FA SYSTEM SECURITY GUIDELINE

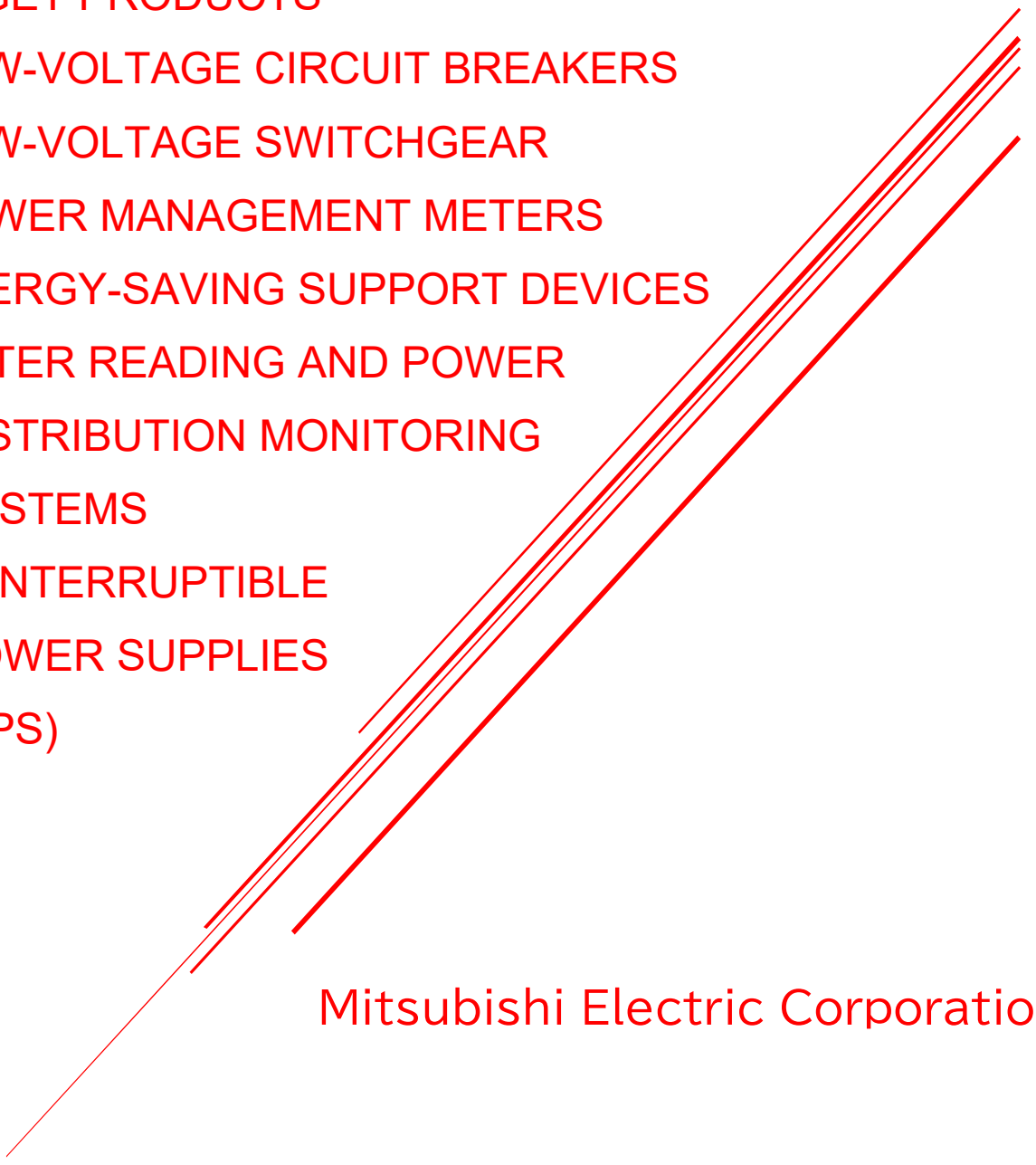
- SEPARATE VOLUME

[POWER DISTRIBUTION AND CONTROL EQUIPMENT] -

V1.0

TARGET PRODUCTS

- LOW-VOLTAGE CIRCUIT BREAKERS
- LOW-VOLTAGE SWITCHGEAR
- POWER MANAGEMENT METERS
- ENERGY-SAVING SUPPORT DEVICES
- METER READING AND POWER DISTRIBUTION MONITORING SYSTEMS
- UNINTERRUPTIBLE POWER SUPPLIES (UPS)



