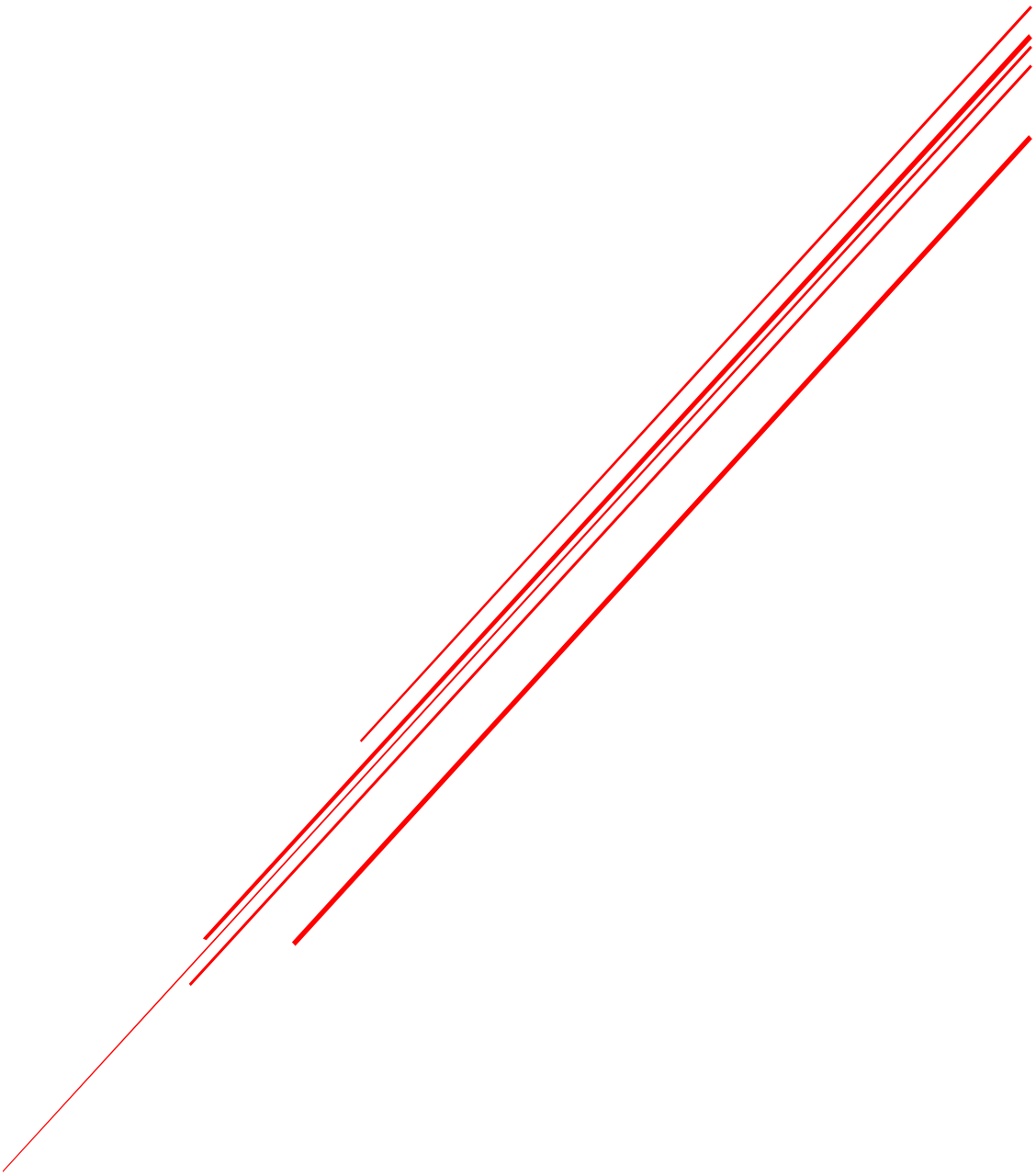
FA SYSTEM SECURITY GUIDELINE

[FREQROL] Edition



MITSUBISHI ELECTRIC CORPORATION

BCN-C22005-1054

Revision history

Date	Document number	Notes
Jan, 2025	BCN-C22005-1054	First edition

Table of content

Contents

1. Introduction 2

1.1 Background 2

1.2 Multi-layer defense strategy to protect FA products 3

2. Security function of FR-D800 series 4

2.1 Position of this chapter 4

2.2 Security Strategy for FR-D800 5

2.2.1 Assumed Usage Environment for the FR-D800 5

2.2.2 Considerations for the FR-D800 8

2.2.3 Countermeasures against threats 9

2.2.4 Security measures to be taken outside the product. 11

2.3 Implementation items regarding security policies and usage environment 13

2.4 Operation and Maintenance of the FR-D800 14

2.4.1 Recommended practices for operating the FR-D800 14

2.4.2 Regular maintenance 14

2.5 Regarding the removal and disposal of the FR-D800 15

3. Contact Information for Security Issues 16

Terms and Definitions

Term	Description
FA [1]	Factory Automation**.** The use of computer control technology to automate factories. It also refers to the equipment used for automation. It is also referred to as Industrial Automation
IEC62443 [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 the ISA99 committee and adopted by the International Electeotechnical Commission (IEC)
Confidentiality [3]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity [4]	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Availability [5]	The state that exists when data can be accessed, or a requested service provided within an acceptable period of time.
Supply chain [6]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Vulnerability [7]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Security key authentication	A function implemented in the PLC CPU to prevent unauthorized browsing and execution of programs. The project data locked with a security key can be viewed only with the engineering tool registered with the same security key. In addition, a programs locked with a security key can be executed only with a module to which the same security key is regised.
