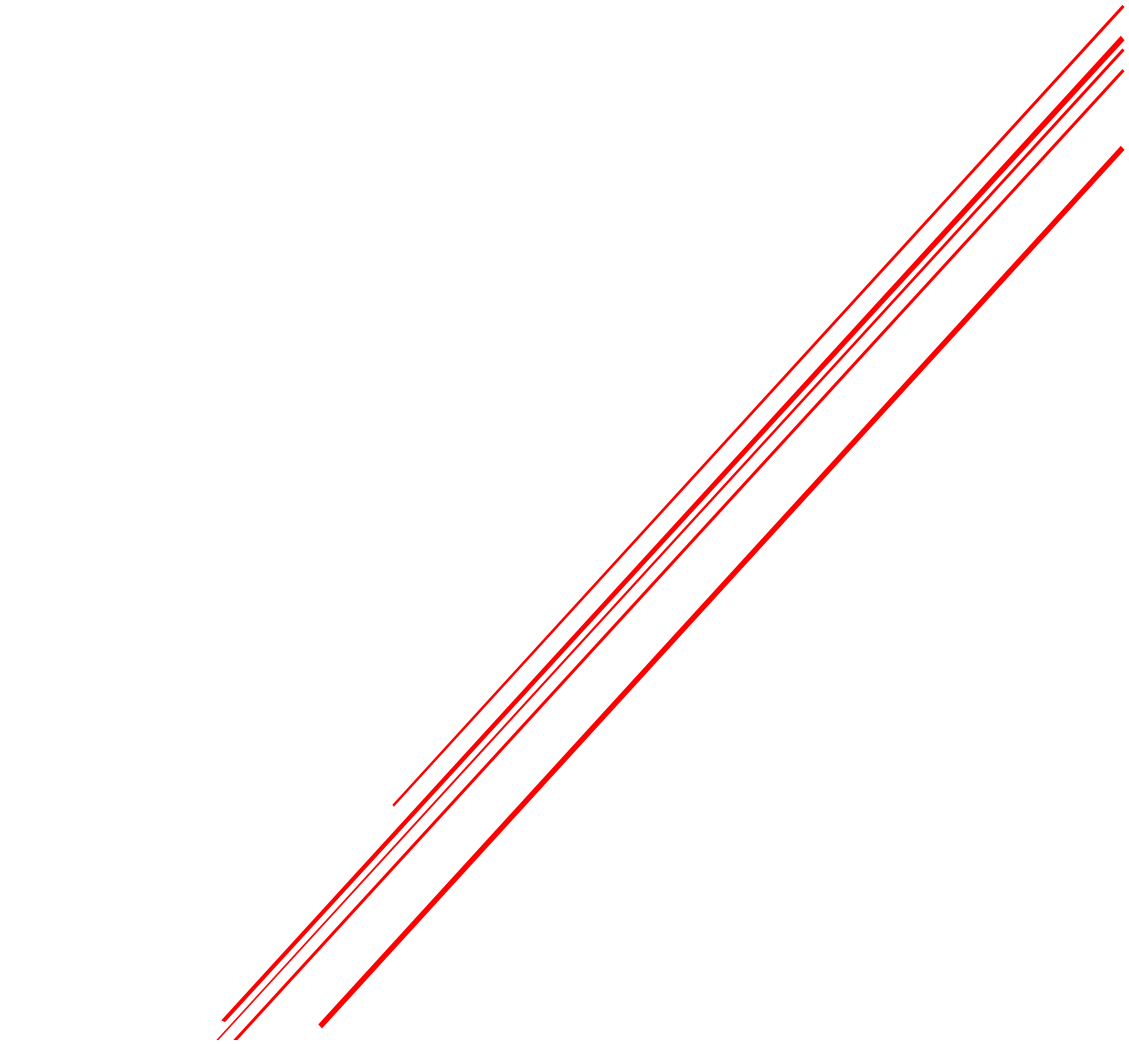
FA SYSTEM SECURITY GUIDELINE

- SEPARATE VOLUME [MELSEC] -



MITSUBISHI ELECTRIC CORPORATION

BCN-P5999-1474-E

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.
Oct. 2025	BCN-P5999-1474-C	MELSEC MX Controller MX-F model and CC-Link IE TSN Class A supported wireless LAN adapter are supported.
Apr. 2026	BCN-P5999-1474-D	The security specifications of the MELSEC MX Controller MX-R model have been updated.
Oct. 2026	BCN-P5999-1474-E	● MELSEC MX Controller MX-F model(with Safety Function) is supported. ● The security specifications of the MELSEC MX Controller MX-F model have been updated. ● MELSEC MX Controller MX-F model (Support EtherCAT) is supported. ● MELSEC MX Controller MX-R model (Support EtherCAT) is supported.

Contents

1. Introduction 1
   1.1. Background 1
   1.2. Defense in depth for protecting FA products 2
   1.3. Disclaimer 3
2. Security of the MELSEC MX Controller MX-R model 4
   2.1. Purpose of this chapter 4
   2.2. Policy on security measures for the MELSEC MX Controller MX-R model 5
      2.2.1. Expected usage environment of the MELSEC MX Controller MX-R model 5
      2.2.2. Threats to the MELSEC MX Controller MX-R model 8
      2.2.3. Policy on countermeasures against threats 9
      2.2.4. Security functions in the MELSEC MX Controller MX-R model 11
      2.2.5. Security measures to be taken outside the product 12
   2.3. Introduction of the MELSEC MX Controller MX-R model 13
      2.3.1. Installation and introduction procedures of the MELSEC MX Controller MX-R model 13
   2.4. How to set and use security functions and options 17
      2.4.1. Initialization of all controller information 17
      2.4.2. Firmware update function 18
      2.4.3. Add-on install function 19
      2.4.4. User authentication function 20
      2.4.5. Event history function 23
      2.4.6. Backup/restoration function of the controller 24
      2.4.7. Encrypted communication function 25
      2.4.8. IP filter function 28
      2.4.9. Usage setting function of default open port 29
      2.4.10. Bandwidth limitation function against DoS attack 31
      2.4.11. Operation setting function 31
   2.5. Operation and maintenance of the MELSEC MX Controller MX-R model 32
      2.5.1. Recommended operation example of the MELSEC MX Controller MX-R model 32
      2.5.2. Periodic maintenance 34
   2.6. Removal and disposal of the MELSEC MX Controller MX-R model 36
3. Security of the MELSEC MX Controller MX-F model 37
   3.1. Purpose of this chapter 37

3.2. Policy on security measures for the MELSEC MX Controller MX-F model 38
3.2.1. Expected usage environment of the MELSEC MX Controller MX-F model 38
3.2.2. Threats to the MELSEC MX Controller MX-F model 42
3.2.3. Policy on countermeasures against threats 43
3.2.4. Security functions in the MELSEC MX Controller MX-F model 45
3.2.5. Security measures to be taken outside the product 46
3.3. Introduction of the MELSEC MX Controller MX-F model 47
3.3.1. Setting and introduction procedures of the MELSEC MX Controller MX-F model 47
3.4. How to set and use security functions and options 51
3.4.1. Initialization function of all information in the controller 51
3.4.2. Firmware update function 52
3.4.3. Add-on install function 53
3.4.4. User authentication function 54
3.4.5. Event history function 57
3.4.6. Backup/restoration function of the controller 58
3.4.7. Encrypted communication function 59
3.4.8. IP filter function 62
3.4.9. Usage setting function of default open port 63
3.4.10. Bandwidth limitation function against DoS attack 65
3.4.11. Operation setting function 65
3.5. Operation and maintenance of the MELSEC MX Controller MX-F model 66
3.5.1. Recommended operation example of the MELSEC MX Controller MX-F model 66
3.5.2. Periodic maintenance 68
3.6. Removal and disposal of the MELSEC MX Controller MX-F model 70
4. Security of the CC-Link IE TSN Class A supported wireless LAN adapter by Mitsubishi Electric 71
4.1. Purpose of this chapter 71
4.2. Policy on security measures for the wireless LAN adapter 72
4.2.1. Expected usage environment of the wireless LAN adapter 73
4.2.2. Threats to the wireless LAN adapter 76
4.2.3. Policy on countermeasures against threats 77
4.2.4. Security functions in the wireless LAN adapter 80
4.2.5. Security measures to be taken outside the product 81
4.3. Introduction of the wireless LAN adapter 83
4.3.1. Installation and introduction procedures 83

4.4. How to set and use security functions and options 86
4.4.1. Wireless encryption mode 87
4.4.2. Wireless authentication mode 87
4.4.3. Wired LAN MAC address filter/wireless LAN MAC address filter 88
4.4.4. Stealth SSID 88
4.4.5. Password authentication 88
4.4.6. Logging function 88
4.4.7. Backup/restoration function 89
4.4.8. Initialization function 89
4.4.9. Firmware update function 90
4.5. Operation and maintenance of the wireless LAN adapter 91
4.5.1. Recommended operation example of the wireless LAN adapter 91
4.5.2. Periodic maintenance 92
4.6. Removal and disposal of the wireless LAN adapter 94
5. Contact information for security issues 95
6. Q&A 96

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.

[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)

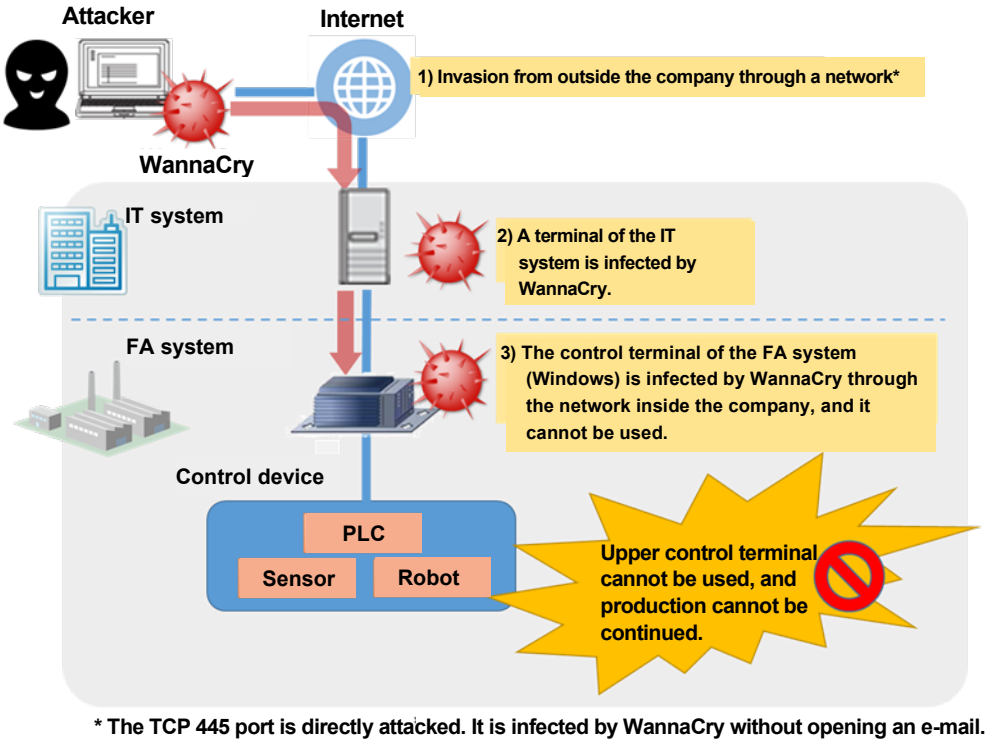


Figure 1 Example of WannaCry infection route and damage to FA system

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.

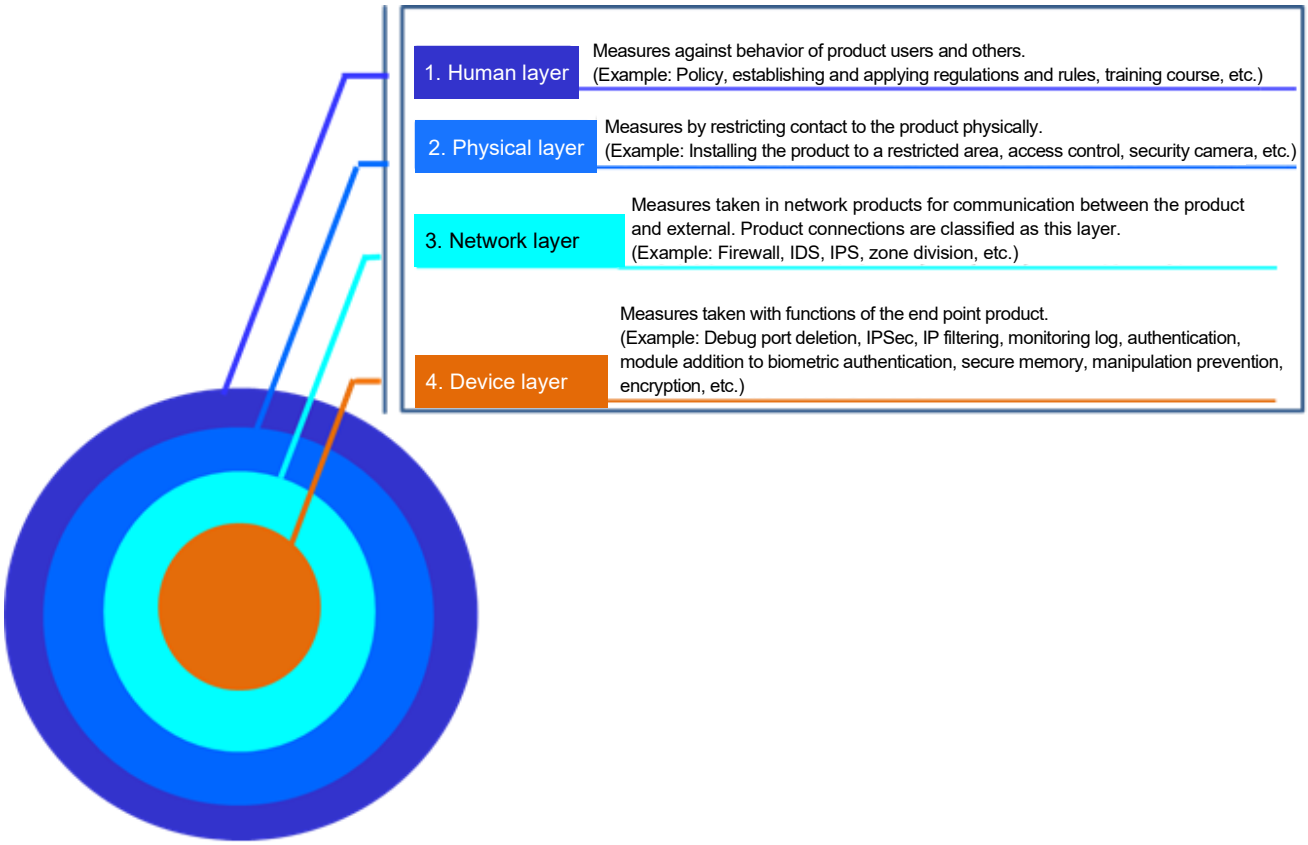


Figure 2 Concept of defense in depth

1.3. Disclaimer

Security-related information in this document is based on the results of our analysis and examination. Appropriate security measures differ depending on the customer's environment. Therefore, this document does not guarantee prevention of all security incidents that may occur in your environment.
Additionally, we recommend that you use the latest versions of firmware and software when using our products. Vulnerability countermeasures are implemented through product updates; thus, we will not be held responsible for any incidents or damages that arise due to the failure to perform updates.

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.

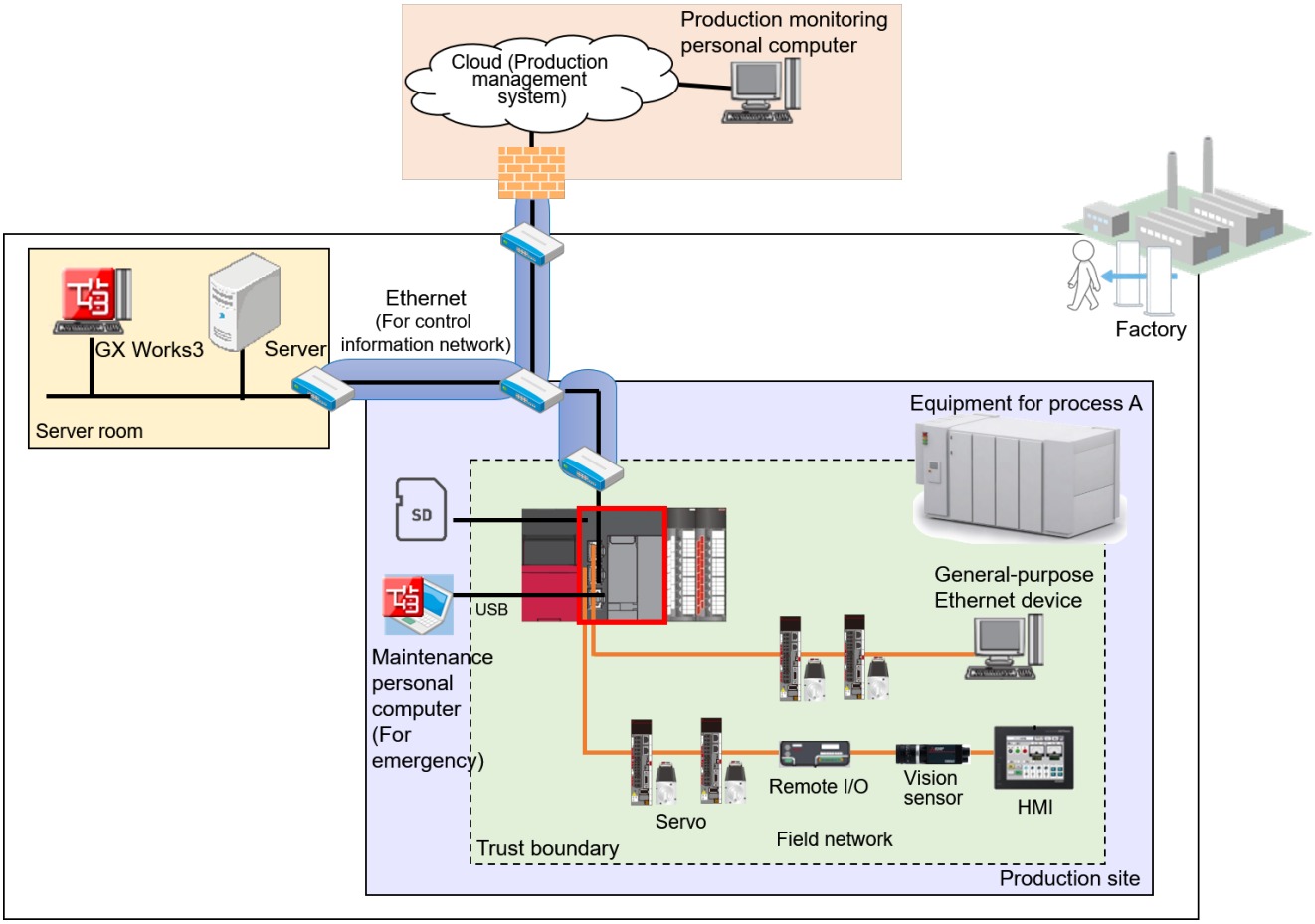
- Expected usage environment (installation environment, network, operation and maintenance, etc.) of the MELSEC MX Controller MX-R model
- Threats to the MELSEC MX Controller MX-R model
- Policy on countermeasures against threats
- Security functions in the MELSEC MX Controller MX-R model
- Security 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 premises 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 various field networks (such as CC-Link IE TSN and EtherCAT) are also installed in addition to the MELSEC MX Controller MX-R models, which means that this equipment is the trust boundary[9]. SD memory 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 a user 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.



* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

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 memory card	An SD memory 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 firewalls	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: GOT
2	Production monitoring personal computer	A device with software for monitoring the status of the control system installed. Examples of Mitsubishi Electric software used for status monitoring: MC Works64 and GX Works3
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. Examples of field network: CC-Link IE TSN and EtherCAT
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 TCP/IP communication
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
10	Server	A server that responds to inquiries from the MELSEC MX Controller MX-R model and stores data. Examples of servers: FTP server, SNTP server, DNS server

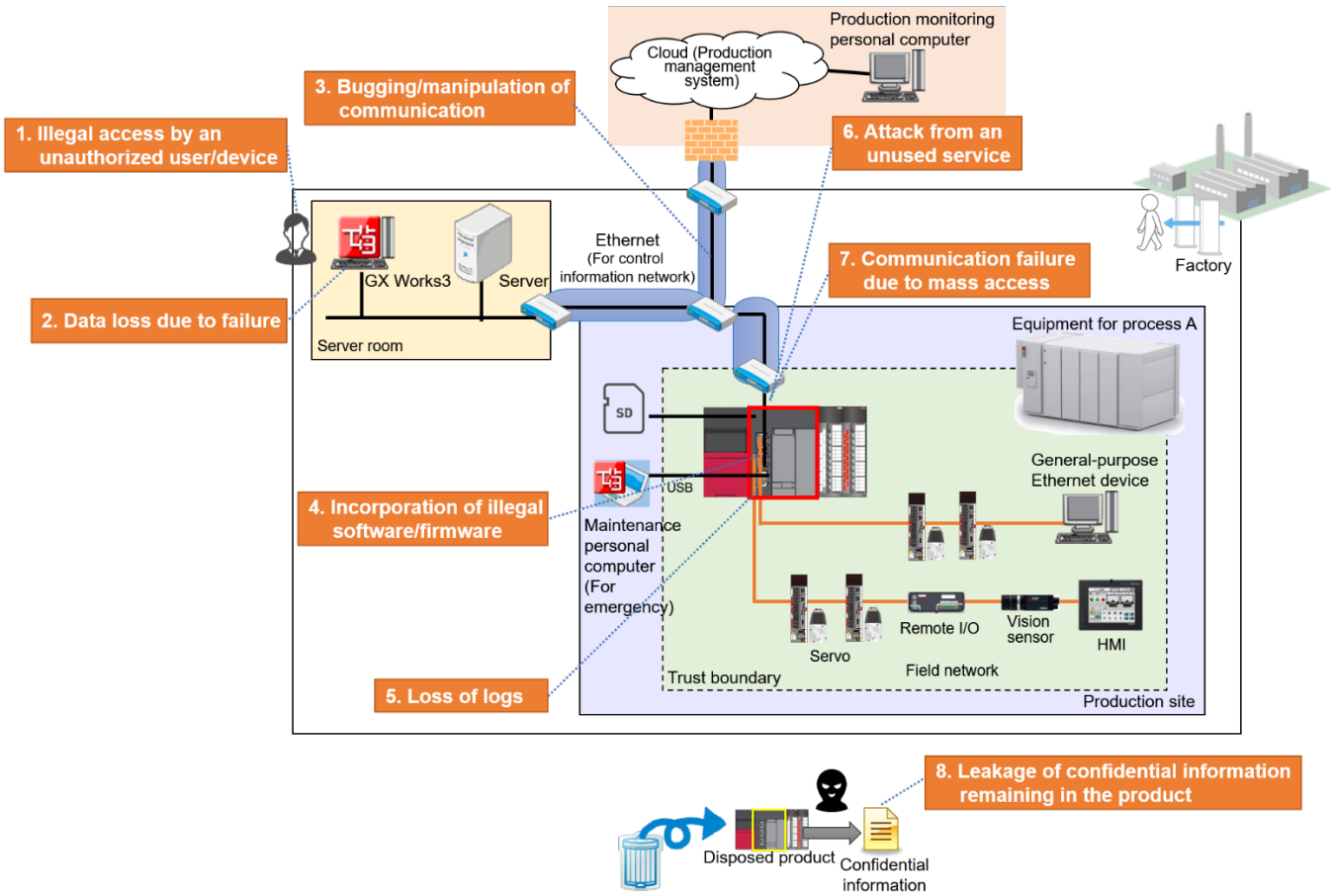
Access to devices can be physically controlled by restricting entry to individual areas of the factory or by applying physical locks to the device storage areas. These physical access controls are also important security elements. For the use of the MELSEC MX Controller MX-R model, the area classification 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 continuing 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 with locks).
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.



* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

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

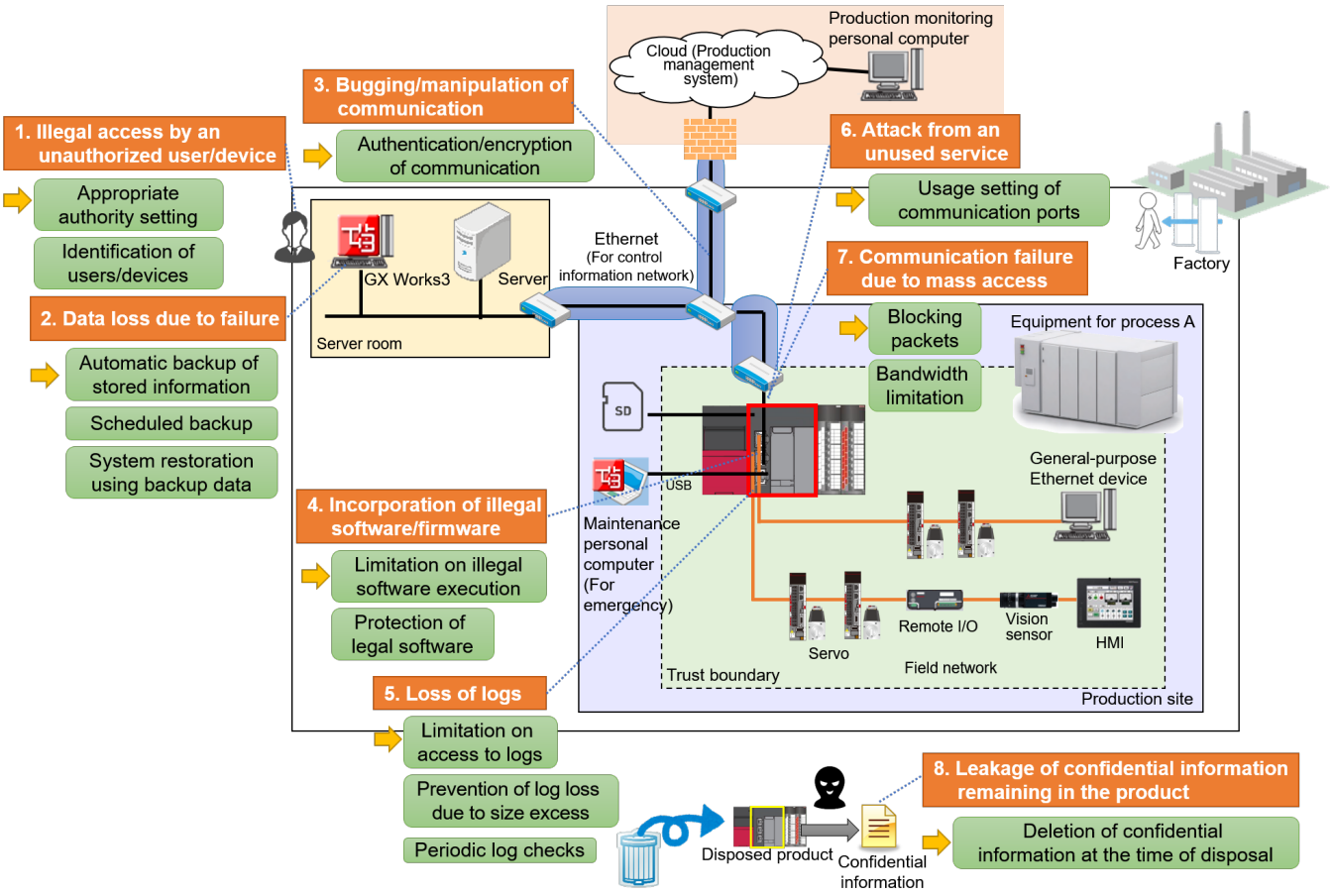
Table 4 Description of threats

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.



* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

Figure 5 Policy on countermeasures against threats to the MELSEC MX Controller MX-R model

Table 5 Policy on countermeasures against threats to the MELSEC MX Controller MX-R model

No.	Threat name	Policy on countermeasures	Related security functions/measures of the MELSEC MX Controller MX-R model	Reference for setting method for the security function
1	Illegal access by an unauthorized user	● Appropriate authority setting ● User identification	◆ User authentication function ■ Physical access restriction ■ Selection of the administrator ■ Installation of firewalls ■ 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 firewalls ■ 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 of all controller information

♦ marks indicate security functions implemented in the MELSEC MX Controller MX-R model.

■ marks indicate security measures to be taken in the customer's environment.

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

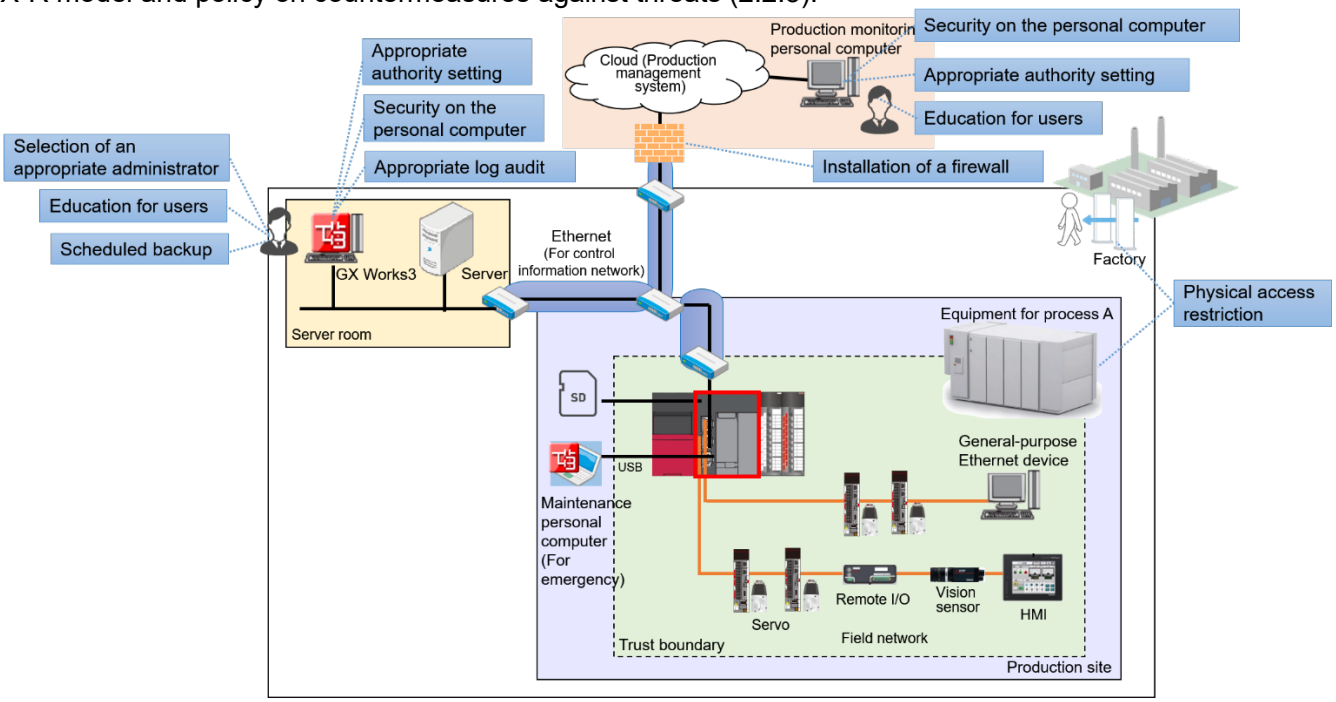
The MELSEC MX Controller MX-R model implements the security functions as described in Table 6 to realize the policy on countermeasures against threats described in 2.2.3.

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

Function name	Description	Target 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 controller.	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 threats (2.2.3).



* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

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
Network layer	Installation of firewalls or VPN	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 monitoring 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. Installation 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 (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.

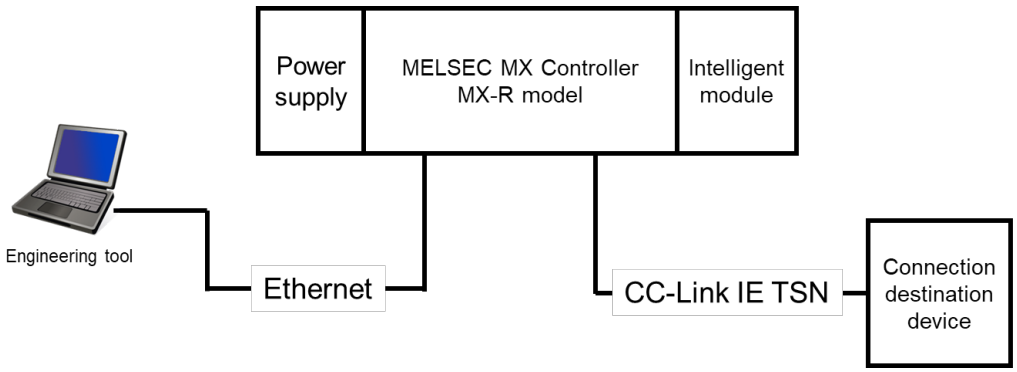


Figure 7 System configuration example

Connect the personal computer with the engineering tool installed to the MELSEC MX Controller MX-R model and perform the settings.

For the engineering tool compatible with the MELSEC MX Controller MX-R models, refer to the following manuals.

- MELSEC MX Controller MX-R Model User's Manual

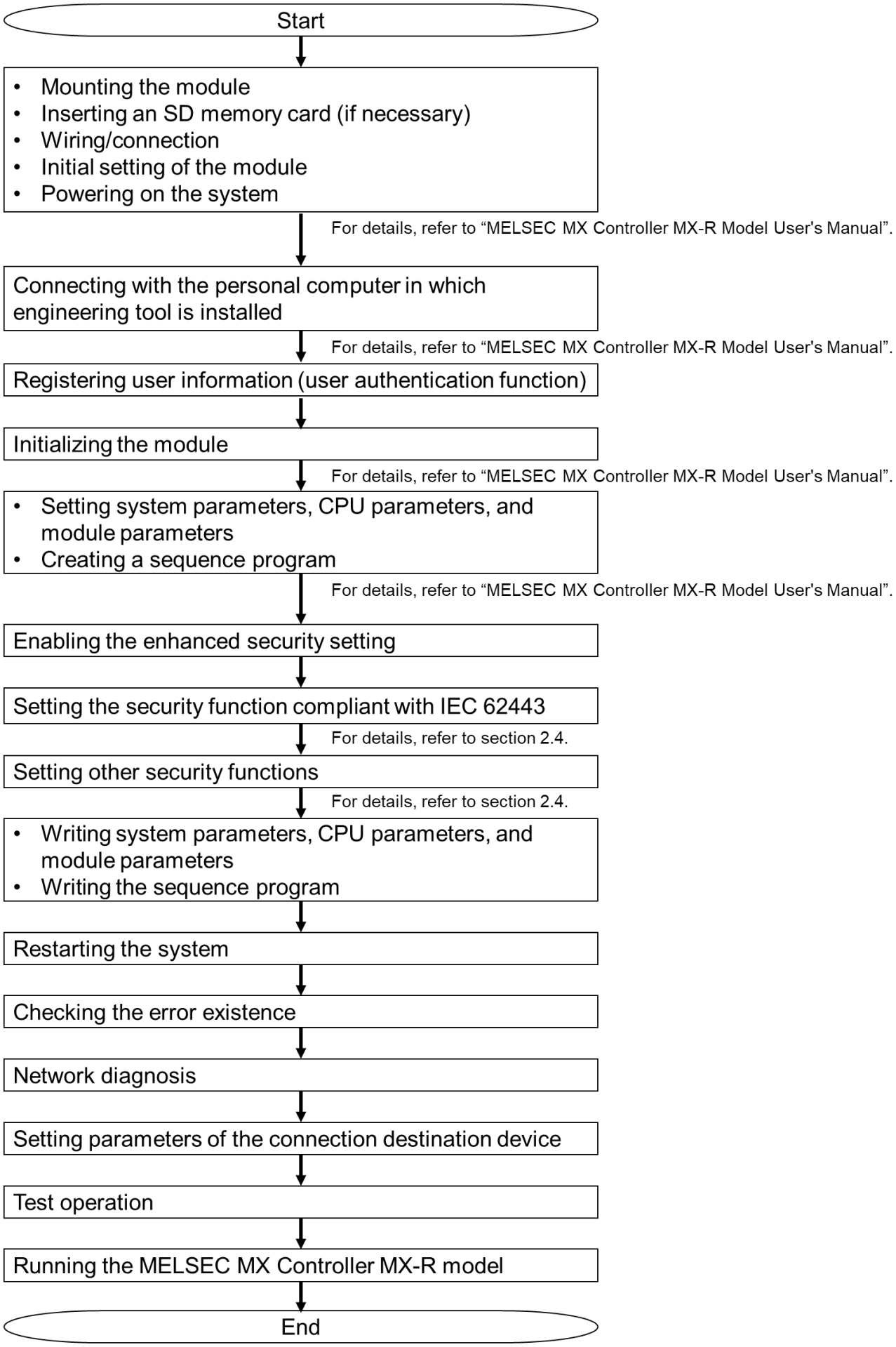


Figure 8 Procedure before operation

• 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 8 Setting for the security function compliant with IEC 62443

No.	Item	Setting for the security function	Reference
1	User authentication function	The user authentication function shall be enabled before setting and operating the encrypted communication function, IP filter function, 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 function	Appropriate storage size of the event history shall be set.	2.4.5
10		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
11		Correct time shall be set so that the time stamps are recorded correctly.	2.4.5
12		The manipulation check function for event history shall be enabled.	2.4.5
13	Backup/restoration function	Encryption setting of backup data shall be performed.	2.4.6.1
14	Encrypted communication function	Communications with external devices beyond the trust boundary shall be encrypted.	2.4.7
15		Communications that require encryption shall be performed in the Ethernet ports built in the MELSEC MX Controller MX-R model.	2.4.7.1
16		The expiration date of the certificate used for encrypted communications shall be set to one year (default setting).	2.4.7.2
17	IP filter function	Accesses from external devices shall be restricted with the IP filter.	2.4.8
18	Usage setting function of default open port	Unused ports shall be set as closed.	2.4.9.1
19		Communications with the outside of the trust boundary shall be performed using the Ethernet ports built in the MELSEC MX Controller MX-R model.	2.4.9

No.	Item	Setting for the security function	Reference
20	Bandwidth limitation function against DoS attack	The bandwidth limitation function against DoS attack shall be set.	2.4.10
21	Bandwidth limitation function against DoS attack, IP filter function, 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 function, usage setting function of default open port, and bandwidth limitation function against DoS attack.	2.4.10.1

Table 9 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. Take measures such as deleting the data before disposing of the device.	2.6
2	Connected devices	Verify prior to use that equipment connected to the MELSEC MX Controller MX-R model is configured and operating 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		Check that the MELSEC MX Controller MX-R model is communicating with the intended devices and not communicating with any unintended devices within the usage environment.	-
5	Use of SD memory card	Use the SD memory card only for backup/restoration, and do not store any data other than backup data.	2.5.1
6	Performance and management of 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 sudden disaster or failure, etc., perform regular backups and manage the backup data appropriately.	2.4.6 2.5
7	Password management	Passwords shall be properly managed to prevent leakage and shall not be reused.	2.4.4
8	Trust boundary	In the following cases, the Web server function shall be used only within a trust boundary. • SNTP, FTP, BACnet, Modbus, and HTTP communications • Connections with other devices using USB ports, CC-Link IE TSN ports, EtherCAT ports, and network drives	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 and 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 of all controller information (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 of all controller information

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 or in the event history 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 updates 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 Management screen in the engineering tool.