Mitsubishi Electric Corporation

IB63K18(ENG)

Revision History

Date	Document number	Notes
June 2026	IB63K18(ENG)	First edition

Contents

1 Introduction 1

1.1 Background 1

1.2 Defense-in-Depth Strategy for Protecting Power Distribution and Control Equipment 2

1.3 Purpose and Usage of This Document 3

1.4 Disclaimer 3

2 Mitsubishi Electric Security Initiatives 4

2.1 Basic Security Policy for Power Distribution and Control Equipment 4

2.2 Mitsubishi Electric Initiatives for Cybersecurity 4

2.3 Product-Specific Security Initiatives for Power Distribution and Control Equipment 4

3 Security Strategy for Power Distribution and Control Equipment 6

3.1 Expected Operating Environment 6

3.2 Threats to Power Distribution and Control Equipment 9

3.3 Security Countermeasure Policies 10

3.4 Overview of Security Functions 11

3.4.1 Authentication Screen 11

3.4.2 Operation History 12

3.5 Supplier Risk Management Activities 12

3.6 Security Support Policy 12

3.6.1 Scope of Support 13

3.6.2 Support Period 13

4 Secure System Construction and Operation by Customers 14

4.1 Installation of Power Distribution and Control Equipment 14

4.2 Operation and Maintenance of Power Distribution and Control Equipment 14

4.2.1 Examples of Secure Operation 14

4.2.2 Periodic Maintenance 16

4.3 Removal and Disposal of Power Distribution and Control Equipment 16

5 Security Contacts 17

5.1 Disclosure of Vulnerability Information 17

Appendix A Inquiries Regarding This Document 18

Terms and Definitions

Term	Definition
IT	Information Technology. A collective term for technologies related to computers, software, and networks.
IoT	Internet of Things. A concept in which various devices and equipment, such as vehicles, home appliances, robots, and facilities, are connected to the Internet to exchange information, enabling automation and creating new value.
FA	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.[1]
Confidentiality	Ensuring that information is accessible only to authorized persons. Unauthorized users must be prevented from accessing or modifying protected information.
Integrity	Maintaining the accuracy, completeness, and trustworthiness of information. Information must not be altered or destroyed without authorization.
Availability	Ensuring that authorized users can access required information and services whenever needed. In industrial control systems, availability also refers to the continuous operation of equipment and facilities during their intended service period.
Security Incident	An event that exposes information systems or control systems to security threats. Also referred to as a cybersecurity incident.
Supply Chain	The flow of materials and information throughout business activities, from procurement and production through inventory management and product delivery.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.[2]
PSIRT	Product Security Incident Response Team. An organization responsible for handling product security incidents and vulnerabilities relating to products manufactured or sold by a company.
IPA	Information-technology Promotion Agency, Japan. An independent administrative institution that promotes cybersecurity measures, information security awareness, and information technology safety initiatives.
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center. An organization that receives reports of cybersecurity incidents, provides technical assistance, performs threat analysis, and supports incident response activities in Japan.
IPS	Intrusion Prevention System Intrusion prevention system. A system that detects unauthorized intrusions via a network and blocks the network in question. While the IDS only notifies of the detection of an intrusion, the IPS automatically blocks communications when an intrusion is detected, preventing the intrusion.
IDS	Intrusion Detection System Intrusion detection system. A system that detects unauthorized intrusions via a network and notifies users of them.
VPN	Virtual Private Network A technology that ensures the security on communication paths by establishing a virtual dedicated line over the Internet or public lines for communications using technology such as encryption.

[1] Mitsubishi Electric FA Terminology Dictionary https://www.mitsubishielectric.co.jp/fa/glosup/fa_reference/index.html
[2] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/vulnerability

1 Introduction

1.1 Background

With the rapid advancement of the Internet, Information Technology (IT), and Internet of Things (IoT) technologies, the utilization of IT within factories has also expanded significantly.

Traditionally, factory systems were often regarded as being immune to malware infections and cyberattacks because they were considered dedicated and closed systems operating within isolated environments.

However, as IT utilization in factory systems has increased, cybersecurity risks have also become increasingly significant.

In 2017, a major cybersecurity incident occurred when malware known as WannaCry targeted Factory systems used for industrial automation, causing production shutdowns at multiple manufacturing facilities (see Figure 1).