File password	A function that prevents unauthorized reading/writing of file using a password.
Remote password	A password that prevents unauthorized access to the PLC CPU from remote users.
Block password	A function that prevents unauthorized browsing of programs using a password.
Service setting function	A function that sets Enable/Disable for services on a FA product such as C controller. This function requires security password therefore unauthorized access can be prevented.

[1] Mitsubishi Electric FA Terminology Dictionary, https://www.mitsubishielectric.com/fa/assist/fa_reference/pdf/k-027-k1209.pdf

[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, the utilization of IT in FA (Factory Automation) systems is progressing with the aim of improving factory productivity. As IT usage in FA systems advances, the traditional thinking that FA systems are "dedicated systems" or "closed (isolated) networks" that are immune to malware infection or cyberattacks is no longer valid. The security risks to FA systems have been increasing. In fact, in 2017, IT systems became a target of cyberattacks...The malware, known as [name of malware], caused significant damage, including halting factory operations (Figure 1).

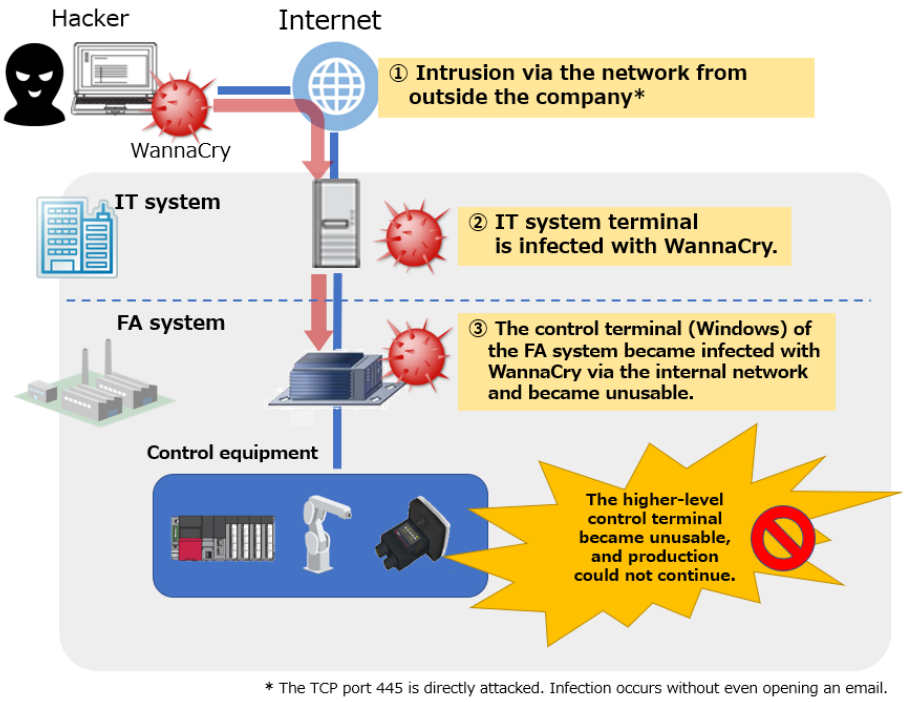


Figure 1: Infection Path and Example of Damage from WannaCry in FA Systems

To protect FA systems from such threats, it is essential to combine multiple layers of security measures in a hierarchical manner, ranging from physical security measures for factory access control to human security measures such as rules and education for users handling products, as well as security measures for networks and FA equipment within the factory. This approach increases the "cost of attack for attackers and raises the barrier for attacks," as well as enhancing "detection and prevention capabilities in case an attack occurs." By improving security and reducing the impact of attacks, this approach helps to mitigate risks. This concept of security measures is called "multi-layer defense," and it is also recommended by the international standard IEC62443[6].

[6] For IEC62443, please refer to the "FA System Security Guidelines.