2.4.3.1. Precautions

The following shows the precautions on using this function.

- 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 updates 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 10 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	The operation authority can be determined by users. 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 the 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.

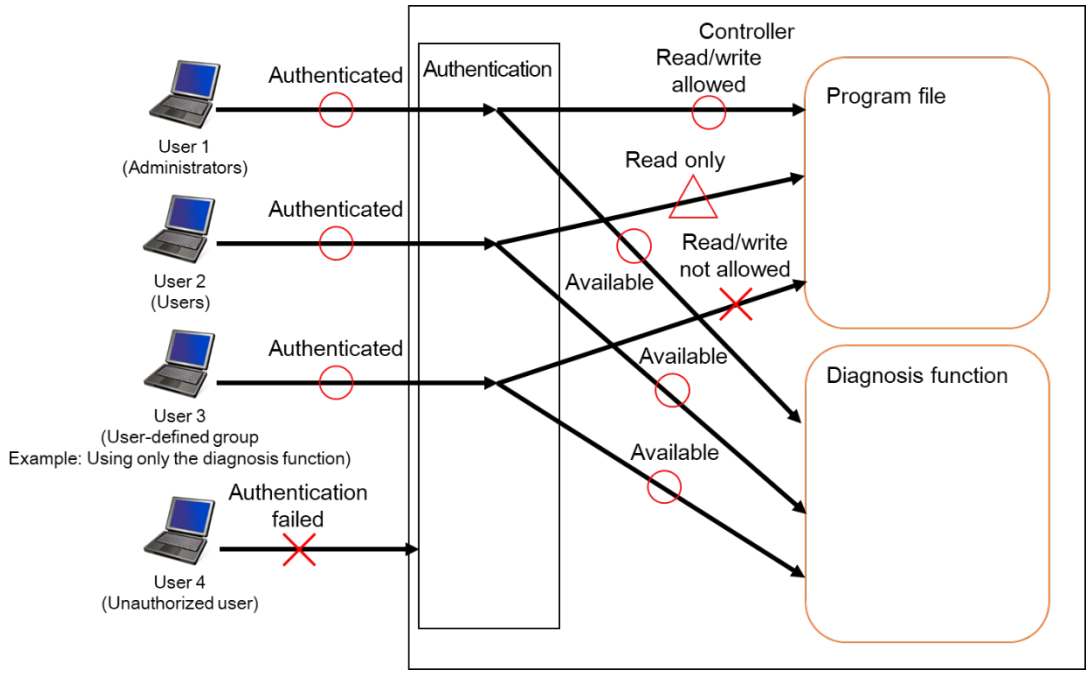


Figure 9 Overview of the user authentication function

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 Operation Setting Other Than User Authentication Target.

* 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.

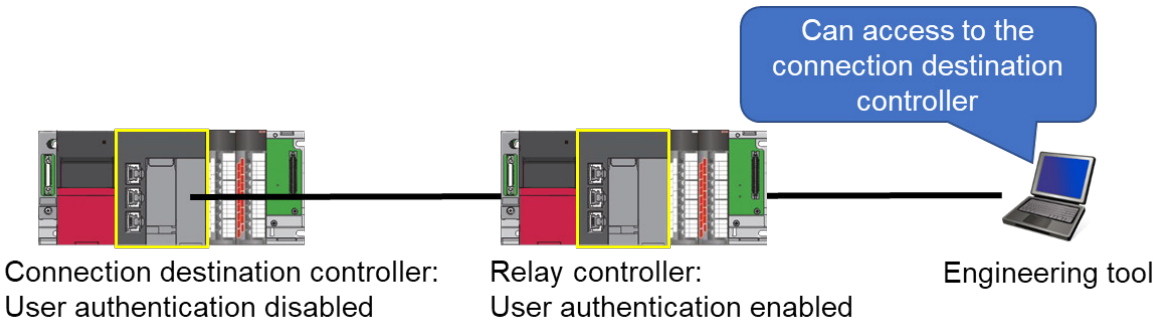


Figure 10 Path for which user authentication is invalid

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 all information initialization 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 that 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 IEC 62443, 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 11 Security events to watch for

No.	Event to watch for	Overview
1	Event related to user authentication	Checking the following is useful for detecting access by unauthorized users. ● Logon failure events of users using the user authentication function ● Lockout events due to consecutive logon failures
2	Event related to file reading/writing	Checking the following is useful for detecting illegal file access. ● Access events such as file access and file reading/writing in unusual patterns
3	Event related to access control by communication path	Checking the following is useful for detecting access by unauthorized users. ● Access events from IP addresses whose access is restricted by the IP filter function
4	Event history deletion event	Checking the following is useful for detecting illegal access. ● A deletion event of an unintended event history which may have been performed for the purpose of clearing traces of the illegal access

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.

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.

2.4.6.3. Recommendations for using backup/restoration

- 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.

2.4.7. Encrypted communication function

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

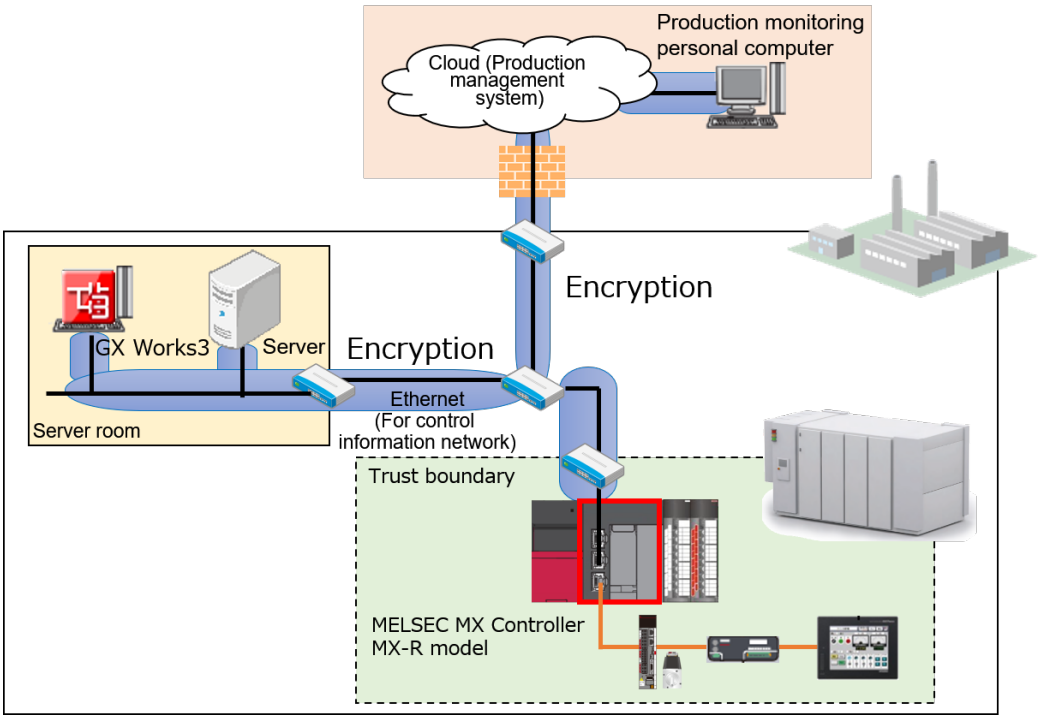


Figure 11 Encrypted communication function

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 12 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
6	Communication via the Web server function

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 Ethernet 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 plaintext 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 via FTP
- Communication via SNTP
- Communication via BACnet
- Communication via Modbus/TCP
- Communication via HTTP
- Communication with a network drive
- Communication using EtherCAT ports

*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 guideline, among the Ethernet ports mounted on the MELSEC MX Controller MX-R model, the port with the CC-Link IE TSN communication function is referred to as a 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.

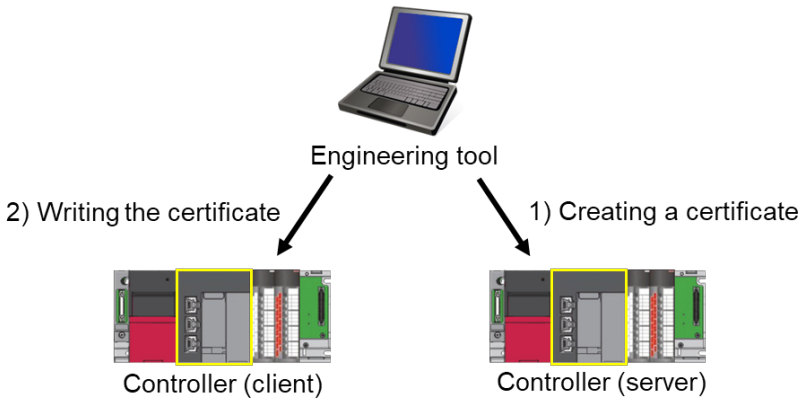


Figure 12 Setting procedure of a certificate

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 function to prevent illegal deletion or modification of the 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

This function identifies the IP address of the access source, and prevents access from an illegal IP address. By setting the IP address of the external device to be allowed or denied in the parameters, 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.

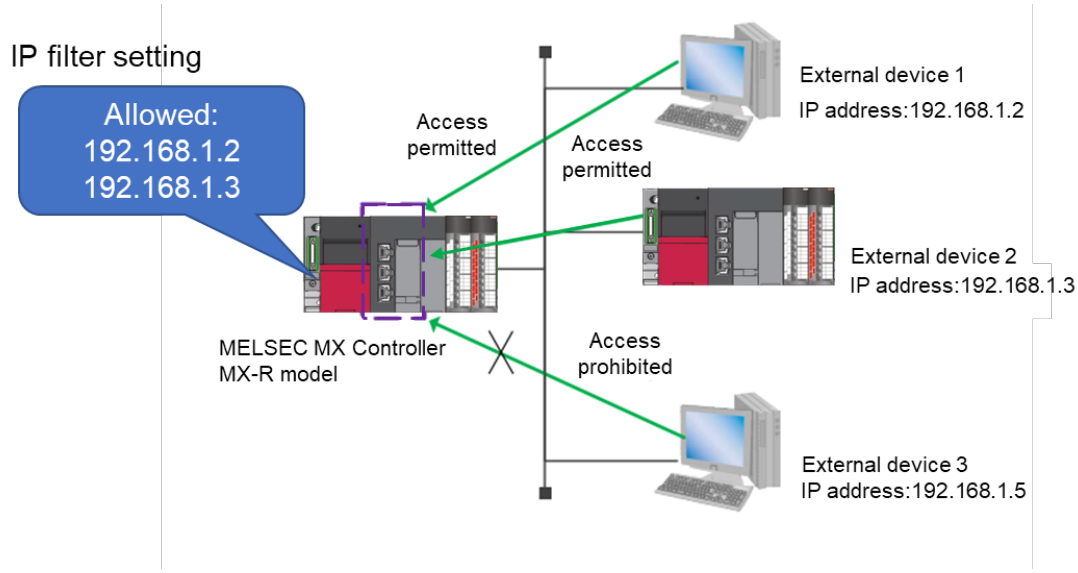


Figure 13 Access restriction by IP filter

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.

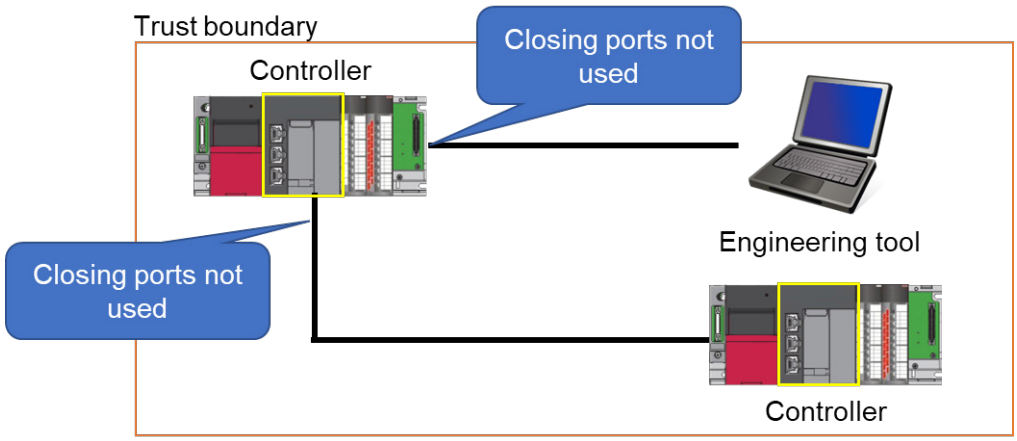


Figure 14 Example of port close setting within the trust boundary

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.

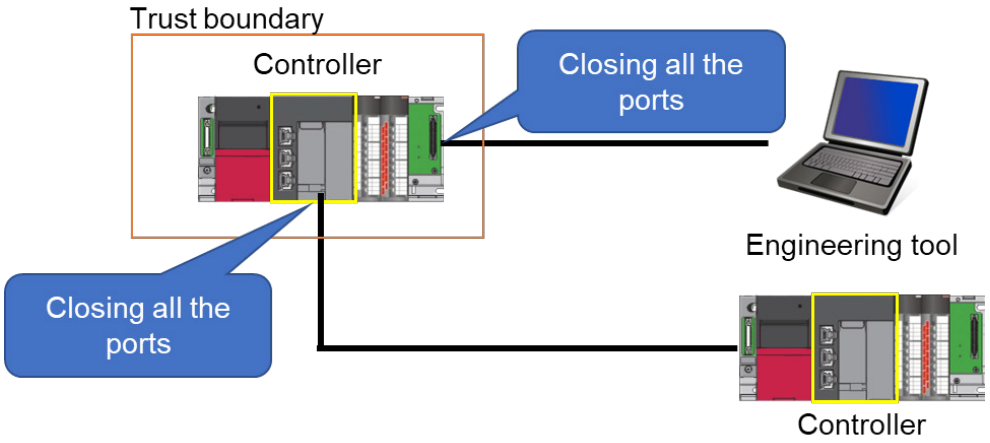


Figure 15 Example of port close setting outside the trust boundary

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 with the engineering tool. 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 function

The operation setting function 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 13 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 immediately upon detecting an error and maintains the last confirmed normal state of external outputs.
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.

2.4.11.1. Precautions

The following shows the precautions on using this function.

- 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 monitoring 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 14 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	Check the logs obtained with the event history function to detect the possibility of illegal access and suspicious behavior (such as log of failed login attempts or the access log to the USB port). Check the results of the security self-diagnostic function and take appropriate measures according to the operation manual.
3	Checking the certificate	If the certificate used for the encrypted communication expires, communications will not be performed properly. Regularly check the expiration date and renew it.

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

No.	Function	Recommended operation method
1	Event history function	Specify the data memory as the save destination for 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 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 destination for the 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 16 Operation verification item of the security function

No.	Function name	Check item
1	Initialization of all controller information (*1)	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.
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 restoration 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. (*2)
		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.
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.

No.	Function name	Check item
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.

*1 When the initialization of all controller information 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 It is recommended to use a packet capture tool or others to check that the communication is performed using an expected protocol (TLS/DTLS).

Table 17 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 from the IP address.

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 procedure below to remove and dispose of the product when you stop using it.

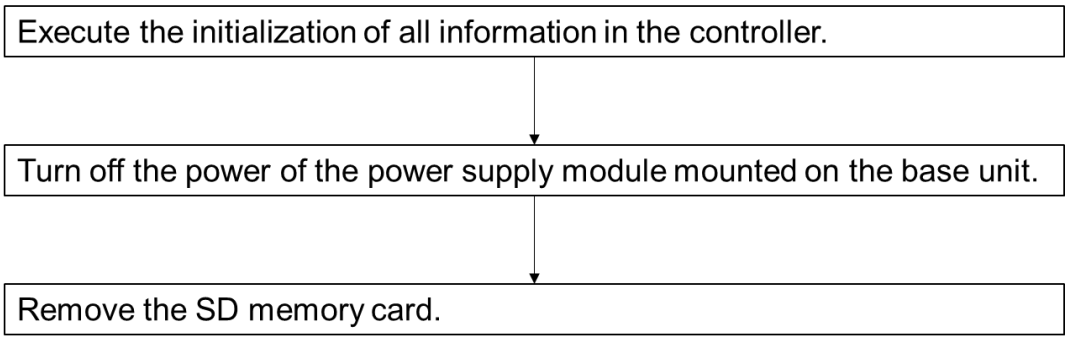


Figure 16 Removal method of the product

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 all information initialization.

- 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 all information initialization 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, there is a possibility that protected assets are stored in that device. Take measures such as deleting the data before removing it so that the information cannot be retrieved.

3. Security of the MELSEC MX Controller MX-F model

3.1. Purpose of this chapter

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

- Policy on security measures for the MELSEC MX Controller MX-F model (Section 3.2):
  This section describes the policy on security measures against threats by identifying possible threats to the MELSEC MX Controller MX-F model. Some countermeasures are performed by the MELSEC MX Controller MX-F model alone while others are performed in combination with other products.
- Introduction method of the MELSEC MX Controller MX-F model (Section 3.3 and 3.4):
  These sections describe the security functions of the MELSEC MX Controller MX-F model, how to set them, and how to install the MELSEC MX Controller MX-F model in an FA system.
- Operation and maintenance method of the MELSEC MX Controller MX-F model (Section 3.5):
  This section describes recommendations on how to manage users and passwords for operating the MELSEC MX Controller MX-F model.
- Removal and disposal method of the MELSEC MX Controller MX-F model (Section 3.6):
  This section describes the recommended methods (e.g., product data deletion functions) for removing and disposing of the MELSEC MX Controller MX-F model.

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

- ◆ MELSEC MX Controller MX-F model User's Manual
- ◆ MELSEC MX Controller MX-F model(with Safety Function) User's Manual

* The MELSEC MX Controller MX-F models include the following models, each supporting different functions.

- MELSEC MX Controller MX-F Model (Support CC-Link IE TSN)
- MELSEC MX Controller MX-F Model (with Safety Functions)
- MELSEC MX Controller MX-F Model (Support EtherCAT)

Read this guideline and the above related manual carefully to fully understand the security of the MELSEC MX Controller MX-F 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-F model, product life cycle initiatives, and examples of FA system construction.