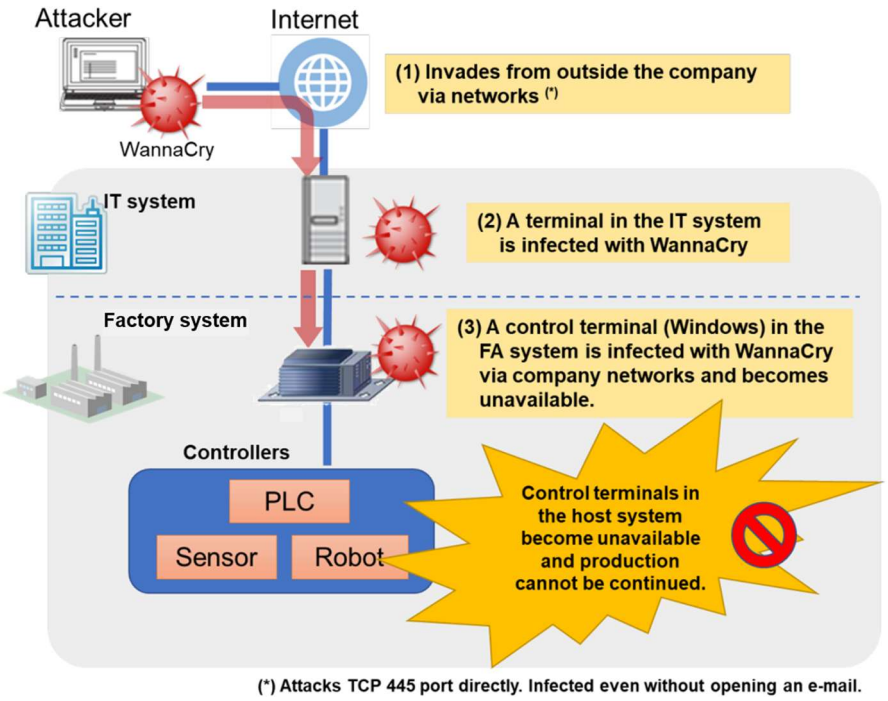


Figure 1. Example of WannaCry Infection Paths and Security Incidents in Factory Systems

To protect factory systems from such threats, it is important to implement multiple layers of security measures, ranging from physical security controls such as facility access management to cybersecurity measures for factory networks and system products.

By adopting multiple security measures in a layered manner:

- The cost of attack for malicious actors is increased.
- The barriers to successful attacks are raised.
- Detection and prevention capabilities are strengthened.
- The opportunities for attacks and their potential impacts are reduced.

This approach is commonly referred to as Defense-in-Depth and is recommended by various international standards and industry best practices.

As a manufacturer and supplier of products used in industrial facilities, Mitsubishi Electric develops products with a Defense-in-Depth philosophy to support customers in achieving and maintaining secure and reliable systems.

1.2 Defense-in-Depth Strategy for Protecting Power Distribution and Control Equipment

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 attacks for the attacker and enhancing detection and prevention capabilities in the event of an attack.

The security function of 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, typical measures include the installation of a firewall to protect against cyberattacks, installation of antivirus software on personal computers, access control in the factory, and installation in locked equipment enclosures.