1.2 Multi-layer defense strategy to protect FA products

In security measures, multi-layer defense is the concept of applying different measures based on various perspectives, such as "human operations," "equipment and facility usage," "network access," "data access," and "application execution." At our company, we divide these perspectives into those related to the environment (outside the product) and those related to the product itself, defining them as "human layer," "physical layer," "network layer," and "device layer" (Figure 2). By implementing multi-layer defense, we raise the cost of attack for attackers and, in addition, enhance detection and prevention capabilities in case of an attack, thereby reducing the impact of attacks. The security features of our products are part of the measures in the device layer or network layer of multi-layer defense. To protect FA systems from cyberattacks, measures are needed across each layer: the human layer, physical layer, network layer, and device layer. For example, we recommend considering the installation of firewalls to prevent intrusions into factory networks, the introduction of antivirus software on computers, and access control management for the factory.

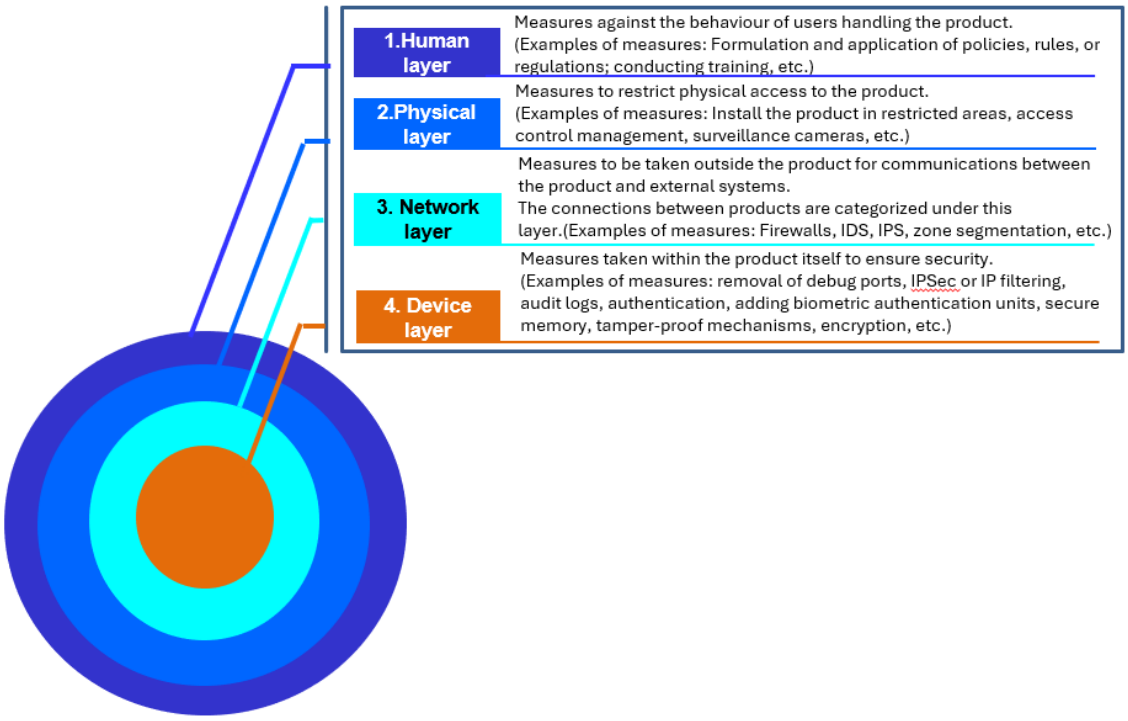


Figure 2: Concept of Multi-Layer Defense

2. Security function of FR-D800 series

2.1 Position of this chapter

In this chapter, we will explain our approach to the security of the FR-D800 and provide information to help you safely and securely use the FR-D800 in your FA systems. The following information will be included:

- FR-D800 Security Strategy (Chapter 2.2):
  We will clarify the threats assumed for the FR-D800 and describe the security measures to address these threats. These measures include both those performed solely on the FR-D800 and those involving combinations with other products.
- FR-D800 Operation and Maintenance Methods (Chapter 2.5):
  We will explain recommendations for user management and password management methods when operating the FR-D800.
- FR-D800 Removal and Disposal Methods (Chapter 2.6):
  We will describe the recommended methods for removing and disposing of the FR-D800, such as data deletion functions within the product.

For detailed specifications and operating procedures of each FR-D800 feature, please refer to the product manual as needed.
We encourage you to carefully read this guideline and the related manuals, and fully understand the security of the FR-D800 to help realize and maintain a safe and secure FA system.
Additionally, for the basic security policies for our FA products, efforts in product lifecycle management, and examples of FA system construction, please refer to the following document:

- FA System Security Guidelines

2.2 Security Strategy for FR-D800

In this chapter, we will explain the security strategy for the FR-D800, covering the following topics:

- The assumed usage environment for the FR-D800 (product installation environment, network, operation and maintenance methods, etc.)
- Threats to the FR-D800
- Countermeasures against these threats
- Security features provided by the FR-D800
- Security measures to be taken outside the product

2.2.1 Assumed Usage Environment for the FR-D800

The assumed environment for installing the FR-D800 is shown in **Figure 3**. Additionally, the preconditions for ensuring security in this installation environment are listed in **Table 1**. The usage environment, which includes these installation environments and preconditions, forms the basis for the security strategy described in the subsequent sections.