- ◆ FA SYSTEM SECURITY GUIDELINE

3.2. Policy on security measures for the MELSEC MX Controller MX-F model

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

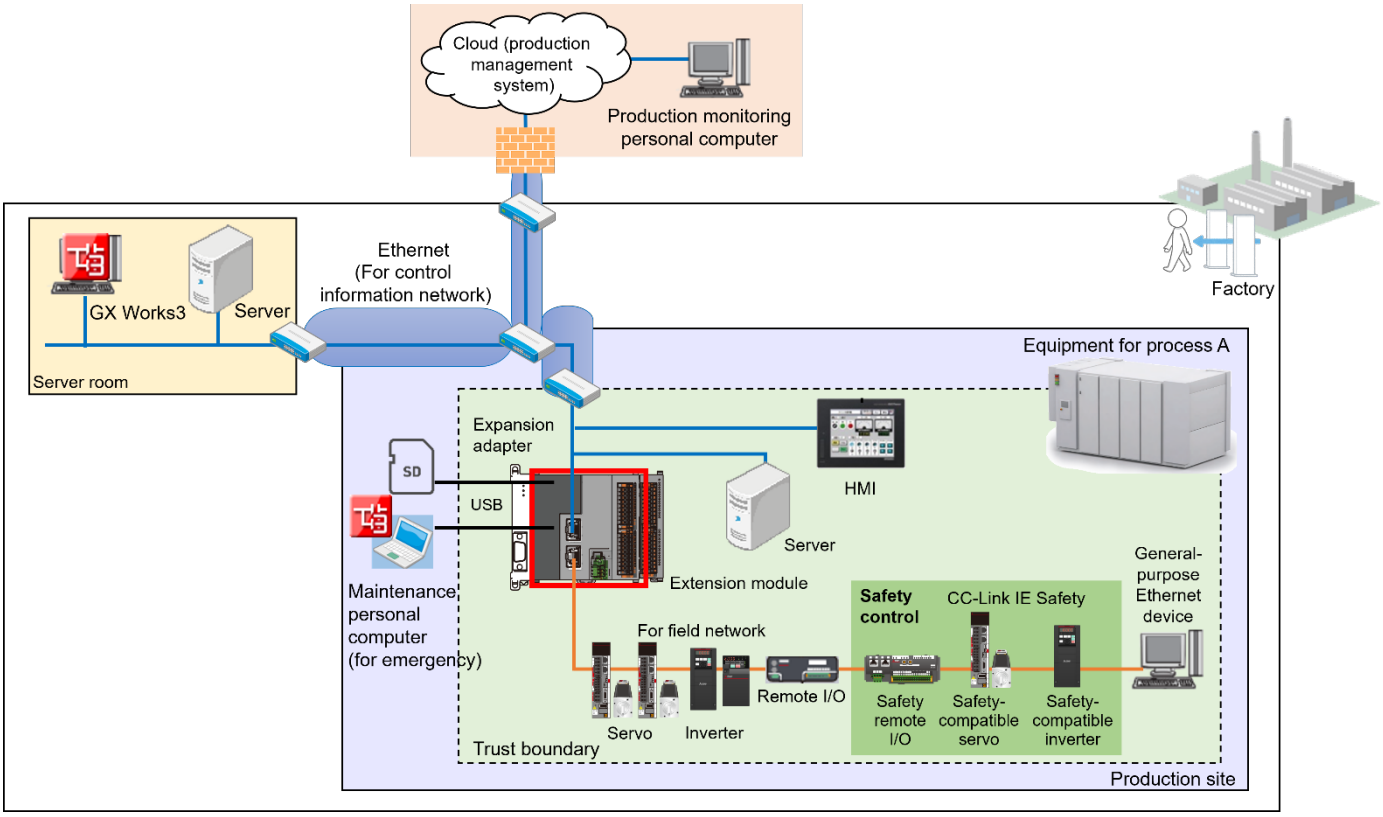
- Expected usage environment (installation environment, network, operation and maintenance, etc.) of the MELSEC MX Controller MX-F model
- Threats to the MELSEC MX Controller MX-F model
- Policy on countermeasures against threats
- Security functions in the MELSEC MX Controller MX-F model
- Security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

3.2.1. Expected usage environment of the MELSEC MX Controller MX-F model

Figure 17 shows the environment where the MELSEC MX Controller MX-F model is expected to be installed. Table 19 shows the prerequisites for ensuring security in the installation environment shown in Figure 17. These installation environment and usage environment including prerequisites are the premises for the policy on security measures described in the subsequent sections.

The MELSEC MX Controller MX-F model is intended for use in equipment to be installed on a production site in a factory. In this equipment, expansion adapters for expanding functions, extension modules, and devices to be connected to them, as well as devices to be connected to various servers and field networks (such as CC-Link IE TSN and EtherCAT) are also installed in addition to the MELSEC MX Controller MX-F models, which means that this equipment is the trust boundary.[12] SD memory cards and maintenance personal computers are connected to the MELSEC MX Controller MX-F 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-F model are installed will be connected to the Internet via firewalls and routers.

12 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.



* Safety control (dark green shading) is supported only by the MX-F model(with Safety Function).

* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

Figure 17 Environment where the MELSEC MX Controller MX-F model is expected to be installed

Table 18 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-F model is installed	The equipment in which the MELSEC MX Controller MX-F 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 memory card	An SD memory card is used in the locked equipment and cannot be inserted or removed without the permission of the administrator.
4	Restrictions on connection range for expansion adapters and extension modules	Devices outside the equipment are not connected to expansion adapters and extension modules.
5	Restrictions on connection range for field network ports	Devices connected to the field network ports are not installed outside the equipment.
6	Physical protection of the debug I/F	The debug I/F is inside the case of the MELSEC MX Controller MX-F model and is not directly accessible physically.
7	Addition of manipulation check information to data created by the engineering tool	Information necessary for manipulation check is automatically added to the information to be written to the MELSEC MX Controller MX-F model that affects its main functions when the user creates the information.
8	Education for users	Users are adequately educated and trained to properly set, manage, and operate the MELSEC MX Controller MX-F model.
9	Selection of an appropriate administrator	A person who will carry out the administration properly without malicious intent is selected as the administrator.
10	Installation of firewalls	Network switches and firewalls are installed between the network to which the MELSEC MX Controller MX-F model is connected and the external network, blocking unnecessary communications from the external network.
11	Security on the personal computers which communicate with the MELSEC MX Controller MX-F model	The personal computers which communicate with the MELSEC MX Controller MX-F model (maintenance personal computers and production monitoring personal computers) have anti-virus software to ensure security.

Table 20 describes the devices and networks in Figure 17.

Table 19 Device/application/network in the environment

No.	Term	Description
1	HMI	A device connected to the MELSEC MX Controller MX-F model to operate it and display information. Example of Mitsubishi Electric HMI: GOT
2	Production monitoring personal computer	A device with software for monitoring the status of the control system installed. Examples of Mitsubishi Electric software used for status monitoring: MC Works64 and GX Works3
3	Maintenance personal computer	A device with an engineering tool necessary for maintaining the MELSEC MX Controller MX-F model installed. Example of Mitsubishi Electric engineering tool: GX Works3
4	Field network	A network used for communication between the MELSEC MX Controller MX-F model and field devices. Examples of field network: CC-Link IE TSN and EtherCAT

No.	Term	Description
5	Control information network	A wireless or wired 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-F model. Example of control information network: Ethernet TCP/IP communication
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 wireless or wired 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-F model and outputs the values generated by the MELSEC MX Controller MX-F model. Example of field devices: Servo, inverter, remote I/O, etc.
10	Server	A server that responds to inquiries from the MELSEC MX Controller MX-F model and stores data. Examples of servers: FTP server, SNTP server, DNS server
11	Expansion adapter	A device used to expand the functions of the MELSEC MX Controller MX-F model. It is a device that uses the serial communication function and analog function.
12	Extension module	A device used to expand the functions of the MELSEC MX Controller MX-F model. It is a device that performs communication using the inter-module communication function.

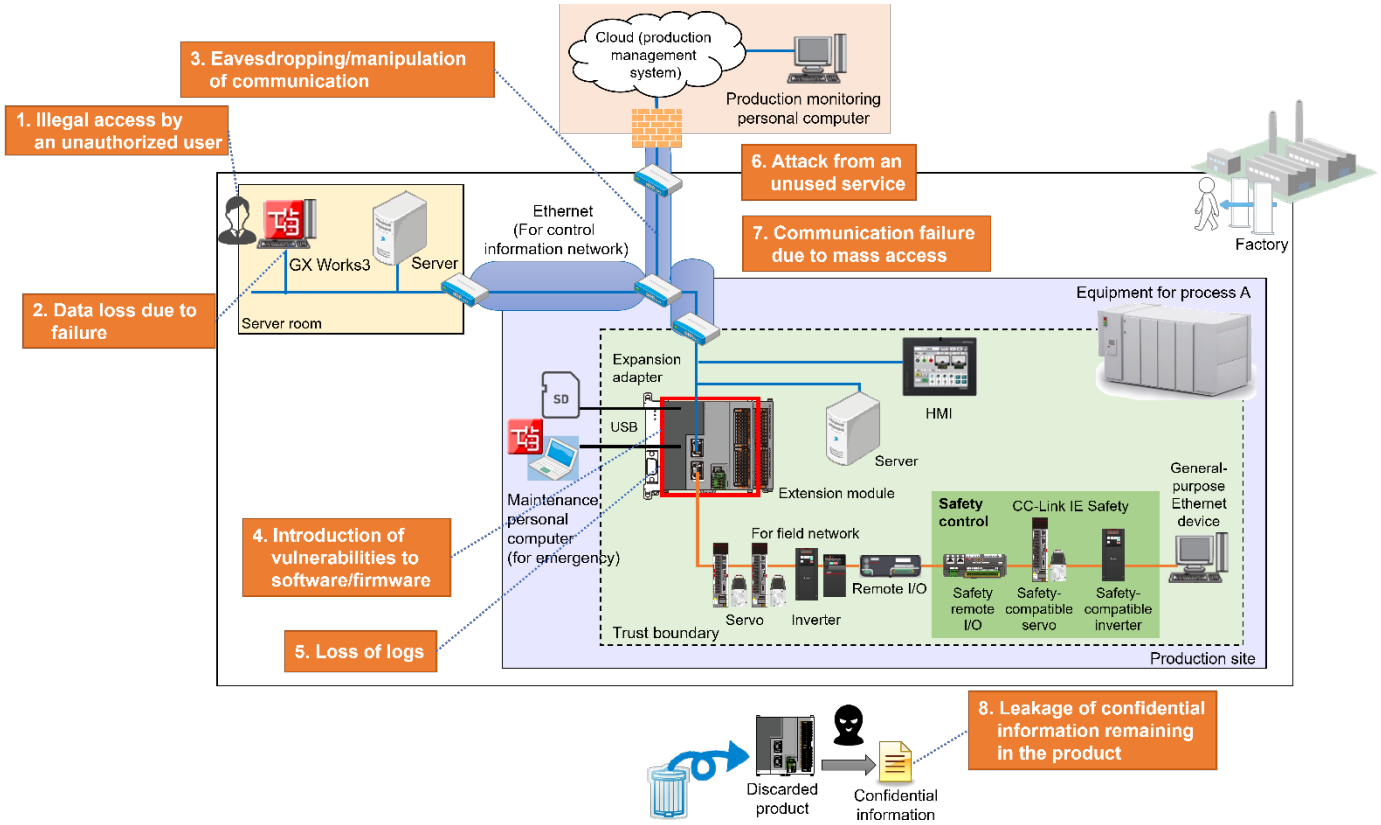
Access to devices can be physically controlled by restricting entry to individual areas of the factory or by applying physical locks to the device storage areas. These physical access controls are also important security elements. For the use of the MELSEC MX Controller MX-F model, the area classification shown in Table 21 is assumed from a security perspective.

Table 20 Area classification and operation method

No.	Term	Description
1	Server room	A room that stores devices critical to continuing 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 with locks).
2	Equipment area of each process	Equipment in which the MELSEC MX Controller MX-F 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 with locks).
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.

3.2.2. Threats to the MELSEC MX Controller MX-F model

We assume the threats shown in Figure 18 and Table 22 in the usage environment of the MELSEC MX Controller MX-F model shown in Figure 17 of 3.2.1 based on the risk assessment of the module and knowledge of publicly known attack cases.



* Safety control (dark green shading) is supported only by the MX-F model(with Safety Function).

* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

Figure 18 Threats to the MELSEC MX Controller MX-F model

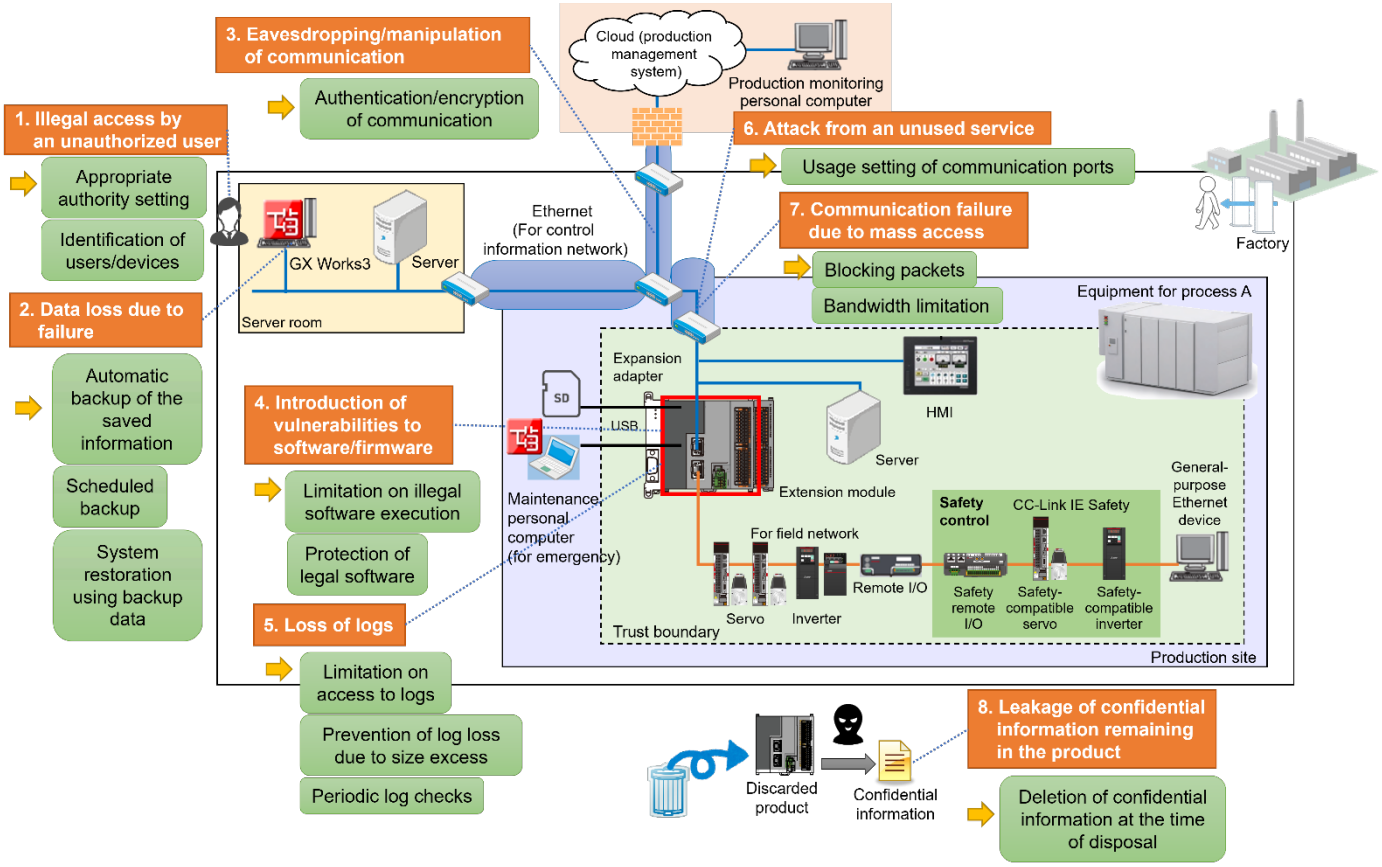
Table 21 Description of threats

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-F 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-F 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-F 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.

3.2.3. Policy on countermeasures against threats

Figure 19 and Table 23 show the policy on countermeasures against threats to the MELSEC MX Controller MX-F model. The policy includes not only the countermeasures to be taken with the MELSEC MX Controller MX-F 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-F model. Therefore, it is necessary to maintain security measures not only for the MELSEC MX Controller MX-F model but also for the entire FA system.



* Safety control (dark green shading) is supported only by the MX-F model(with Safety Function).

* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

Figure 19 Policy on countermeasures against threats to the MELSEC MX Controller MX-F model

Table 22 Policy on countermeasures against threats to the MELSEC MX Controller MX-F model

No.	Threat name	Policy on countermeasures	Related security functions/measures of the MELSEC MX Controller MX-F model	Reference for setting method for the security function
1	Illegal access by an unauthorized user	● Appropriate authority setting ● User identification	◆ User authentication function ■ Physical access restriction ■ Selection of the administrator ■ Installation of firewalls ■ Security on the personal computer	3.4.4 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	3.4.6 Backup/restoration function of the controller
3	Eavesdropping/manipulation of communication	● Authentication/encryption of communication	◆ Encrypted communication function ■ Physical access restriction ■ Installation of firewalls ■ Security on the personal computer	3.4.7 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	3.4.2 Firmware update function 3.4.3 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	3.4.5 Event history function
6	Attack from an unused service	● Usage setting of communication ports	◆ Usage setting function of default open port ■ Education for users	3.4.9 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	3.4.8 IP filter function 3.4.10 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 function of all information in the controller	3.4.1 Initialization function of all information in the controller

◆ marks indicate security functions implemented in the MELSEC MX Controller MX-F model.

■ marks indicate security measures to be taken in the customer's environment.