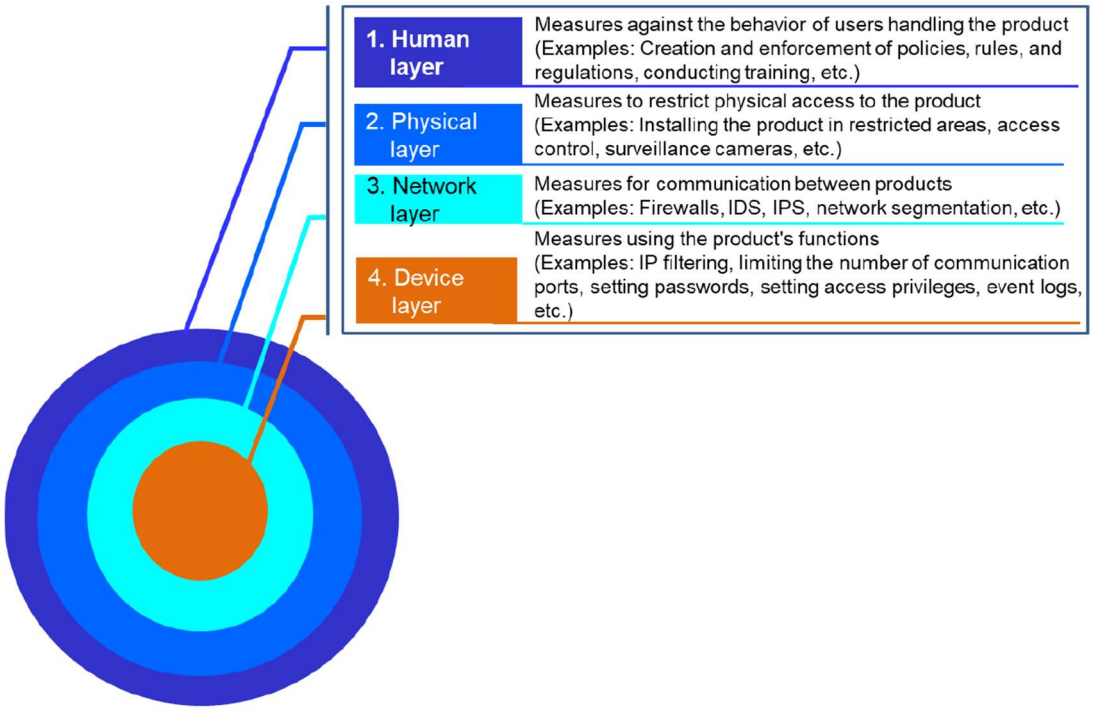


Figure 2. Defense-in-Depth Concept

1.3 Purpose and Usage of This Document

The purpose of this document is:

1. To help customers understand Mitsubishi Electric's approach to the security of power distribution and control equipment.
2. To provide recommendations that customers should consider when using these products.

Unless otherwise specified, the term "product" in this document refers to Mitsubishi Electric power distribution and control equipment.

This document is intended to be used in conjunction with the FA System Security Guideline (XFB3-20PS001). It summarizes product-specific characteristics and highlights differences from the general FA System Security Guideline where applicable.

Table 1. Purpose of Each Chapter

Chapter	Title	Purpose
Chapter 2	Mitsubishi Electric Security Initiatives	Understanding Mitsubishi Electric's security philosophy and activities for product security
Chapter 3	Security Strategy for Power Distribution and Control Equipment	Establishing security policies for your operating environment
Chapter 4	Secure System Construction and Operation by Customers	Building and operating systems with security considerations
Chapter 5	Security Contacts	Contact points when communication with Mitsubishi Electric is required

1.4 Disclaimer

The security information described in this document has been prepared based on analyses and evaluations conducted by Mitsubishi Electric.

Appropriate security measures vary depending on the customer's specific operating environment.

Accordingly, compliance with the recommendations described in this document does not guarantee prevention of all possible security incidents that may occur within a customer's environment.

2 Mitsubishi Electric Security Initiatives

2.1 Basic Security Policy for Power Distribution and Control Equipment

This section explains Mitsubishi Electric's basic product security policy.

Mitsubishi Electric is committed to providing safe, secure, and reliable products based on domestic and international concepts and standards for control system security.

In cooperation with partner companies, Mitsubishi Electric continuously undertakes activities aimed at maintaining and improving the following six elements within customers' operating environments:

- Health: Health of people associated with Mitsubishi Electric products
- Safety: Safety of people associated with Mitsubishi Electric products
- Environment: Protection of the environment surrounding Mitsubishi Electric products
- Availability: Continuity of factory operations and availability of data
- Integrity: Integrity of data
- Confidentiality: Confidentiality of data

As a company providing power distribution solutions and other related services for industrial facilities, Mitsubishi Electric continuously strengthens cybersecurity measures to ensure safe and secure operating environments for customers.

These efforts contribute to:

- Maintaining Health, Safety, and Environment (HSE)
- Maintaining and improving Availability, Integrity, and Confidentiality (AIC)

Protecting factories from cyberattacks that could compromise Availability, Integrity, or Confidentiality also helps reduce the risk of incidents affecting Health, Safety, and Environment.

For this reason, this document primarily focuses on measures that support the maintenance and improvement of:

- Availability
- Integrity
- Confidentiality

2.2 Mitsubishi Electric Initiatives for Cybersecurity

For detailed information regarding Mitsubishi Electric's cybersecurity initiatives, refer to Section 2.2 of the FA System Security Guideline (XFB3-20PS001).

Power distribution and control equipment security activities are conducted in accordance with the same principles applied to Mitsubishi Electric's Factory Automation cybersecurity initiatives.

2.3 Product-Specific Security Initiatives for Power Distribution and Control Equipment

In accordance with the basic policy described above, Mitsubishi Electric provides information regarding its approach to product security and guidance to help customers use products safely and securely within their systems.