The FR-D800 is intended for use within equipment installed in the production area of a factory. This equipment includes not only the FR-D800 but also devices connected to the CC-Link IE TSN network, creating a trust boundary within the equipment. The maintenance computer, which connects to the FR-D800, is portable and can be used outside of the equipment, thus it lies outside the trust boundary. Furthermore, there is a server room in the factory, where production monitoring computers and various servers are installed. The network within the factory where the FR-D800 is installed is assumed to be connected through a firewall and router, not directly to the internet.

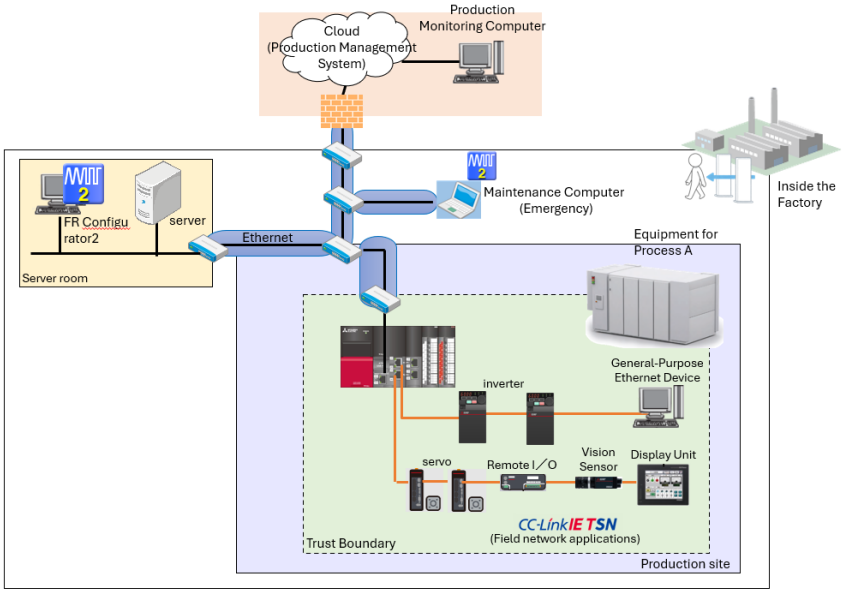


Figure 3: Assumed Environment for Installing the FR-D800

[7] This is the boundary that separates trusted areas from other areas. For example, security features such as authentication functions are often set up at the trust boundary. Users who successfully authenticate can enter the trusted area, while users who fail authentication are unable to access anything within the trusted are

Table 1 Assumptions for installation environment

No.	Assumption	Description
1	Implementation of entry and exit management	Access to the factory is restricted through entry and exit management.
2	Locking of equipment where the FR-D800 is installed	Equipment where the FR-D800 is installed is locked, and devices within the equipment cannot be operated or modified without the administrator's permission.
3	User education	Users receive sufficient education and training to appropriately configure, manage, and operate the FR-D800.
4	Selection of appropriate administrators	Administrators are selected based on their integrity and ability to perform management tasks responsibly.
5	Installation of a firewall	A network switch or firewall is installed between the network connected to the FR-D800 and external networks, blocking unnecessary communications from external sources.
6	Security of PCs communicating with the FR-D800	Computers communicating with the FR-D800 (e.g., maintenance PCs or production monitoring PCs) are equipped with antivirus software and other security measures to ensure protection.

Table 2 provides explanations for each device and network depicted in Figure 3.

Table 2 Devices, applications, and networks in the environment

No.	Terms	Description
1	Display	Devices connected to FR-D800 for operation and information display**:** An example of a display device for our products is the GOT2000 series.
2	Production monitoring PC	Devices with software installed to monitor the status of the control system.
3	Maintenance PC	Devices with engineering tools installed for maintaining FR-D800: An example of an engineering tool for our products is FR Configurator 2.
4	Field network	Network used for communication between FR-D800 and field devices**.**
5	Control information	Network inside the firewall used for communication between FR-D800 and production monitoring PCs: An example of a control information network is Ethernet.
6	Network	Devices equipped with packet filtering functions, bandwidth limiting functions, and address translation functions such as NAT (Network Address Translation) and NAPT (Network Address Port Translation)**.**
7	Firewall	Devices using network layer information from the OSI reference protocol to separate networks through virtual routers or VLAN (Virtual Local Area Network): A combination of network routers and switches can also be used.
8	Network switch	Network outside the firewall, where the factory's network management authority does not apply: An example of an external network is the internet.
9	External network	Devices that generate values to input into FR-D800 and output values generated by FR-D800: Examples of field devices are inverters and servos.