3.2.4. Security functions in the MELSEC MX Controller MX-F model

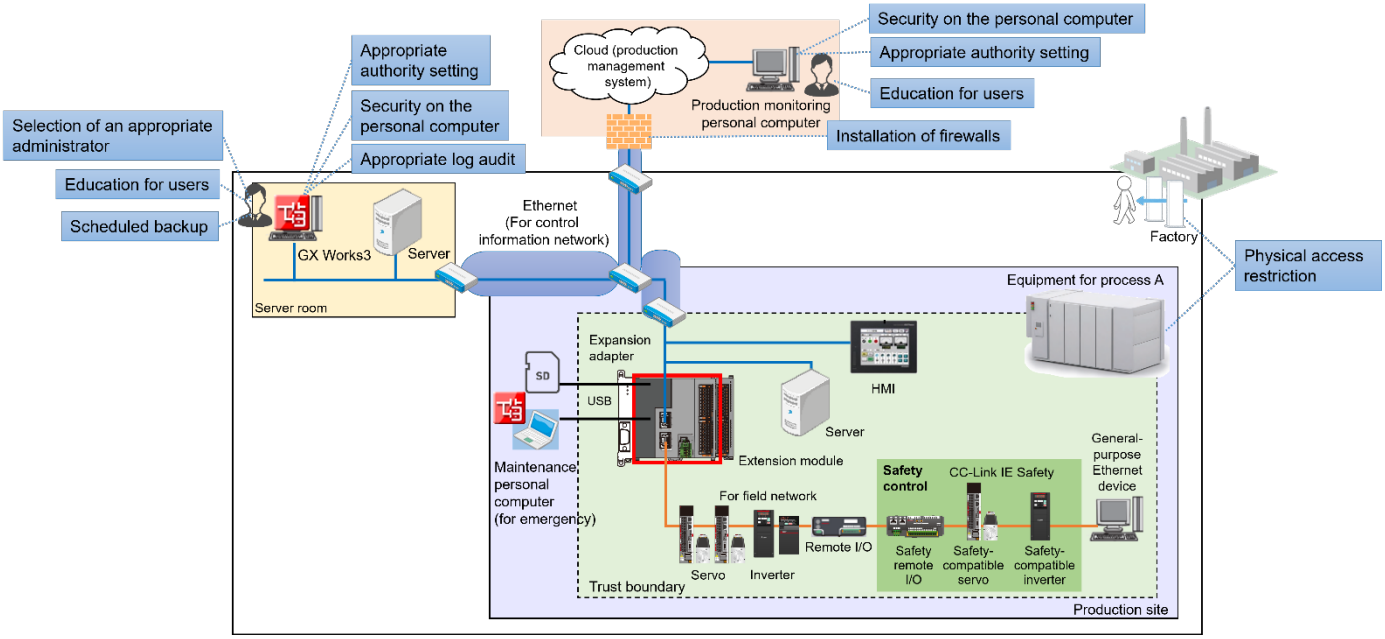
The MELSEC MX Controller MX-F model implements the security functions as described in Table 24 to realize the policy on countermeasures against threats described in 3.2.3.

Table 23 Security functions in the MELSEC MX Controller MX-F 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 function of all information in the controller	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 controller.	2. Data loss due to failure

3.2.5. Security measures to be taken outside the product

Figure 20 and Table 25 show the security measures recommended to be taken in the usage environment of the customer with the prerequisites (Table 19) in the usage environment (Figure 17) of the MELSEC MX Controller MX-F model and policy on countermeasures against threats (3.2.3).



* Safety control (dark green shading) is supported only by the MX-F model(with Safety Function).

* Connection to general-purpose Ethernet devices via the EtherCAT ports is not supported.

Figure 20 Security measures to be taken in the usage environment

Table 24 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-F 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-F 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
Network layer	Installation of firewalls or VPN	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-F 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

3.3. Introduction of the MELSEC MX Controller MX-F model

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

3.3.1. Setting and introduction procedures of the MELSEC MX Controller MX-F model

To use the MELSEC MX Controller MX-F model in a system (Figure 21), it is recommended that the MELSEC MX Controller MX-F model be operated according to the procedure described in Figure 22.

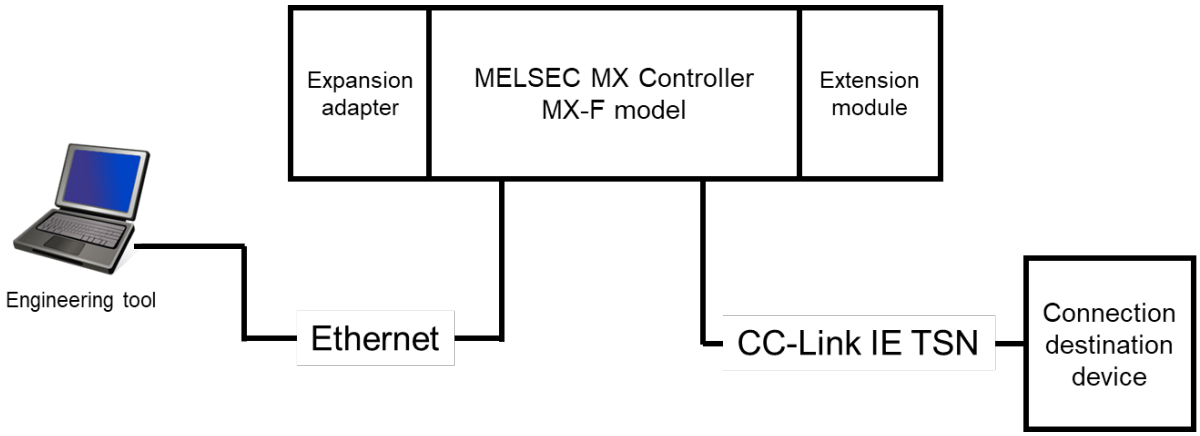


Figure 21 System configuration example

Connect the personal computer with the engineering tool installed to the MELSEC MX Controller MX-F model and perform the settings.

For the engineering tool compatible with the MELSEC MX Controller MX-F models, refer to the following manuals.

- MELSEC MX Controller MX-F model User's Manual
- MELSEC MX Controller MX-F model(with Safety Function) User's Manual

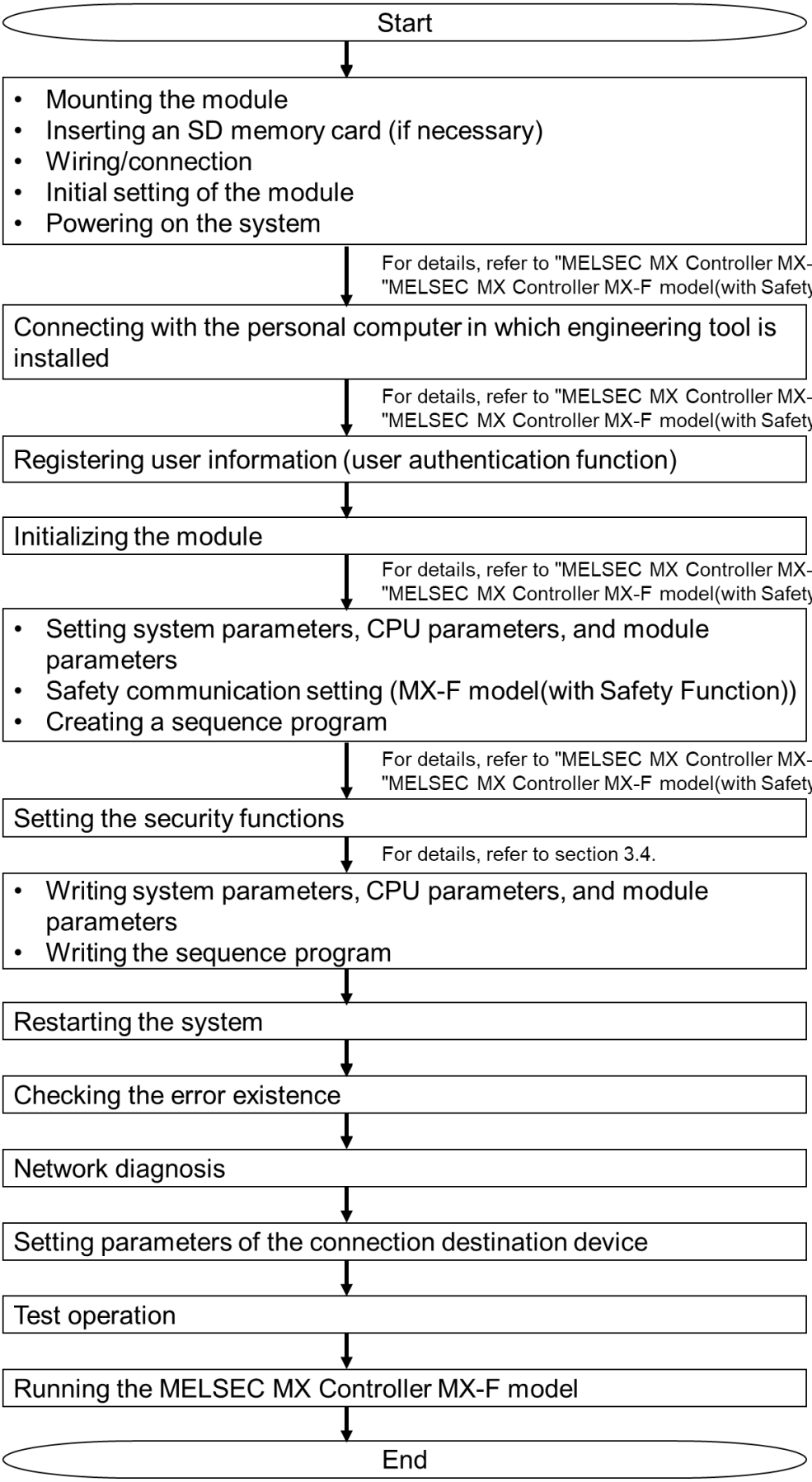


Figure 22 Procedure before operation

• Settings for the security functions of the MELSEC MX Controller MX-F model and the security policy

Perform the following items (Table 27) as the settings for the security functions of the MELSEC MX Controller MX-F model. In addition, when operating, please follow the implementation details described in Table 28.

Table 25 Settings for the security functions of the MELSEC MX Controller MX-F model

No.	Item	Setting for the security function	Reference
1	User authentication function	The user authentication function shall be enabled before setting and operating the encrypted communication function, IP filter function, usage setting function of default open port, bandwidth limitation function against DoS attack, and time setting.	3.4.4.2
2		Operation authority for each user group shall be set properly.	3.4.4.1
3		Passwords shall be periodically changed. (It is recommended that you enable the password expiration date setting.)	3.4.4
4		Each password shall be difficult to guess. (It is recommended that you set the password strength setting to “Strong”.)	3.4.4.2
5		Appropriate lockout time and the number of lockouts shall be set.	3.4.4
6		Appropriate usage notification messages giving warning to the logged on users shall be set.	3.4.4
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).	3.4.4.2
8		When using the Web server function, it shall be configured so that the user authentication function is enabled.	3.4.4.3
9	User authentication function Ethernet communication function FTP server function	Appropriate timers for connection and session shall be set.	3.4.4
10	Event history function	Appropriate storage size of the event history shall be set.	3.4.5
11		Event history shall be periodically backed up to a personal computer since oldest entries will be overwritten when the storage size is exceeded.	3.4.5
12		Correct time shall be set so that the time stamps are recorded correctly.	3.4.5
13		The manipulation check function for event history shall be enabled.	3.4.5
14	Backup/restoration function	Encryption setting of backup data shall be performed.	3.4.6.1
15	Encrypted communication function	Communications with external devices beyond the trust boundary shall be encrypted.	3.4.7
16		Communications that require encryption shall be performed in the Ethernet ports built in the MELSEC MX Controller MX-F model.	3.4.7.1
17		The expiration date of the certificate used for encrypted communications shall be set to one year (default setting).	3.4.7.2
18		When using the Web server function, a server certificate shall be created so that HTTPS is used in principle. When using HTTP communication, it shall be used only within a trust boundary.	3.4.7.3
19	IP filter function	Accesses from external devices shall be restricted with the IP filter.	3.4.8
20		Unused ports shall be set as closed.	3.4.9.1

No.	Item	Setting for the security function	Reference
21	Usage setting function of default open port	Communications with the outside of the trust boundary shall be performed using the Ethernet ports built in the MELSEC MX Controller MX-F model.	3.4.9
22	Bandwidth limitation function against DoS attack	The bandwidth limitation function against DoS attack shall be set.	3.4.10
23	Bandwidth limitation function against DoS attack, IP filter function, 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 function, usage setting function of default open port, and bandwidth limitation function against DoS attack.	3.4.10.1

Table 26 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-F model, there is a possibility that protected assets (data) are stored in that device. Take measures such as deleting the data before disposing of the device.	3.6
2	Connected devices	Verify prior to use that the equipment connected to the MELSEC MX Controller MX-F model is configured and operating as intended.	-
3		Terminate the session as soon as communication with the device connected to the MELSEC MX Controller MX-F model is no longer required.	-
4		If the system configuration, including devices connected to the MELSEC MX Controller MX-F model, has been changed, perform operation verification to check that only the intended devices are accessed.	-
5	Use of SD memory card	Use the SD memory card only for backup/restoration, and do not store any data other than backup data.	3.5.1
6	Performance and management of backups	Since there is a possibility that the protected assets (data) of the MELSEC MX Controller MX-F model and connected devices within the system may be lost due to sudden disaster or failure, etc., perform regular backups and manage the backup data appropriately.	3.5
7	Password management	Passwords shall be properly managed to prevent leakage and shall not be reused.	3.4.4
8	Trust boundary	In the following cases, the Web server function shall be used only within a trust boundary. • SNTP, FTP, BACnet, Modbus, HTTP, and SMB communications • Connections with other devices using USB ports, CC-Link IE TSN ports, and EtherCAT ports	3.4.7

3.4. How to set and use security functions and options

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

For the operation procedures of the functions, refer to "MELSEC MX Controller MX-F Model User's Manual" and "MELSEC MX Controller MX-F model(with Safety Function) User's Manual".

This section describes the following security functions.

- Initialization function of all information in the controller (Section 3.4.1)
- Firmware update function (Section 3.4.2)
- Add-on install function (Section 3.4.3)
- User authentication function (Section 3.4.4)
- Event history function (Section 3.4.5)
- Backup/restoration function of the controller (Section 3.4.6)
- Encrypted communication function (Section 3.4.7)
- IP filter function (Section 3.4.8)
- Usage setting function of default open port (Section 3.4.9)
- Bandwidth limitation function against DoS attack (Section 3.4.10)
- Operation setting function (Section 3.4.11)

3.4.1. 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

3.4.2. Firmware update function

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

3.4.2.1. Precautions

The following shows the precautions on using this function.

- Check that the firmware version is correctly updated using the engineering tool or in the event history 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[13]. 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 updates 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.

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

3.4.3. 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. If tampering with the add-on is detected during an add-on update, a stop error will occur.

3.4.3.1. Precautions

The following shows the precautions on using this function.

- 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 updates 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.

3.4.4. 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.

3.4.4.1. 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 27 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	The operation authority can be determined by users. 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 the minimum operation authority be granted according to the role of the group to be created.
Figure 23 shows the overview of the user authentication function. In Figure 23, 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.

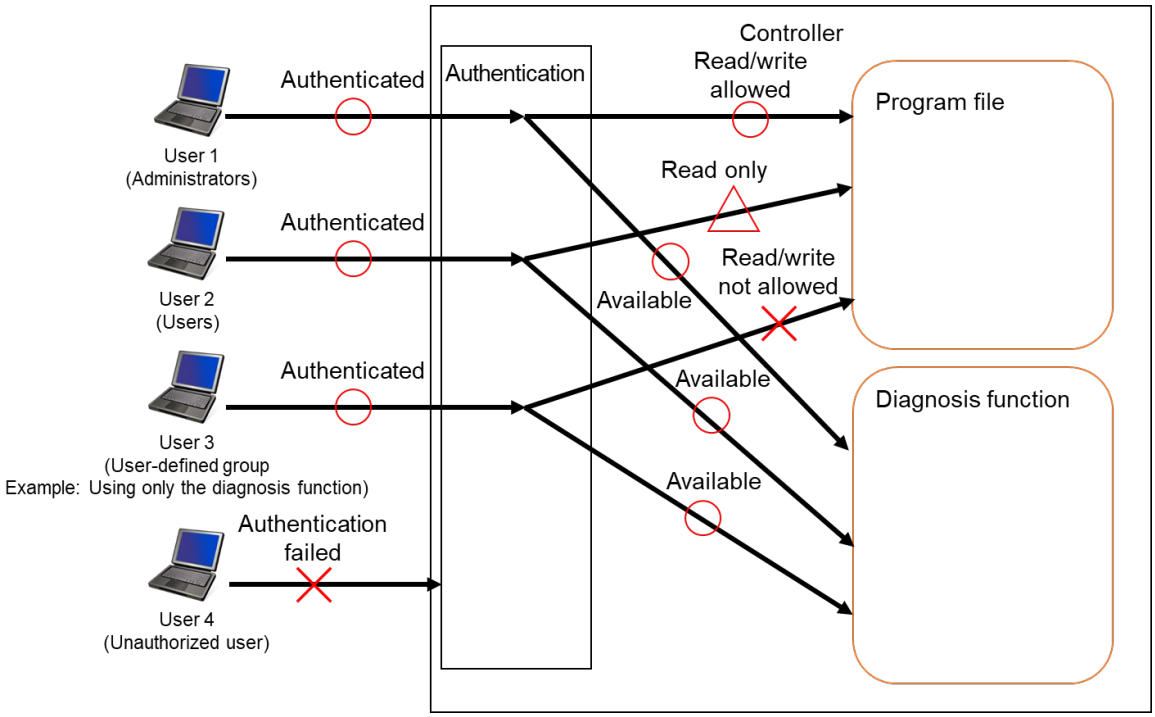


Figure 23 Overview of the user authentication function

3.4.4.2. Recommended settings

To enhance security, 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.

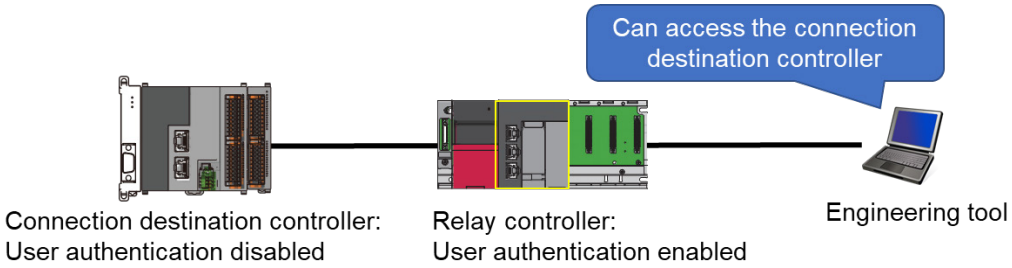


Figure 24 Path for which user authentication is invalid

3.4.4.3. 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.
- When using the Web server function, configure it to use the user authentication function and restrict access.

3.4.5. 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.
To enhance security, specify the data memory as the save destination for the event history.

3.4.5.1. 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 28 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 for detecting 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.

3.4.6. 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.

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. For both the above operations, use the engineering tool.

3.4.6.1. Encryption of backup data

When this function is used, encryption of backup data can be set with an engineering tool. To use the controller with security enhanced, 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.

3.4.6.2. 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.

3.4.6.3. Recommendations for using backup/restoration

- 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.