The following information is provided:

Security Strategy for Power Distribution and Control Equipment (Chapter 3)

To clearly identify threats relevant to products and establish security countermeasure policies, the following topics are described:

- Expected Operating Environment (Section 3.1)
- Threats to Power Distribution and Control Equipment (Section 3.2)
- Security Countermeasure Policies (Section 3.3)

The countermeasure policies include:

- Measures implemented within the product itself
- Measures implemented through combinations of products and surrounding systems

Security Functions of Power Distribution and Control Equipment (Section 3.4)

This document also outlines the security functions provided by products.

In addition, precautions and recommendations for mitigating product security risks are described.

Additional Activities Necessary for Security Assurance

The following topics are also addressed:

- Supplier Risk Management Activities (Section 3.5)
- Security Support Policy (Section 3.6)

Secure System Construction and Operation by Customers (Chapter 4)

This chapter describes actions customers should take when deploying and operating Mitsubishi Electric products securely.

Topics include:

Installation of Power Distribution and Control Equipment (Section 4.1)

Recommendations regarding appropriate installation methods and secure use of product functions.

Operation and Maintenance of Power Distribution and Control Equipment (Section 4.2)

Recommendations regarding operational management, maintenance practices, and security considerations during system operation

Product Removal and Disposal (Section 4.3)

Recommendations regarding deletion of product data and other security considerations when products are removed, transferred, or disposed of.

Customers are encouraged to carefully read this guideline together with the manuals for their respective products in order to fully understand the security characteristics of the products and to support the realization and maintenance of safe and secure systems.

3 Security Strategy for Power Distribution and Control Equipment

This chapter describes the strategy for ensuring security through product security functions and operational measures, covering the following topics:

- Expected Operating Environment (product installation environment, network configuration, operation, and maintenance methods)
- Threats to Power Distribution and Control Equipment
- Security Countermeasure Policies
- Overview of Product Security Functions
- Security Support Policy

3.1 Expected Operating Environment

Figure 3 shows the expected operating environment, while Table 2 lists the security assumptions for each installation environment. These environments and assumptions underpin the security strategy described in this document.

The products are intended for buildings and equipment in industrial facilities, where multiple devices, including Mitsubishi Electric products, are typically installed. Factories may also include server rooms with production management PCs and other servers.

Network-enabled products are assumed to connect to factory networks, such as Ethernet[3]. Communications with external networks, including the Internet, are assumed to pass through firewalls, routers, or other security devices.