In a factory, access can be physically restricted by limiting entry to specific areas or by securing storage locations for equipment with physical locks. These physical access controls are also important security elements. In the use of the FR-D800, the area divisions shown in Table 3 are assumed from a security perspective.

Table 3 Area division and operational methods

No.	Terms	Description
1	Server Room	A room that houses devices critical for the continuous operation of the control system, such as network management devices. Protective measures (e.g., locking management to restrict entry to authorized personnel only) are implemented to prevent unauthorized access or destructive actions.
2	Equipment Area of Each Process	The area where devices such as FR-D800 are stored. Protective measures (e.g., locking management) are implemented to restrict access and operations to specific individuals who are authorized to enter the production site.
3	Production Site	An area where only users of the control system are allowed to enter.
4	Factory	An area that includes both the accessible zones and the server room.

2.2.2 Considerations for the FR-D800

Our company considers the usage environment of the FR-D800 as shown in Figure 3 of Section 2.1.1, and based on risk assessments of the product and insights from known attack cases, Figures 4 and Table 4 outline the factors influencing the FR-D800.

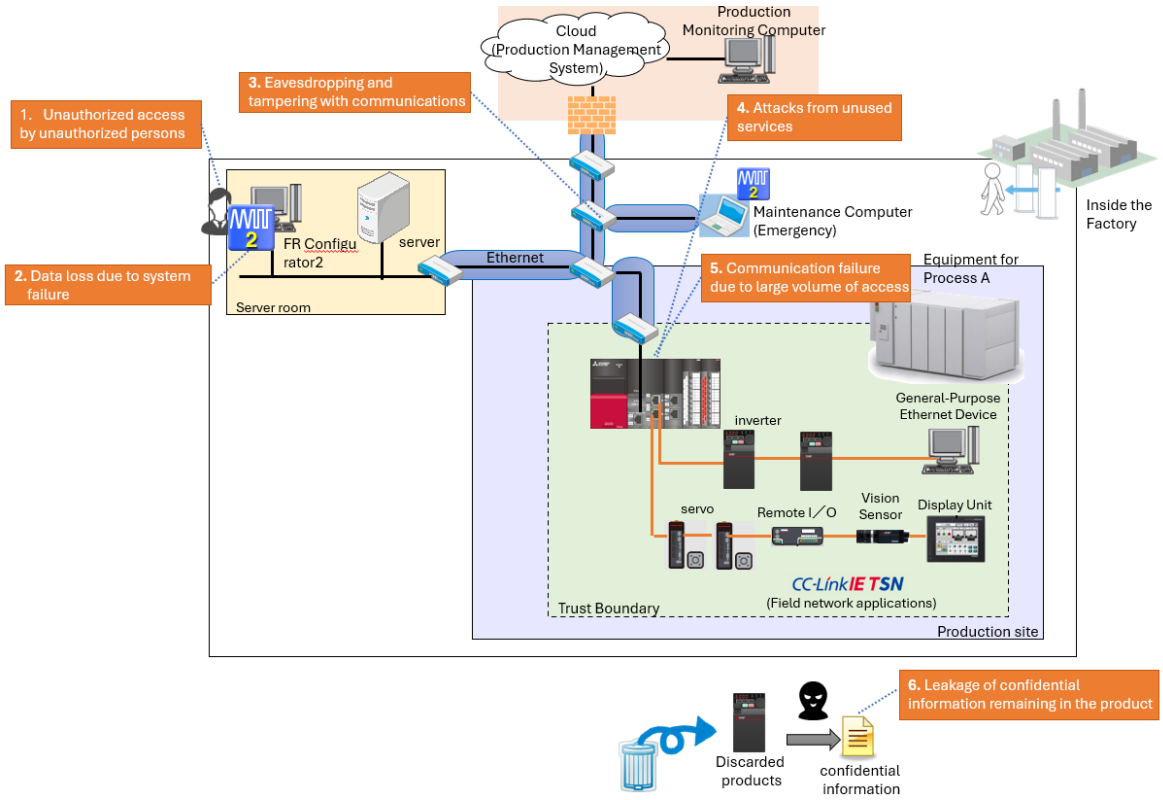


Figure 4: Considerations for FR-D800

Table 4 : Explanation of consideration points

No.	Point	Description
1	Unauthorized access by unauthorized persons	Unauthorized access by individuals not permitted by the administrator.
2	Data loss due to system failure	Loss of information stored in FR-D800 or making it unusable due to equipment failure caused by disasters or other factors.
3	Eavesdropping and tampering with communications	Eavesdropping or tampering with communications between FR-D800 and external systems.
4	Attacks from unused services	Unauthorized access through unused communication ports or protocols.
5	Communication failure due to large volume of access	Communication traffic within the network increases, preventing necessary communications.
6	Leakage of confidential information remaining in the product	Leakage of confidential information extracted from discarded products or equipment.