3.4.7. Encrypted communication function

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

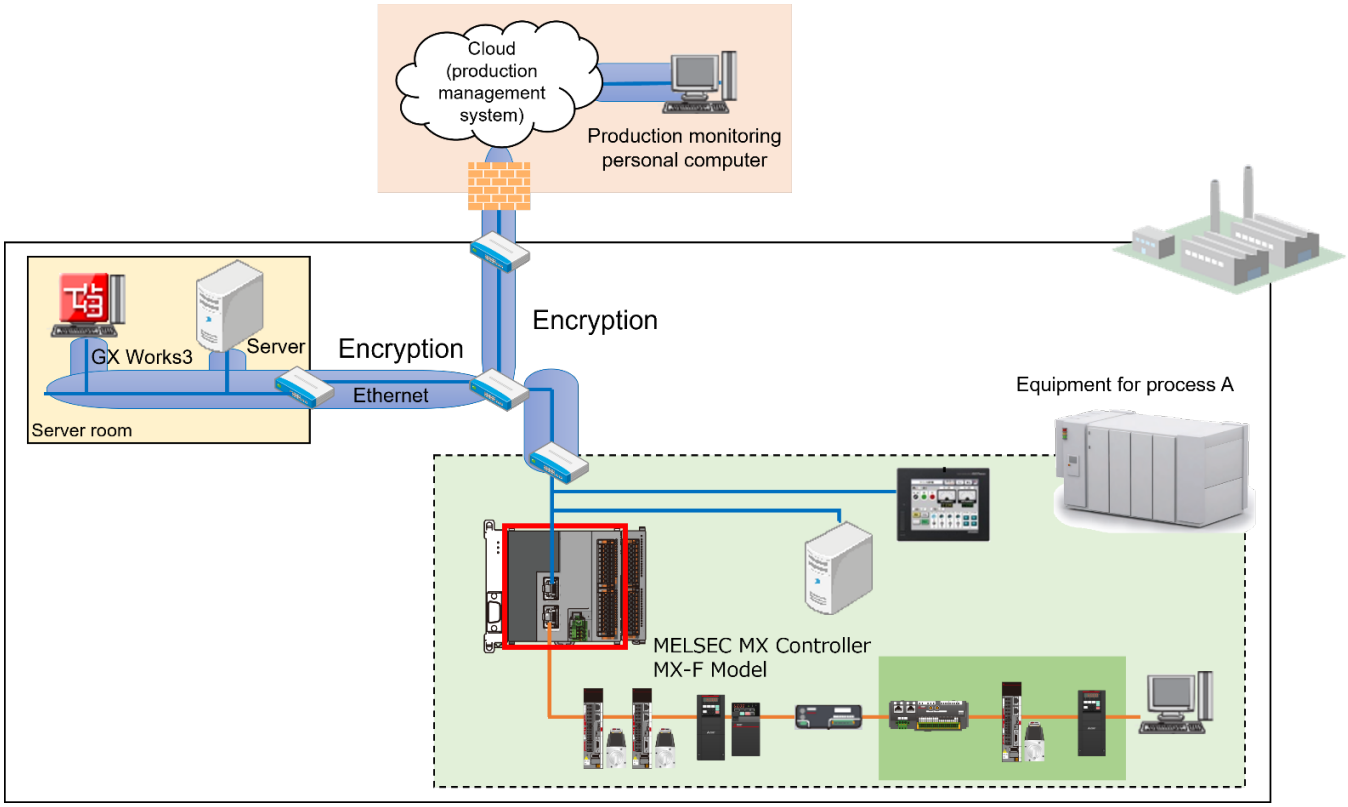


Figure 25 Encrypted communication function

3.4.7.1. 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 29 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
6	Communication via the Web server function

To enhance security, encrypt the above 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-F 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
- Communication via FTP
- Communication via SNTP
- Communication by BACnet
- Communication by Modbus/TCP
- Communication by Modbus RTU
- Communication via MC protocol

* TLS/DTLS version

- When using TLS or DTLS for encrypted communication, set the version to be the same as that of the communication partner.
- In this setting, specify the version of TLS/DTLS. Separately set the external devices to which encrypted communication will be used.
- If encrypted communication is used for multiple external devices with mixed TLS versions, such as TLS 1.2 and TLS 1.3, set the encryption communication version to TLS 1.2/TLS 1.3. If either TLS 1.2 or TLS 1.3 is selected, encrypted communication will fail with external devices using a different version.

3.4.7.2. 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 enhance security, 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.

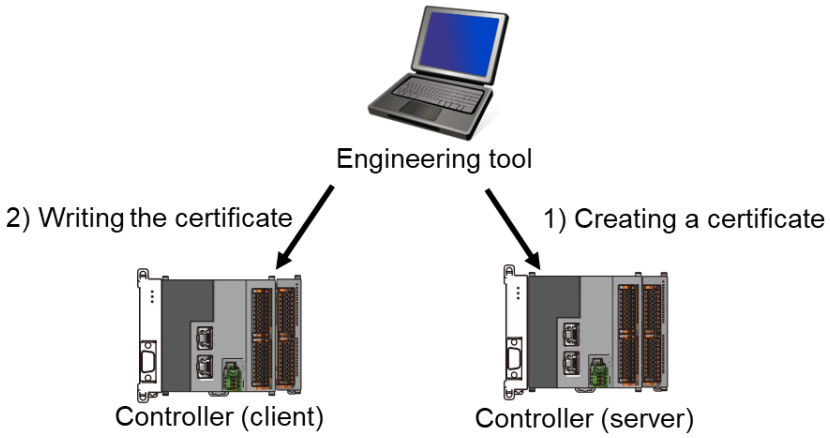


Figure 26 Setting procedure of a certificate

3.4.7.3. 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 function to prevent illegal deletion or modification of the 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.
- When using the Web server function, create a digital certificate so that communication is performed only via HTTPS in principle.

3.4.8. IP filter function

The IP filter function identifies the IP address of the access source, and prevents access from an illegal IP address. By setting the IP address of the external device to be allowed or denied in the parameters, 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.

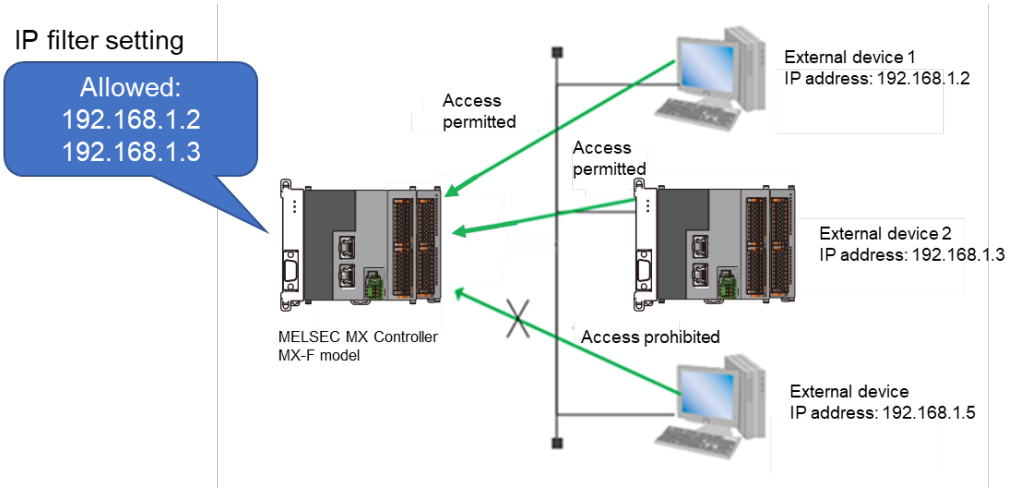


Figure 27 Access restriction by IP filter

3.4.8.1. Recommendations for using IP filters

- Use of the IP filter function is recommended when using in an environment connected to a LAN line.
- To enhance security, 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.

3.4.9. 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.

3.4.9.1. 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.

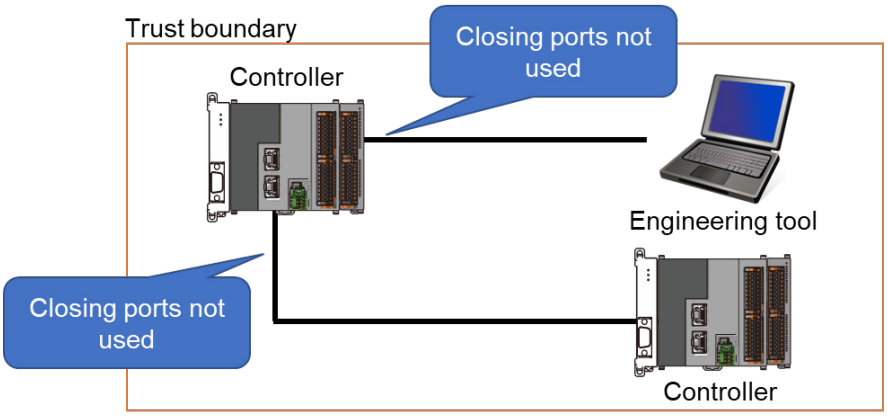


Figure 28 Example of port close setting within the trust boundary

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.

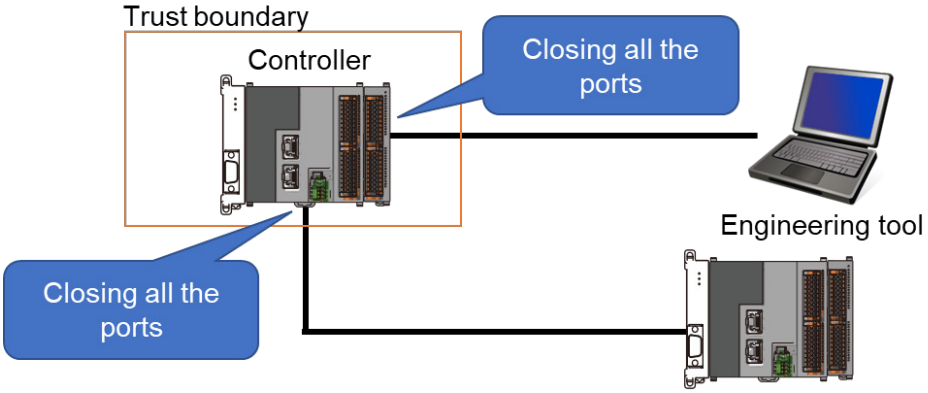


Figure 29 Example of port close setting outside the trust boundary

3.4.9.2. Precautions

The following shows the precautions on using this function.

- To enhance security, set the unused ports (including the ports set as default open 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.

3.4.10. 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.

3.4.10.1. Recommendations for bandwidth limitation settings

When using this function, set the transmission bandwidth and reception bandwidth that can be used with the engineering tool. 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 enhance security, use this function with the IP filter or usage setting function of default open port.

3.4.11. Operation setting function

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

Table 30 Behavior of the MELSEC MX Controller MX-F model with operation setting

No.	Operation setting	Output	Behavior
1	Stop operation	Hold	The MELSEC MX Controller MX-F model stops operation immediately upon detecting an error and maintains the last confirmed normal state of external outputs.
2	Continue operation	-	When the MELSEC MX Controller MX-F model detects an error, it executes a program other than the program (instruction) in which the error occurred.

3.4.11.1. Precautions

The following shows the precautions on using this function.

- When setting “Continue calculation”, be sure to verify the operation when an error occurs in advance and confirm that there are no problems.
- Regardless of the operation settings described above (Table 32), the safety outputs of the MELSEC MX Controller MX-F model(with Safety Function) are cleared when the operation stops.
- If an instruction execution error is detected in the safety program of the MELSEC MX Controller MX-F model(with Safety Function), operation will stop regardless of the operation settings described above (Table 32).

3.5. Operation and maintenance of the MELSEC MX Controller MX-F model

3.5.1. Recommended operation example of the MELSEC MX Controller MX-F model

As physical security measures on the MELSEC MX Controller MX-F model, restricting access to certain areas in the factory and installing the MELSEC MX Controller MX-F 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-F 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-F model can be operated. To prevent these personal computers from being compromised, which causes files stored in the MELSEC MX Controller MX-F 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-F 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-F 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-F 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-F model is installed, performing the check items related to each function as shown in Table 33 is recommended.

Table 31 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.
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-F model, selecting an appropriate person as the administrator is recommended. It is recommended that users of the MELSEC MX Controller MX-F model receive adequate education and training to properly set, manage, and operate the product. Use the MELSEC MX Controller MX-F 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 32 Functions that use an SD memory card and recommended alternative operation methods

No.	Function	Recommended operation method
1	Event history function	Specify the data memory as the save destination for the 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 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 destination for the 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.

3.5.2. 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 35 is recommended. In addition, Table 36 lists the functions where the function settings affect security. Periodically check that these settings are correct as well.

Table 33 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.
		The firmware shall not be changed unintendedly.
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.
		Logoff shall be performed after the specified logoff timeout period has elapsed.
		The set warning message shall be displayed at the time of a logon operation.
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.
		The event history shall be saved in the specified save destination.
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.
		When automatic backup is set, backup files shall be generated at the specified execution timing (date and time specification, time and day of the week specification, or stop error occurrence specification).
		If automatic backup/retry is enabled and a function that cannot be executed simultaneously is running, a retry shall be performed.
		When the backup data upper limit setting is enabled, the system shall operate as specified when the backup data reaches the upper limit.

No.	Function name	Check item
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 restoration execution request operation is performed.
		If the restoration of special relays and special registers is enabled when restoration is performed, the values of the special relays and special registers shall be restored.
		When automatic restoration is set, performing an automatic restoration execution request operation shall succeed, and the system shall return to the state at the time of backup.
		When initialization for automatic restoration is enabled, drives other than the restoration target drive shall be initialized.
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.
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 34 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-F 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 from the IP address.

3.6. Removal and disposal of the MELSEC MX Controller MX-F model

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

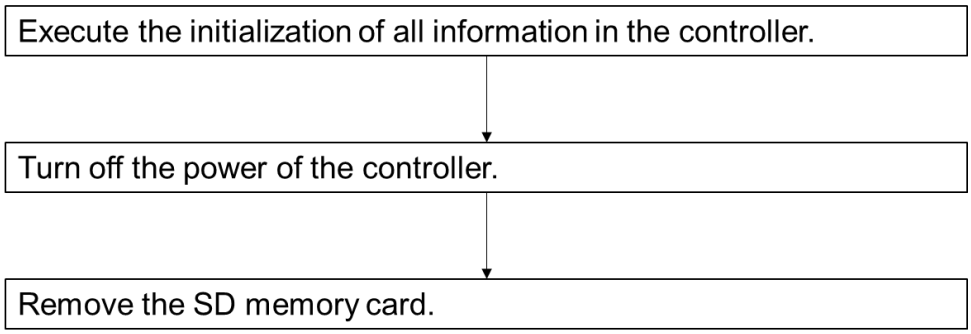


Figure 30 Removal method of the product

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 the initialization function of all information in the controller. 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-F model after the system is shut down with the appropriate procedures according to the operation manual.

When removing a device connected to the MELSEC MX Controller MX-F model in the system, there is a possibility that protected assets are stored in that device. Take measures such as deleting the data before removing it so that the information cannot be retrieved.

4. Security of the CC-Link IE TSN Class A supported wireless LAN adapter by Mitsubishi Electric

4.1. Purpose of this chapter

This chapter provides the following information to explain our approach to the security of the CC-Link IE TSN Class A supported wireless LAN adapter by Mitsubishi Electric (wireless LAN adapter) so that it can be used safely and securely in customers' FA systems.

- Policy on security measures for the wireless LAN adapter (Section 4.2):
  This section describes the policy on security measures against threats by identifying possible threats to the wireless LAN adapter. Some countermeasures are performed by the wireless LAN adapter alone while others are performed in combination with other products.
- Introduction method of the wireless LAN adapter (Section 4.3 and 4.4):
  These sections describe the security functions of the wireless LAN adapter, how to set them, and how to install the wireless LAN adapter in an FA system.
- Operation and maintenance method of the wireless LAN adapter (Section 4.5)
  This section describes recommendations on how to manage users and passwords for operating the wireless LAN adapter.
- Removal and disposal method of the wireless LAN adapter (Section 4.6):
  This section describes the recommended methods (e.g., product data deletion functions) for removing and disposing of the wireless LAN adapter.

In addition, refer to the following operation manual for the detailed specifications and operation methods for each function of the wireless LAN adapter as necessary.

- ◆ CC-Link IE TSN Class A Supported Wireless LAN Adapter User's Manual

Read this guideline and the above related operation manual carefully to fully understand the security of the wireless LAN adapter, 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 wireless LAN adapter, product life cycle initiatives, and examples of FA system construction.

- ◆ FA SYSTEM SECURITY GUIDELINE

4.2. Policy on security measures for the wireless LAN adapter

This section describes the following policy on security measures for the wireless LAN adapter.

- Expected usage environment (installation environment, network, operation and maintenance, etc.) of the wireless LAN adapter
- Threats to the wireless LAN adapter
- Policy on countermeasures against threats
- Security functions in the wireless LAN adapter
- Security measures to be taken outside the product

4.2.1. Expected usage environment of the wireless LAN adapter

Figure 31 shows the environment where the wireless LAN adapter is expected to be installed. Table 37 shows the prerequisites for ensuring security in the installation environment shown in Figure 31. These installation environment and usage environment including prerequisites are the premises for the policy on security measures described in the subsequent sections.

The wireless LAN adapter is installed on the top of equipment or inside resin boxes within factory production areas, designed for use in environments where unauthorized removal is prevented by measures such as wire locks. In this equipment, devices that communicate via CC-Link IE TSN, including the manager station, are also installed, which means that this equipment is the trust boundary[14]. Maintenance personal computers are connected to the wireless LAN adapter for use through wireless communication, 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 wireless LAN adapters are installed will be connected to the Internet via firewalls and routers.

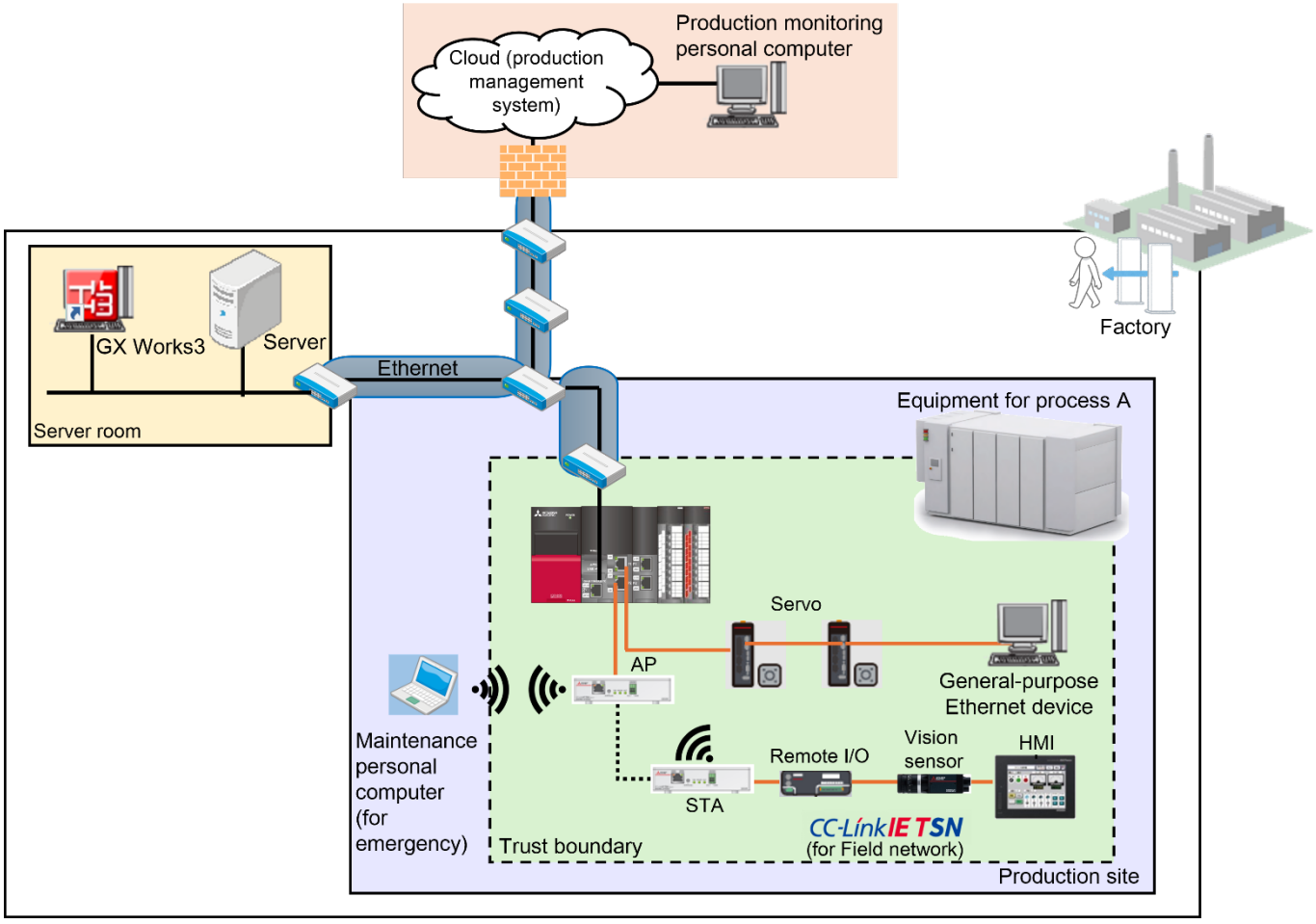


Figure 31 Environment where the wireless LAN adapter is expected to be installed

[14] 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.