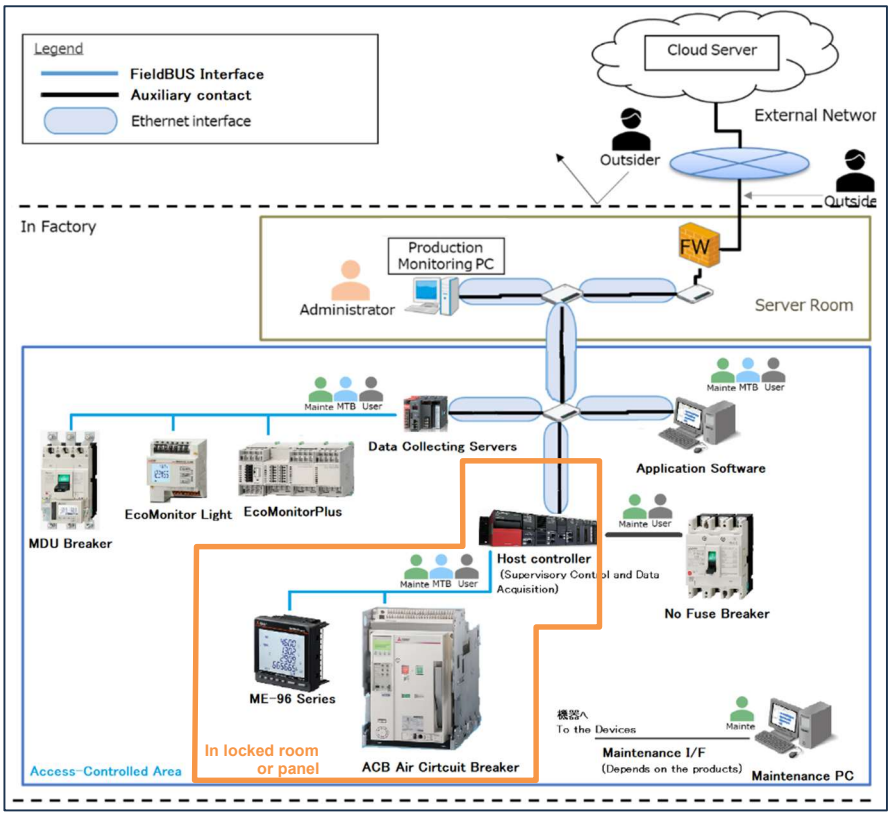


Figure 3. Expected Product Installation Environment

[3] Trade Marks:
・Ethernet is a registered trademark of FUJIFILM Business Innovation Corp.
・Some of our product names are also registered trademarks.
・Trademark symbols such as “TM” and “(R)" may not be explicitly indicated in this document.

Table 2. Assumptions for the Installation Environment

No.	Assumption	Description
1	Access Control	Entry and exit to the factory are restricted through access control measures.
2	Locked Equipment Enclosures	Operator panels and equipment enclosures containing the products are locked, preventing unauthorized operation or modification.
3	Removable Media Management	Storage media such as SD cards and USB memory devices are stored in locked locations and can be removed or used only with administrator authorization.
4	User Training	Users are sufficiently trained to properly configure, manage, and operate the products.
5	Appropriate Administrator Selection	Administrators are trusted individuals capable of carrying out management responsibilities appropriately.
6	Firewall Installation	Firewalls or network switches are installed between factory networks and external networks to block unnecessary external communications.
7	Security of Connected PCs	PCs communicating with the products, such as maintenance PCs or production monitoring PCs, are protected by antivirus software and other security controls.
8	Appropriate Password Management	Passwords are managed according to internationally recognized and validated password management guidelines[4].

The devices, applications, and networks shown in Figure 3 are described in Table 3.

Table 3. Devices, Applications, and Networks in the Environment

No.	Term	Description
1	Production Management PC	Device equipped with software used to monitor factory systems.
2	Maintenance PC	Device equipped with engineering tools used for product maintenance.
3	Cloud Server	Server used by customers to collect and manage operational information from products.
4	Field Communication / Auxiliary Contacts	Network used for communications and status notifications between products and field devices.
5	Firewall	Device providing packet filtering, communication control, bandwidth limitation, NAT, and NAPT functions.
6	Network Switch	Device used to separate networks through VLANs or virtual routing functions. A combination of routers and switches may also be used.
7	External Network	A network outside the factory's administrative control. The Internet is a typical example.
8	Wireless Network	A network using radio communications rather than cables. Wireless LAN is a typical example.

Physical protection measures, such as restricting access to designated factory areas or securing equipment storage locations with locks, are also important security controls.

[4] An example of password guidelines is NIST SP 800-63B, published by the National Institute of Standards and Technology (NIST).
NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management
https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final

From a security perspective, the operating environment is divided into the areas shown in Table 4.

Table 4. Area Classification and Operational Control

No.	Area	Description
1	Server Room	Room containing network management devices and other equipment critical to continuous operation of the control system. Protected against unauthorized access through measures such as restricted-entry lock management.
2	Power Receiving and Distribution Panels	Locations where power is received from the utility or distributed to downstream systems. Monitoring and protection devices are installed.
3	Control Panel	Contains control units, drive units, and related devices. Access is restricted through measures such as locked enclosures.
4	Restricted Access Area (Production Area)	Area that may be accessed only by personnel involved in operation and maintenance of machinery and control systems.
5	Factory	Area containing both restricted-access production areas and server rooms.

Table 5 shows the Users of the factory system.

Table 5. Definition of Users

No.	User	Details	Definition	Malicious or not	Remarks
1	End user (User)	Administrator (Administrator)	The administrator manages local servers, such as production PCs, and may access information security areas (i.e. Server Room) or authorized access areas. As an employee of the user or an affiliate, they must pass identity checks, receive training, and not intentionally pose a threat.	Not malicious	
2		Asset owner Operator Maintenance worker	They use the products for various activities and may enter authorized access areas to operate or maintain equipment. They are assumed to be employees of the factory owner, its affiliates, or companies contracted to perform related services. They undergo identity verification and training and are assumed not to intentionally pose a threat.	Not malicious	
3	Machine tool builder (MTB) Panel manufacturer, Equipment manufacturer etc.	Designer Maintenance worker	They install and maintain systems incorporating Mitsubishi Electric products and may enter authorized access areas with the factory manager's permission to maintain equipment. They are assumed to be employees of the relevant manufacturer or its affiliates. They undergo identity verification and training and are assumed not to intentionally pose a threat.	Not malicious	
4	Maintenance personnel contracted by Mitsubishi Electric (Mainte)	Maintenance worker	They maintain the products and may enter authorized access areas to maintain control equipment using a PC or display unit provided with the product. They are assumed to be employees of Mitsubishi Electric or its affiliates. They undergo identity verification and training and are assumed not to intentionally pose a threat.	Not malicious	
5	Third party (Outsider)	-	People not included above, including individuals who can physically access the factory or unspecified persons on the Internet. They may attempt unauthorized access to Internet-accessible services or local networks by exploiting vulnerabilities.	Malicious	