2.2.3 Countermeasures against threats

The statement describes the countermeasures against threats for the FR-D800, which are outlined in Figure 5. These countermeasures not only include actions taken by the FR-D800 itself but also those that need to be implemented in the customer's operational environment.

To realize the multi-layered defense discussed in section 1.2, security measures are required not only in the layers that the FR-D800 can address, but also in the human, physical, and network layers. Therefore, it is necessary to establish security measures not only for the FR-D800 itself but also for the entire FA system.

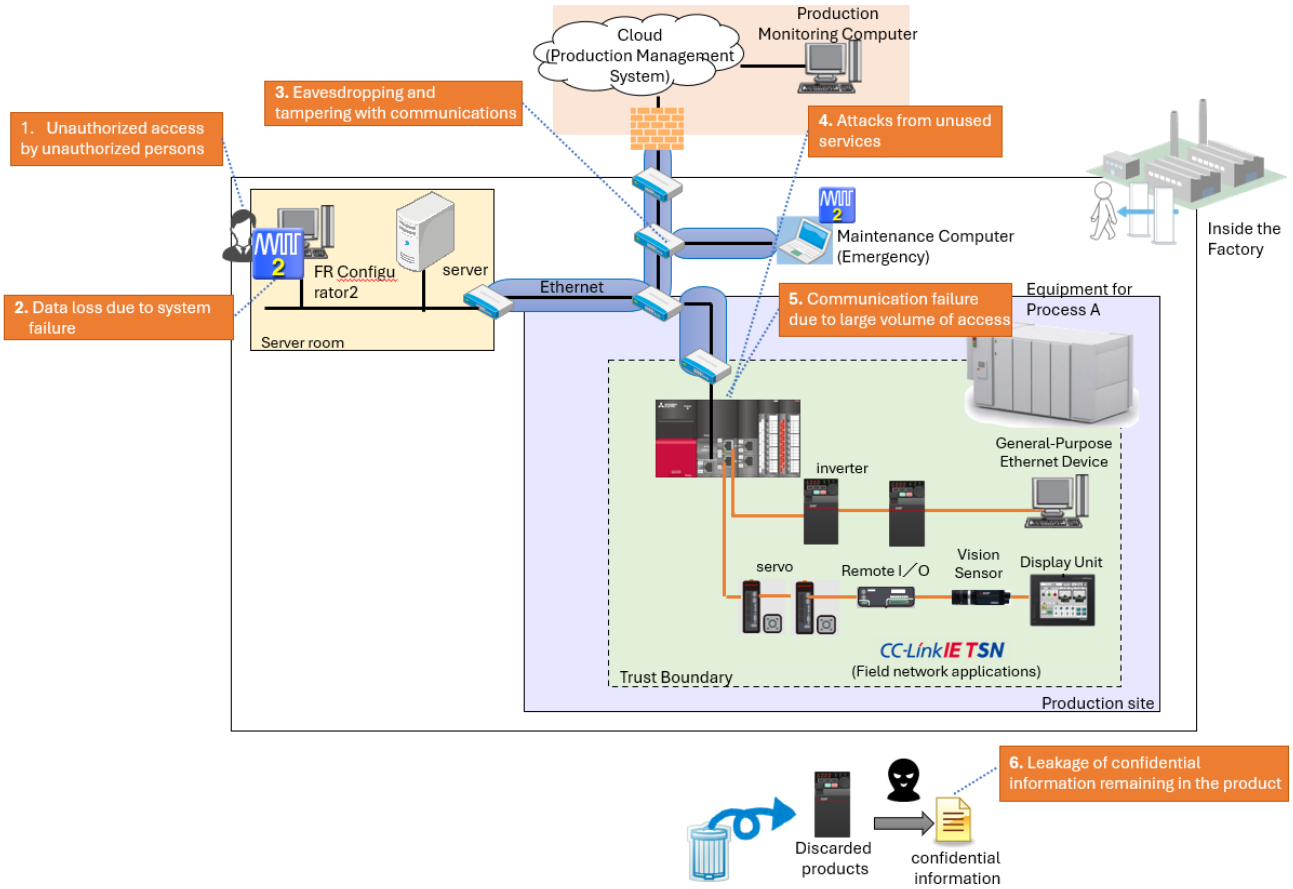


Figure 5: Countermeasures for threats in FR-D800

Table 5 Countermeasures for threats in FR-D800

No.	Points	Countermeasures	Related Countermeasures
1	Unauthorized access by unauthorized persons	• Proper permission settings • User identification	• User authentication functionality • Physical access restrictions • Selection of administrators • Installation of firewalls • PC security
2	Data loss due to failures	• Automatic backup of stored information • Planned backup strategy • System recovery using backup data	• Planned backup
3	Eavesdropping and tampering with communication	• Authentication and encryption of communications	• Encrypted communication functionality • Physical access restrictions • Installation of firewalls
4	Attacks from unused services	• Configuration of communication port usage	• Default open port usage settings • User education
5	Communication disruption due to heavy traffic	• Packet blocking • Bandwidth limitation	• IP filtering functionality • Bandwidth restriction for DoS attacks
6	Information leakage of confidential information remaining in products	• Deletion of confidential information upon termination of use	• Initialization of all controller information