Table 35 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 wireless LAN adapter is installed	The equipment in which the wireless LAN adapter is installed is locked, and the devices in the equipment cannot be operated or changed without the permission of the administrator.
3	Education for users	Users are adequately educated and trained to properly set, manage, and operate the wireless LAN adapter.
4	Selection of an appropriate administrator	A person who will carry out the administration properly without malicious intent is selected as the administrator.
5	Installation of firewalls	Network switches and firewalls are installed between the network to which the wireless LAN adapter is connected and the external network, blocking unnecessary communications from the external network.
6	Security on the personal computers which communicate with the wireless LAN adapter	The personal computers which communicate with the wireless LAN adapter (maintenance personal computers and production monitoring personal computers) have anti-virus software to ensure security.
7	Activation of the stealth SSID function	The stealth SSID function of the wireless LAN adapter is activated to prevent access from unintended devices by not notifying its SSID on the network.
8	Activation of the MAC address filter function	The MAC addresses of devices permitted to be connected are pre-registered to the wireless LAN adapter, and access from unregistered devices is prohibited.
9	Setting of the login password	A login password has been set for the web interface of the wireless LAN adapter.

Table 38 describes the devices and networks in Figure 31.

Table 36 Device/application/network in the environment

No.	Term	Description
1	HMI	A device connected to the manager station via the wireless LAN adapter to operate it and display information. Example of Mitsubishi Electric HMI: GOT
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 software necessary for maintaining the wireless LAN adapter installed. The required software is a web browser.
4	CC-Link IE TSN	A network used for communication between a CC-Link IE TSN manager station and device station.
5	Ethernet network	A network that is inside a firewall and used for communication between a production monitoring personal computer or other devices and the wireless LAN adapter. Example of network: Ethernet TCP/IP communication
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	External network	A network that is outside the firewall and beyond the factory's authority to manage the network. Example of external network: Internet

No.	Term	Description
8	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.
9	Manager station	A device that controls the whole CC-Link IE TSN.
10	Device station	A device that communicates using CC-Link IE TSN. Examples of connected devices: Servo, remote I/O, HMI
11	Ethernet device	IP communication compatible devices (such as personal computer, vision sensor, barcode reader).
12	Wireless LAN adapter (AP)	Indicate the CC-Link IE TSN Class A supported wireless LAN adapter. They support AP (Access point) and STA (Station), and are indicated as shown on the left according to the operation mode.
13	Wireless LAN adapter (STA)	
14	Web interface	A web page used for monitoring the parameter settings and connection status built in the wireless LAN adapter.

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 wireless LAN adapter, the area classification shown in Table 39 is assumed from a security perspective.

Table 37 Area classification and installation location

No.	Term	Description
1	Server room	A room that stores devices critical to continuing 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 with locks).
2	Equipment area of each process	Equipment in which the wireless LAN adapter 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 with locks).
3	Manufacturing process	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.

4.2.2. Threats to the wireless LAN adapter

We assume the threats shown in Figure 32 and Table 40 in the usage environment of the wireless LAN adapter shown in Figure 31 of 4.2.1 based on the risk assessment of the module and knowledge of publicly known attack cases.

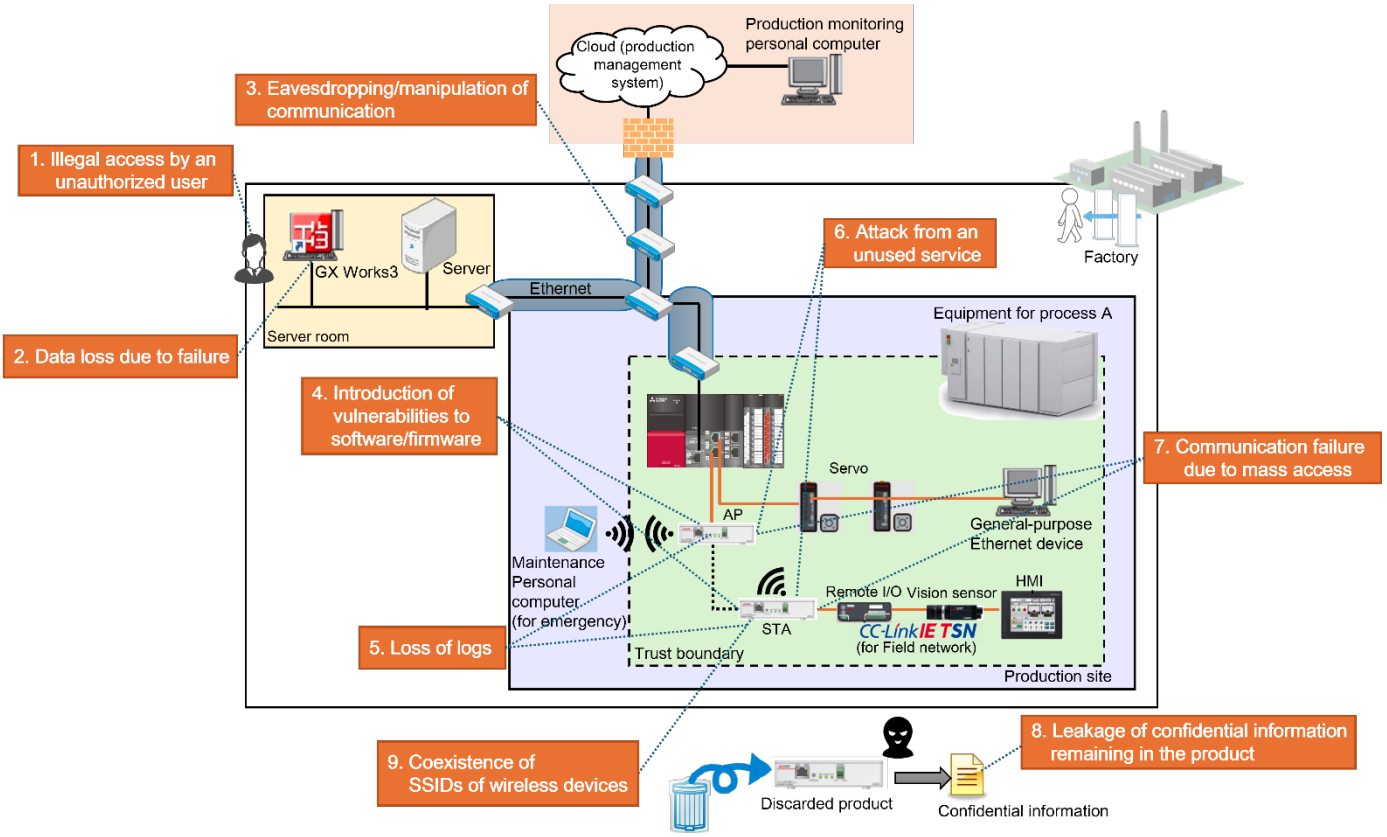


Figure 32 Threats to the wireless LAN adapter

Table 38 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 wireless LAN adapter 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 wireless LAN adapter 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 wireless LAN adapter, 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.
9	Coexistence of SSIDs of wireless devices	Using the same SSID as wireless devices for other purposes may cause unintended connections with those devices.

4.2.3. Policy on countermeasures against threats

Figure 33 and Table 41 show the policy on countermeasures against threats to the wireless LAN adapter. The policy includes not only the countermeasures to be taken with the wireless LAN adapter, 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 wireless LAN adapter. Therefore, it is necessary to maintain security measures not only for the wireless LAN adapter but also for the entire FA system.

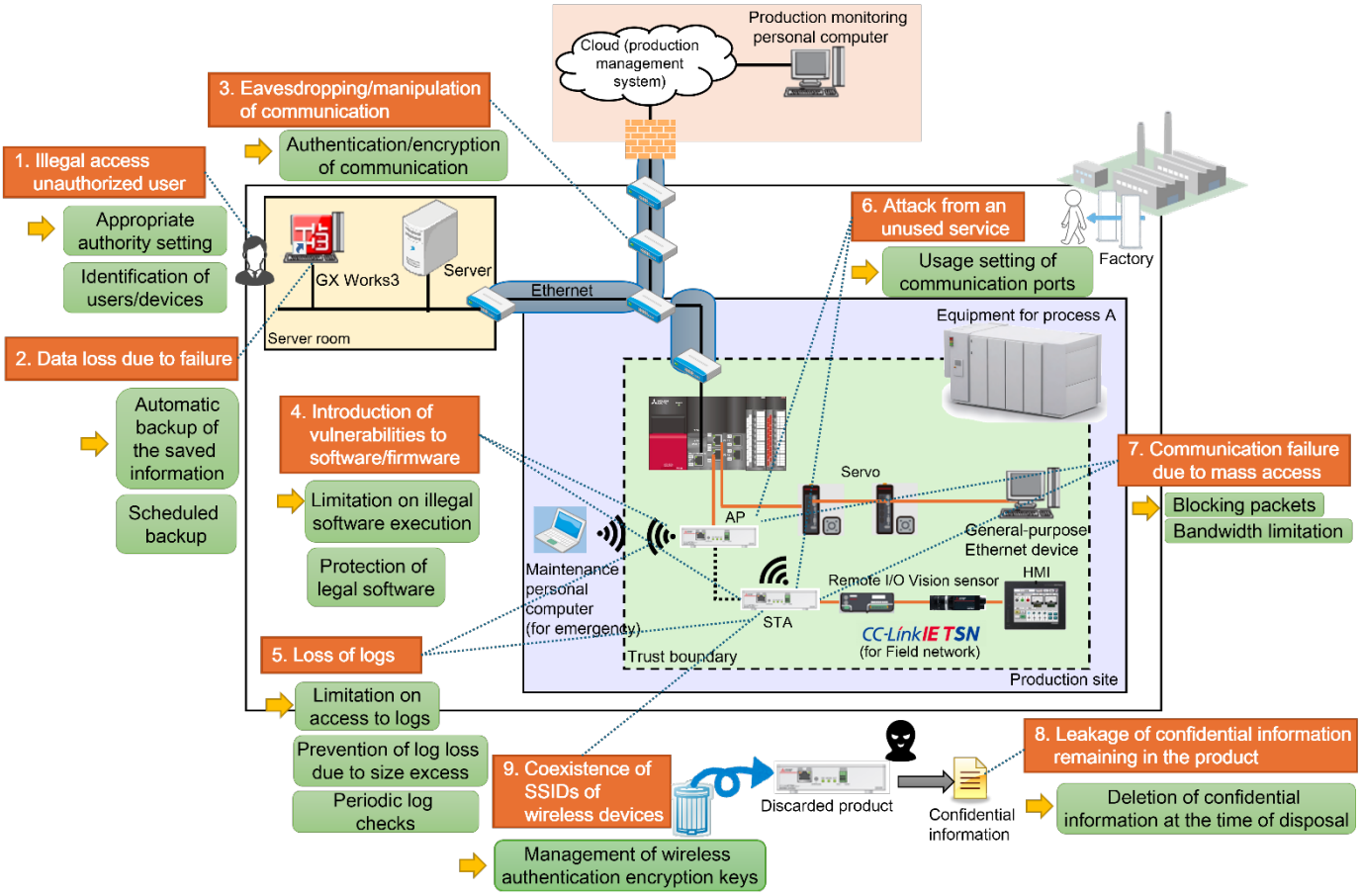


Figure 33 Policy on countermeasures against threats to the wireless LAN adapter

Table 39 Policy on countermeasures against threats to the wireless LAN adapter

No.	Threat name	Policy on countermeasures	Related security functions/measures of the wireless LAN adapter	Reference for setting method for the security function
1	Illegal access by an unauthorized user	● Appropriate authority setting ● User identification	● Wireless encryption mode ● Wireless authentication mode ● Wired LAN MAC address filter ● Wireless LAN MAC address filter ● Stealth SSID ● Password authentication ■ Physical access restriction ■ Selection of the administrator ■ Installation of firewalls ■ Security on the personal computer Password authentication	4.4.1 Wireless encryption mode 4.4.2 Wireless authentication mode 4.4.3 Wired LAN MAC address filter/wireless LAN MAC address filter 4.4.4 Stealth SSID 4.4.5 Password authentication
2	Data loss due to failure	● Automatic backup of the saved information ● Scheduled backup ● System restoration using backup data	● Backup/restoration function ■ Scheduled backup	4.4.7 Backup/restoration function
3	Eavesdropping/ manipulation of communication	● Authentication/ encryption of communication	● Wireless encryption mode ● Wireless authentication mode ■ Physical access restriction ■ Installation of firewalls ■ Security on the personal computer	4.4.1 Wireless encryption mode 4.4.2 Wireless authentication mode
4	Introduction of vulnerabilities to software/firmware	● Limitation on illegal software execution ● Protection of legal software	● Firmware update function	4.4.9 Firmware update function
5	Loss of logs	● Limitation on access to logs ● Prevention of log loss due to size excess ● Periodic log checks	● Logging function ■ Log audit ■ Security on the personal computer	4.4.6 Logging function
6	Attack from an unused service	● Usage setting of communication ports	■ Education for users ■ Usage setting of open port	-
7	Communication failure due to mass access	● Blocking packets ● Bandwidth limitation	● Wired LAN MAC address filter ● Wireless LAN MAC address filter ● Stealth SSID ■ Management by purpose of wireless channel	4.4.3 Wired LAN MAC address filter/wireless LAN MAC address filter 4.4.4Stealth SSID
8	Leakage of confidential information remaining in the product	● Deletion of confidential information at the time of disposal	● Initialization function	4.4.8 Initialization function

9	Coexistence of SSIDs of wireless devices	● Management of wireless communication settings	■ Management of encryption keys for the wireless encryption mode and wireless authentication mode ■ Management of SSID	-

● marks indicate security functions implemented in the wireless LAN adapter.

■ marks indicate security measures to be taken in the customer's environment.

4.2.4. Security functions in the wireless LAN adapter

The wireless LAN adapter implements the security functions as described in Table 42 to realize the policy on countermeasures against threats described in Section 4.2.3.

Table 40 Security functions in the wireless LAN adapter

Function name	Description	Target threat
Wireless encryption mode	Encrypts wireless communications using the specified encryption mode.	1. Illegal access by an unauthorized user/device 3.Eavesdropping/manipulation of communication
Wireless authentication mode	Checks the legitimacy of the communication partner in wireless communications using the specified authentication mode.	1. Illegal access by an unauthorized user/device 3. Eavesdropping/manipulation of communication
Wired LAN MAC address filter	Restricts devices that can be connected to the wireless LAN adapter from the wired LAN side with their MAC addresses.	1. Illegal access by an unauthorized user/device 7. Communication failure due to mass access
Wireless LAN MAC address filter	Restricts devices that can be connected to the wireless LAN adapter from the wireless LAN side with their MAC addresses.	1. Illegal access by an unauthorized user/device 7. Communication failure due to mass access
Stealth SSID	Makes the SSID of the wireless LAN adapter private to prevent unintended devices from connecting.	1. Illegal access by an unauthorized user/device 7. Communication failure due to mass access
Password authentication	Restricts connections to the web interface used to set the wireless LAN adapter using password authentication.	1. Illegal access by an unauthorized user/device
Logging function	Saves logs of the operations performed via the wireless LAN adapter and the connection status.	5. Loss of logs
Backup/restoration function	Backs up the wireless LAN adapter settings and restores the settings.	2. Data loss due to failure
Initialization function	Initializes the settings of the wireless LAN adapter.	8. Leakage of confidential information remaining in the product

For the detailed specifications and setting method for each function, refer to "CC-Link IE TSN Class A Supported Wireless LAN Adapter User's Manual".

4.2.5. Security measures to be taken outside the product

Figure 34 and Table 43 show the security measures recommended to be taken in the usage environment of the customer with the prerequisites (Table 37) in the usage environment (Figure 31) of the wireless LAN adapter and policy on countermeasures against threats (4.2.3).

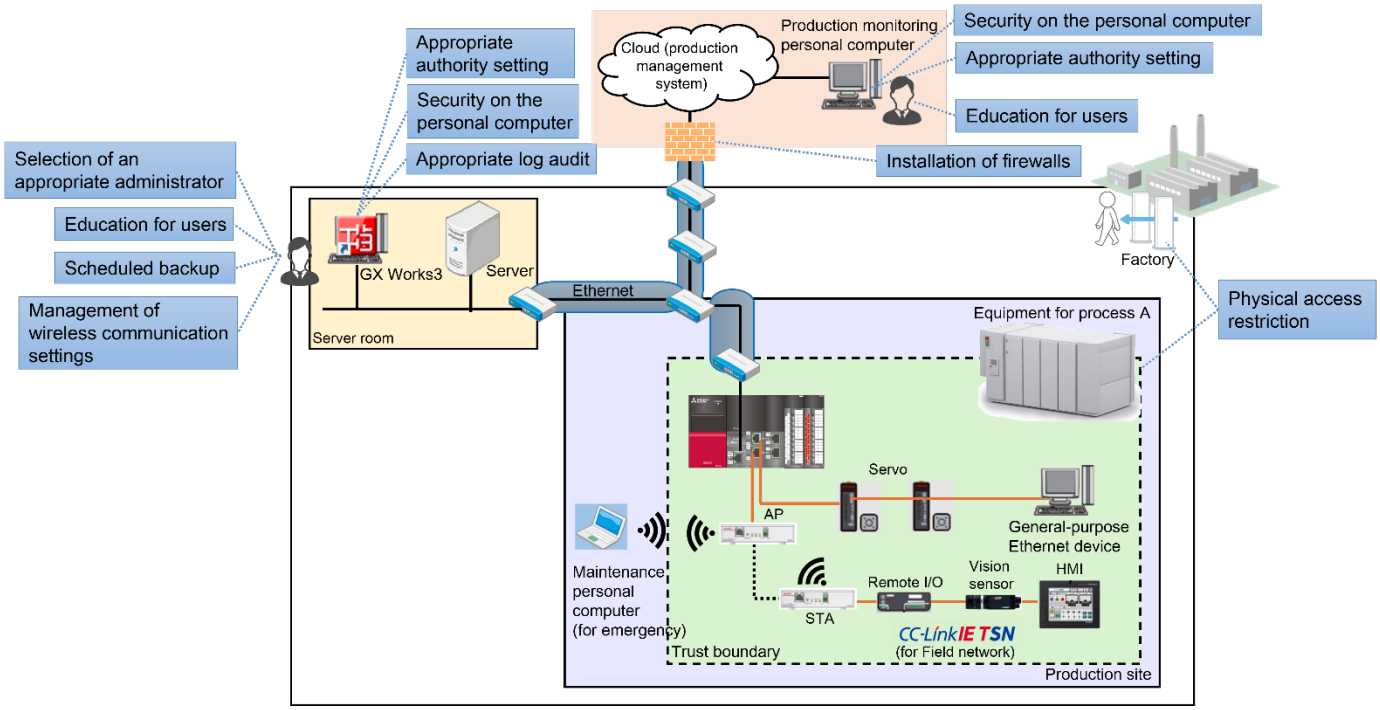


Figure 34 Security measures to be taken in the usage environment

Table 41 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 wireless LAN adapter 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 wireless LAN adapter 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
Network layer	Installation of firewalls	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 wireless LAN adapter (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

4.3. Introduction of the wireless LAN adapter

This section describes how to introduce the wireless LAN adapter in a system and how to set and use the security functions of the wireless LAN adapter.