3.2 Threats to Power Distribution and Control Equipment

Based on risk assessments and publicly known attack scenarios, Mitsubishi Electric identifies the threats shown in Figure 4 and Table 6.

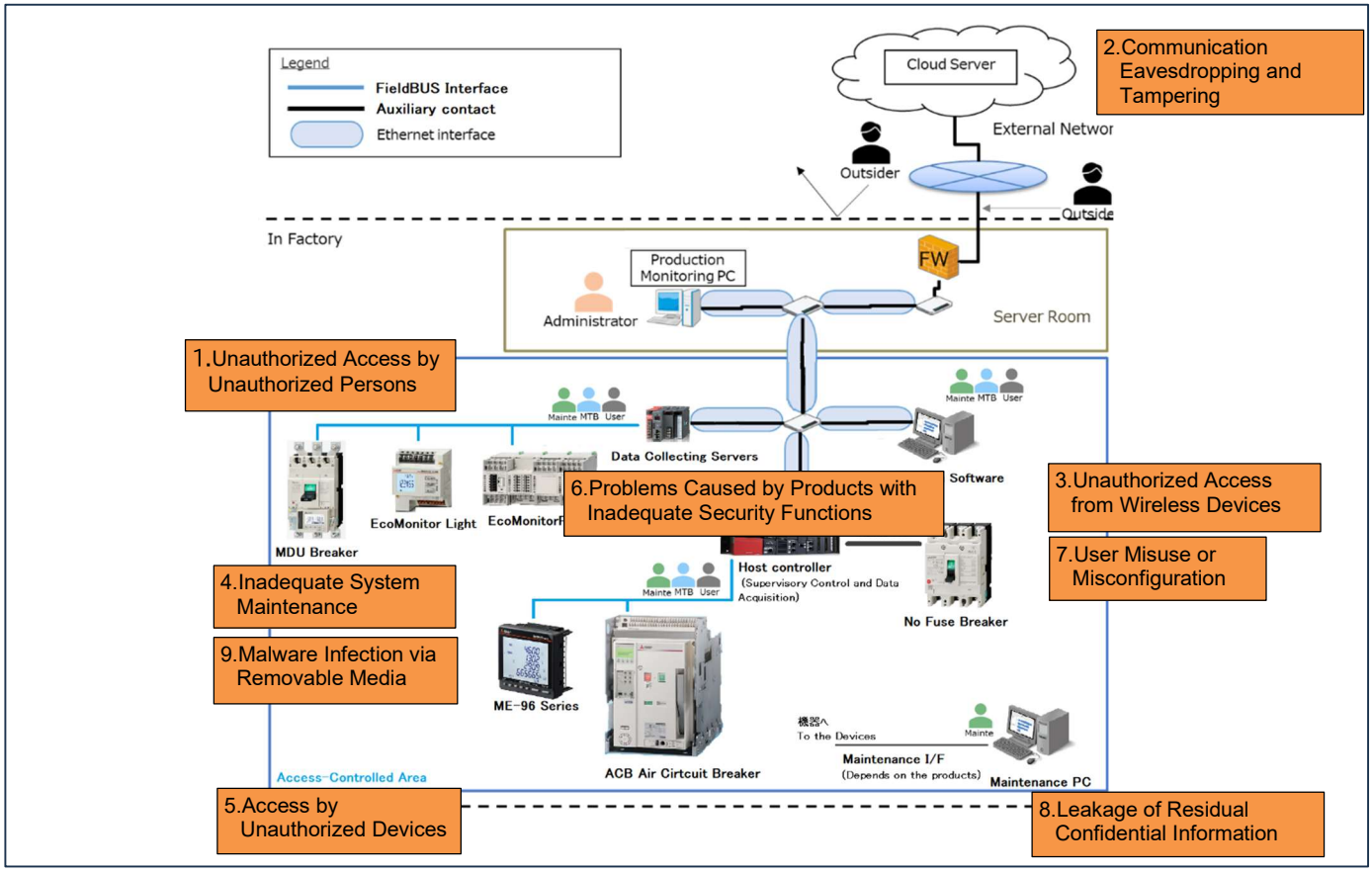


Figure 4. Threats to Products

Table 6. Threat Descriptions

No.	Threat	Description
1	Unauthorized Access by Unauthorized Persons	Attempts to access the product by persons not authorized by the administrator.
2	Communication Eavesdropping and Tampering	Communications between the product and external systems are intercepted or altered.
3	Unauthorized Access from Wireless Devices	Unauthorized access through external wireless devices.
4	Inadequate System Maintenance	The system is not properly maintained, vulnerabilities remain unaddressed, or the system operates in an environment where communication data may be accidentally altered.
5	Access by Unauthorized Devices	Unauthorized access attempts from unauthorized devices.
6	Problems Caused by Products with Inadequate Security Functions	Unauthorized access through products with inadequate security functions.
7	User Misuse or Misconfiguration	Unexpected behavior caused by user misuse or misconfiguration.
8	Leakage of Residual Confidential Information	Sensitive information remains on discarded or transferred products and is extracted by unauthorized parties.
9	Malware Infection via Removable Media	Malware introduced through SD cards or USB memory devices causes malfunction or disruption.

3.3 Security Countermeasure Policies

Table 7 presents the security countermeasure policies corresponding to the threats identified in Table 6. These policies include not only measures implemented by the products themselves but also measures that must be implemented by customers within their operational environments.

As described in Section 1.2, Defense-in-Depth requires security controls at the Human, Physical, and Network Layers in addition to the Device Layer. For this reason, product security measures alone are not sufficient; security must be addressed across the entire system.

Table 7. Security Countermeasure Policies

No.	Threat	Security Policy	Related Functions and Measures
1	Unauthorized Access by Unauthorized Persons	Appropriate access rights and user identification	★User authentication, ◆access restriction, ◆locked equipment, ◆administrator selection, ◆firewalls, ◆IDS/IPS, ◆PC security
2	Communication Eavesdropping and Tampering	Communication authentication and encryption	◆access restriction, ◆locked equipment, ◆firewalls, ◆IDS/IPS, ◆PC security