2.2.4 Security measures to be taken outside the product.

The recommended security measures for the customer's operating environment, taking into account the preconditions (Table 1) and countermeasures for threats (2.2.3) in the FR-D800 usage environment (Figure 3), are shown in Figure 6 and Table 6.

Figure 6: Security Measures to be Implemented in the Operational Environment

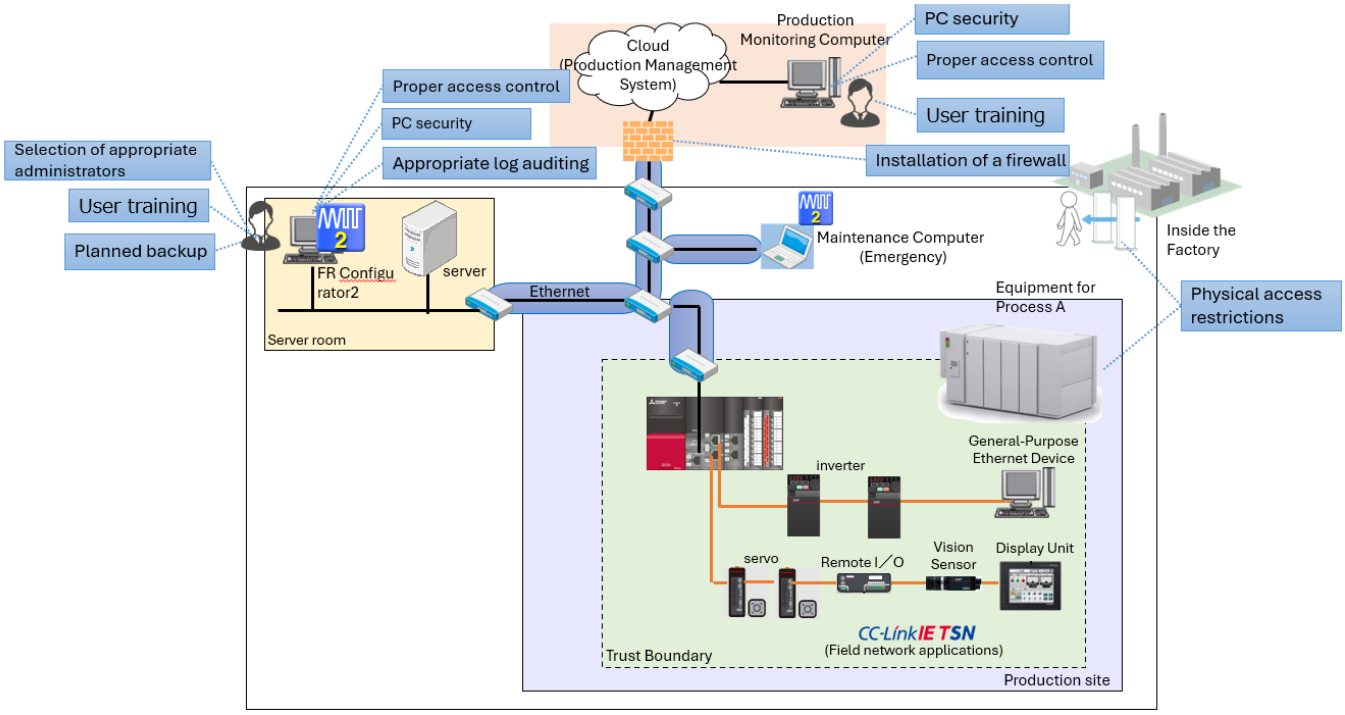


Table 6 Explanation of Security Measures in the Operational Environment

Layer of Defense	Countermeasure	Description	Threats Targeted
Physical layer	Physical access restriction	To prevent unauthorized access, place the inverter in a locked cabinet or similar secured environment that is inaccessible to outsiders.	1. Unauthorized access by people or devices 3. Eavesdropping and tampering with communications
Human layer	User training	Provide training to users on securing the FR-D800, covering the following topics: • Setting the allowable communication ports and protocols • Backup and restore settings	1. Unauthorized access by people or devices 2. Data loss due to failures
Human layer	Administrator selection	Select administrators who are trustworthy and unlikely to abuse their privileges.	1. Unauthorized access by people or devices
Human layer	Log auditing	Administrators should regularly audit system logs according to operation rules and manuals. Periodic checks should also be performed to ensure the integrity of the logs.	5. Loss of logs
Human layer	Planned backup	Implement scheduled backups to prevent forgetting to back up critical data.	2. Data loss due to failures