4.3.1. Installation and introduction procedures

To use the wireless LAN adapter in a system (Figure 35), it is recommended that the wireless LAN adapter be operated according to the procedure described in Figure 36.

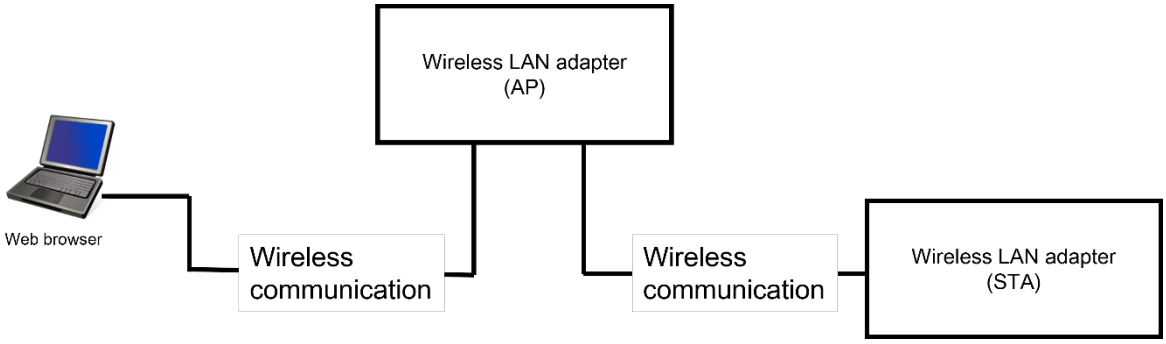


Figure 35 System configuration example

Connect to the wireless LAN adapter from a web browser in the personal computer and configure the settings. The recommended web browser is Google Chrome®[15].

[15] Google Chrome is a registered trademark or trademark of Google LLC.

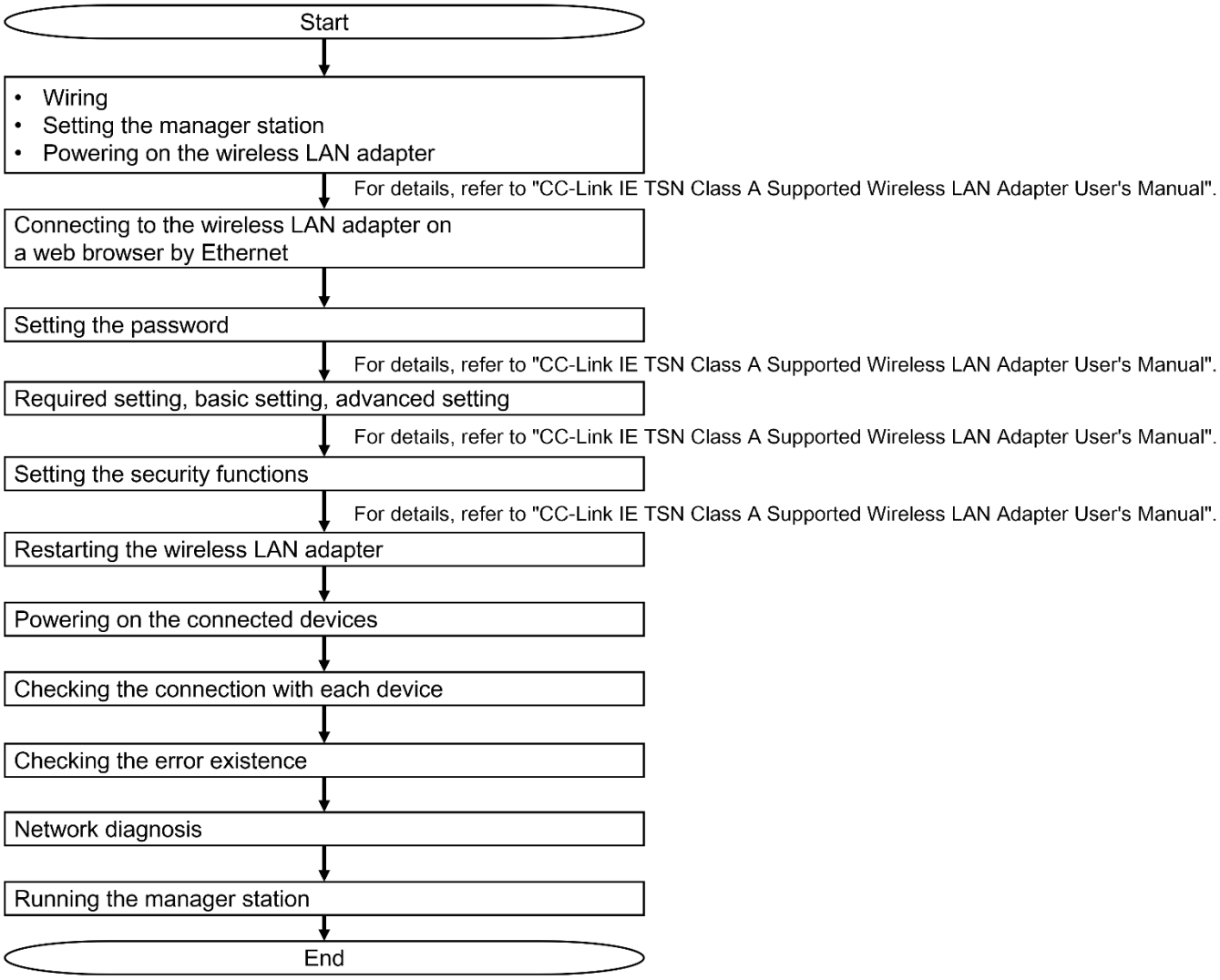


Figure 36 Procedure before operation

• Settings for the security functions of the wireless LAN adapter and the security policy

Perform the following items (Table 44) as the settings for the security functions of the wireless LAN adapter. In addition, when operating, please follow the implementation details described in Table 45.

Table 42 Setting the security functions of the wireless LAN adapter

No.	Item	Setting for the security function	Reference
1	Wireless encryption mode	Encryption shall be enabled to prevent communication interception.	4.4.1
2	Wireless authentication mode	Authentication shall be enabled to ensure the legitimacy of the communication partner.	4.4.2
3	Wired LAN MAC address filter	Accesses from external devices on the wired LAN side shall be restricted with the wired LAN MAC address filter.	4.4.3
4	Wireless LAN MAC address filter	Accesses from external devices on the wireless LAN side shall be restricted with the wireless LAN MAC address filter.	
5	Stealth SSID	The stealth SSID shall be enabled to prevent unintended devices from connecting.	4.4.4
6	Password authentication	Passwords shall be periodically changed.	4.4.5
7		Each password shall be difficult to guess.	
8	Logging function	Logs shall be periodically read to a personal computer since oldest entries will be overwritten when the storage size is exceeded.	4.4.6

Table 43 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 the wireless LAN adapter, delete the setting data and log data before disposal.	4.6
2	Connected devices	Verify prior to use that the equipment connected to the wireless LAN adapter is configured and operating as intended.	-
3	Performance and management of backups	Since there is a possibility that the protected assets (data) of the wireless LAN adapter and connected devices within the system may be lost due to sudden disaster or failure, etc., perform regular backups and manage the backup data appropriately.	4.4.7 4.5
4	Password management	Passwords shall be properly managed to prevent leakage and shall not be reused.	4.4.5
5	Management of SSID	SSIDs shall be properly managed to avoid using the same SSID as wireless devices for other purposes.	-
6	Management of encryption key	Encryption keys to be used in the wireless encryption mode and wireless authentication mode shall be properly managed to prevent leakage and shall not be reused.	-
7	Management of channel	Channels shall be properly managed to avoid using the same channel as wireless devices for other purposes.	-

4.4. How to set and use security functions and options

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

For the operation procedures of the function, refer to "CC-Link IE TSN Class A Supported Wireless LAN Adapter User's Manual".

This section describes the following security functions.

- Wireless encryption mode (Section 4.4.1)
- Wireless authentication mode (Section 4.4.2)
- Wired LAN MAC address filter (Section 4.4.3)
- Wireless LAN MAC address filter (Section 4.4.3)
- Stealth SSID (Section 4.4.4)
- Password authentication (Section 4.4.5)
- Logging function (Section 4.4.6)
- Backup/restoration function (Section 4.4.7)
- Initialization function (Section 4.4.8)
- Firmware update function (Section 4.4.9)

4.4.1. Wireless encryption mode

Wireless communications are encrypted using the following wireless encryption modes. Set the same wireless encryption mode for the access point and station.

- AES
- TKIP
- AUTO(TKIP/AES)

4.4.2. Wireless authentication mode

Encryption is performed using the following combinations of authentication modes and encryption modes. Set the same wireless encryption mode for the access point and station.

Table 44 Combinations of authentication modes and encryption modes

Authentication mode	Encryption mode
WPA3-Personal	AES
WPA2-Personal	AES
WPA/WPA2-Personal	AUTO(TKIP/AES)
WPA3-Enterprise 192-bit security	AES
WPA3-Enterprise	AES
WPA2-Enterprise	AES
WPA/WPA2-Enterprise	AUTO (TKIP/AES)
Enhanced Open	AES

4.4.2.1. Precautions

The following shows the precautions on using this function.

- Write the certificate generated in the RADIUS server to the wireless LAN adapter.
- WPA3 is a stronger authentication function than the previous WPA2 or WPA, therefore we recommend using WPA3.
- Set passwords that are difficult for third parties to guess.
- When STA is set to Enhanced Open, it will not be connected to Open APs to avoid plaintext communication.
- Operating the authentication information, such as encryption keys, at its default value results in security vulnerabilities. Before using this function, change the authentication information, such as encryption keys, and then enable the function.

4.4.3. Wired LAN MAC address filter/wireless LAN MAC address filter

Restrict connections to the wireless LAN adapter via wired LAN/wireless LAN with the MAC address of the connected device.

The MAC address 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 MAC filter function to secure the wireless LAN adapter and system against attacks such as illegal access from external devices in accordance with the concept of defense in depth.

4.4.4. Stealth SSID

Preventing the wireless LAN adapter (AP) from notifying its SSID to wireless client devices limits unnecessary connections to the wireless LAN adapter (AP). Register the SSID of the wireless LAN adapter (AP) only to the wireless LAN adapter (STA) or wireless client devices to be connected.

4.4.5. Password authentication

Access to the web interface of the wireless LAN adapter is restricted through password authentication.

4.4.5.1. Precautions

The following shows the precautions on using this function.

- Password authentication cannot be disabled.
- Set a password that is difficult for third parties to guess. Also, manage the set password so that it is not disclosed to third parties.
- If you lose your password, reset it.

4.4.6. Logging function

Status of the connection to the wireless LAN adapter and event information are stored in the built-in memory of the wireless LAN adapter. The saved logs can be checked with the web interface and backed up in text format to the personal computer currently accessing it.

4.4.7. Backup/restoration function

The backup function encrypts the settings of the wireless LAN adapter and backs them up to a folder on your personal computer. The restoration function restores the backed up settings to the wireless LAN adapter.
It is recommended that the settings be backed up periodically using 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.
If the restoration fails, the backup data has been manipulated or rewritten. Do not use the backup data in question, but use other backup data.

4.4.7.1. Precautions

The following shows the precautions on using this function.

- The backup file does not contain the certificate or password of the authentication server.
- Restoration cannot be performed for the wireless LAN adapter with a different password from the wireless LAN adapter for which backup was performed.
- Do not modify the backup file after saving it. If the backup file is modified, the behavior during restoration cannot be guaranteed.

4.4.8. Initialization function

This function restores the settings in the wireless LAN adapter to their factory default settings. When disposing of the wireless LAN adapter, it is recommended that this function be used to delete the setting information.
When using a wireless LAN adapter for which the initialization function has been used once again, configure the password authentication setting again.
The initialization function only initializes the setting data, and the log data will not be deleted. The log data must be deleted individually using the logging function.

4.4.9. Firmware update function

The firmware update function updates the firmware of the wireless LAN adapter via the web interface.

4.4.9.1. Precautions

The following shows the precautions on using this function.

- Check that the firmware version that can be checked with the web interface is correctly updated.
- Download the firmware update file from the MITSUBISHI ELECTRIC FA Global Website[16]. 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 updates as necessary.
- Since the operations of the wireless LAN adapter cannot be guaranteed during the update, check that the wireless LAN adapter 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.

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

4.5. Operation and maintenance of the wireless LAN adapter

4.5.1. Recommended operation example of the wireless LAN adapter

As physical security measures on the wireless LAN adapter, restricting access to certain areas in the factory and installing the wireless LAN adapter in a secure location where it can be monitored (e.g., installing on the top of the control panel or inside resin boxes and fixing with wire locks) 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 wireless LAN adapter communicates with a personal computer (maintenance personal computer or production management personal computer) via a network. The setting of the wireless LAN adapter can be changed using the web browser of the personal computer. To prevent these personal computers from being compromised, which could lead to the leakage of settings related to encrypted communications and others of the wireless LAN adapter or changes to settings that permit unauthorized device connections, implementing the following security measures on the personal computers that are connected to the wireless LAN adapter 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 wireless LAN adapter 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. Additionally, when communicating with the wireless LAN adapter from personal computers outside the trusted boundary, restrict the personal computers that can be connected using the MAC address filter function or similar methods.

As a part of the continuous security operations in the factory where the wireless LAN adapter is installed, performing the check items related to each function as shown in Table 47 is recommended.

Table 45 Item to be checked for continuous security operations

No.	Function name	Check item
1	Backup	Back up the settings in preparation for a product failure.
2	Checking the obtained logs	To detect suspicious behavior, checking the logs obtained with the logging function is useful. For example, the devices connected to the wireless LAN adapter and the history of setting changes can be checked. Also, check the history of the error occurrence 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 wireless authentication mode. If the certificate expires, communications will not be performed properly. Renew the certificate.

For using the wireless LAN adapter, selecting an appropriate person as the administrator is recommended. It is recommended that users of the wireless LAN adapter receive adequate education and training to properly set, manage, and operate the product. Use the wireless LAN adapter appropriately in accordance with the operation manual and this guideline.

4.5.2. Periodic maintenance

Perform security maintenance periodically (at least once a year recommended) to secure your systems and wireless LAN adapter. Specifically, checking the normal operations of the functions listed in Table 48 is recommended. In addition, Table 49 lists the functions where the function settings affect security. Periodically check that these settings are correct as well.

Table 46 Operation verification item of the security function

No.	Function name	Check item
1	Initialization function of the wireless LAN adapter	After performing an initialization operation on a wireless LAN adapter with various settings configured, accessing the adapter via a web browser shall display the login password setting window. * When the initialization function of wireless LAN adapter is performed for this verification, all the settings are initialized. Therefore, back up the settings before verification.
2	Firmware update function	Firmware update using the firmware update information file for wireless LAN adapters shall succeed, and result in the intended firmware version.
		Firmware update using the firmware update information file for other than wireless LAN adapters shall fail and firmware version is not changed from the original version.
3	Password authentication function	The user shall be able to log in to the web interface only when the correct password is entered.
		If an incorrect password is entered and the user fails to log in, a login error page shall be displayed.
4	Logging function	Event logs shall be saved in the web interface operation log.
		Wireless LAN connection logs shall be saved in the web interface wireless LAN log.
5	Backup function of the wireless LAN adapter	Backups shall be executed via the web interface, and backup files shall be saved on the personal computer currently accessing the system.
6	Restoration function of the wireless LAN adapter	Restoring a setting file that was backed up via the web interface shall revert the setting to its state at the time of backup.
7	Wireless authentication mode	When communicating with a wireless LAN adapter (STA) into which a certificate created on the target RADIUS server has been imported, the connection history shall be saved in the wireless LAN log.
		When communicating with a wireless LAN adapter (STA) into which a certificate created on a server other than the target RADIUS server has been imported, the unauthorized device connection history shall be saved in the event log.

No.	Function name	Check item
8	Wireless encryption mode	When a wireless LAN adapter (AP) and a wireless LAN adapter (STA) with the same wireless encryption mode communicate with each other, the connection history shall be saved in the wireless LAN log.
9	Wired LAN MAC address filter/wireless LAN MAC address filter	Wireless client devices with MAC addresses that differ from the specified ones shall not be connected.
10	Stealth SSID	The wireless LAN adapter (AP) with the stealth SSID enabled shall not be detected through access point search for the wireless LAN adapter (STA).

Table 47 Setting check item of the security function

No.	Function name	Check item
1	Wired LAN MAC address filter/wireless LAN MAC address filter	Check the MAC addresses of devices that can access the wireless LAN adapter. If MAC addresses of unnecessary devices remain, delete their registration information.

4.6. Removal and disposal of the wireless LAN adapter

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

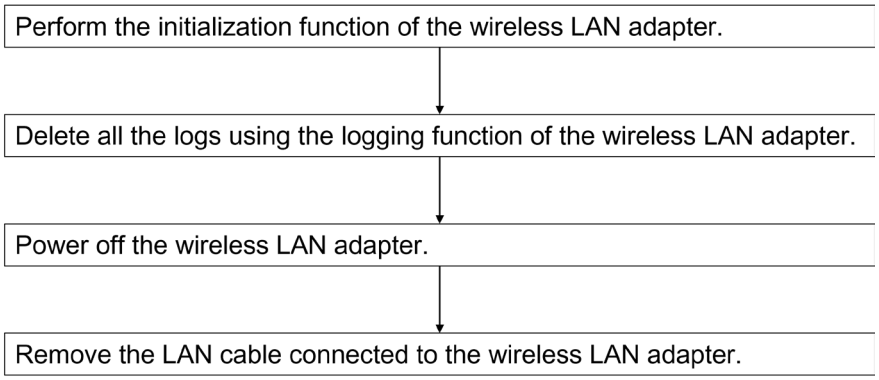


Figure 37 Removal method of the product

If the data needs to be backed up before deleted, use the backup function to make a backup.

If the 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.

To ensure the control stability of the entire factory, check that communication disconnections caused by wireless LAN adapter shutdowns do not affect the connected devices before proceeding with the appropriate steps in the operation manual.
When removing a device connected to the wireless LAN adapter in the system, there is a possibility that protected assets are stored in that device. Take measures such as deleting the data before removing it so that the information cannot be retrieved.

5. Contact information for security issues

We collect information on product vulnerabilities from external security researchers and coordinating bodies (such as domestic and foreign CERTs[17]) 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/

[17] Computer Emergency Response Team

6. 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. Mitsubishi Electric’s Approach to FA Security“ 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 “2. Mitsubishi Electric’s Approach to FA Security” of the “FA System 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] 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 development lifecycle” 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.