Network layer	Firewall Installation	Install firewalls to prevent unauthorized access from external networks.	1. Unauthorized access by people or devices 3. Eavesdropping and tampering with communications
Device layer	PC Security	Ensure proper security measures, such as antivirus software, are implemented on PCs (maintenance PCs and production management PCs) that communicate with FR-D800.	1. Unauthorized access by people or devices 3. Eavesdropping and tampering with communications 5. Loss of logs

2.3 Implementation items regarding security policies and usage environment

This chapter explains the implementation items regarding security policies and usage environment.

Table 7 Implementation Items Regarding Security Policies and Usage Environment

No.	Item	Action	Reference
1	Caution when removing/disposing of connected devices	When removing or disposing of devices connected to the FR-D800, ensure to erase any data stored on the device before disposal, as it may contain protected assets (data).	2.5
2	Connected devices	Verify that the devices connected to the FR-D800 are properly configured and executed before use.	-
3		Terminate the session promptly when communication with connected devices is no longer required.	-
4	Backup implementation and management	Perform regular backups to prevent loss of protected assets (data) in case of sudden disasters or failures, and manage backup data properly.	2.5
5	Password management	Properly manage passwords to prevent leaks, and avoid reusing passwords.	-
6	Trusted boundary	Use SNTP, FTP, BACnet, Modbus communication, and other devices connected through the CC-Link IE TSN port within the trusted boundary.	-

2.4 Operation and Maintenance of the FR-D800

2.4.1 Recommended practices for operating the FR-D800

As a physical security measure for the FR-D800, it is recommended to implement area access restrictions within the factory and to install the FR-D800 in a secure and monitored location (such as a device or a locked cabinet) to protect it from unauthorized access and physical destruction. In particular, rooms containing network management devices or other critical devices for the continuous operation of the control system should be differentiated from other areas, with lock management to ensure that only authorized personnel can enter or exit.

The FR-D800 communicates with PCs (maintenance PCs and production management PCs) via the network. Engineering software can be installed on these PCs, enabling the manipulation of files stored on the FR-D800. To prevent breaches and ensure that files stored on the FR-D800 are not leaked or written with unintended operations, the following security measures are recommended for PCs connected to the FR-D800:

- Theft prevention measures such as wire locks for PCs
- Access control for PC users
  - Only authorized personnel should be able to log into the PC
  - Strict management of login information
  - Introduction of fingerprint authentication
- Installation of antivirus software

To protect the trusted boundaries where the FR-D800 is installed or the network where the PCs are located from unnecessary external access, it is recommended to install network devices such as firewalls and routers at the boundary between the factory's network and the Internet, or on the outside of the trusted boundary. Additionally, if a PC located outside the trusted boundary communicates with the FR-D800, the port numbers set for encrypted communication should be configured in the firewall's packet filter allowlist along the communication path.
When using the FR-D800, it is recommended to appoint an appropriate person as the administrator. Additionally, it is advised to provide sufficient education and training for the users of the FR-D800 to ensure proper setup, management, and operation. The operation of the FR-D800 should be in accordance with the instruction manual and these guidelines.

2.4.2 Regular maintenance

To ensure the safety of the system and inverter, it is recommended to perform regular security maintenance, at least once a year, as shown in Table 5.

2.5 Regarding the removal and disposal of the FR-D800

If the disposal or transfer of the product is not done properly, there is a possibility of data leakage from the product. To prevent data leakage, when discontinuing the use of the product, please ensure to perform a full information reset (All Clear) before removing and disposing of the product. If data backup is necessary, save the inverter's parameter settings (parameter list) using tools such as FR Configurator2.

For the stability of the entire factory's control system and the protection of data stored within the system, please ensure to follow the correct procedure as outlined in the user manual after shutting down the system when stopping the FR-D800.

Additionally, when removing equipment connected to the FR-D800 within the system, there may be protected assets stored on the equipment. Please ensure to delete data and take measures to prevent the retrieval of information before removal.

3. Contact Information for Security Issues

To improve the information security quality of our products, we collect information regarding vulnerabilities from external security researchers and coordination bodies (such as CERT[8] both domestically and internationally). For information regarding vulnerabilities in our products, please contact the relevant coordination body or reach out to us through the contact form on our website.

Mitsubishi Electric Product Vulnerability Reporting Desk (Contact Form)

https://www.mitsubishielectric.co.jp/psirt/contact/

[8] Computer Emergency Response Team