3	Unauthorized Access from Wireless Devices	Restriction of connected devices	◆Elimination of unauthorized devices
4	Inadequate System Maintenance	System maintenance and vulnerability remediation	◆Device selection, ◆periodic maintenance, ◆software/firmware updates
5	Access by Unauthorized Devices	Restriction of connected devices	◆Elimination of unauthorized devices, ◆access restriction, ◆locked equipment
6	Problems Caused by Products with Inadequate Security Functions		
7	User Misuse or Misconfiguration	File protection, data backup, system recovery	◆User education, ★operation history, ★backup and restore
8	Leakage of Residual Confidential Information	Secure deletion of confidential information before disposal	◆User data deletion function
9	Malware Infection via Removable Media	Restriction of connected devices	◆Elimination of unauthorized devices and operational controls

◆ Measures in the operating environment

★security functions of Mitsubishi Electric products

3.4 Overview of Security Functions

This section provides an overview of the security functions available in applicable products.

For detailed specifications and operating procedures, refer to the instruction manual for each product.

Table 8. Examples of Product Security Functions

Function		Implementation Example / Description
Authentication	User Authentication	Authentication required to use product functions. Some products provide dedicated authentication mechanisms for specific functions such as configuration changes, FTP access, or e-mail transmission.
	Other Authentication Functions	Some products provide authentication functions for connecting to external systems such as cloud services.
Logging	Operation Log	Records communication events, device operations, and related activities. Application software may utilize the operating system's event logging functions.
	Error Log	Records errors and faults. Application software may utilize the operating system's event logging functions.
Encryption	Communication Encryption	Some products provide encryption capabilities when accessing external web services.
	Internal Data Encryption	Some products encrypt data stored internally within the device.
Other	CPU Protection Function	Certain products prevent unauthorized software/firmware updates by third parties, allowing updates only through authorized maintenance procedures.

3.4.1 Authentication Screen

The Authentication Screen function restricts access to product functions and stored data.

Users attempting to access protected functions or data must be authenticated by entering a password.

By restricting access through password authentication, unauthorized operations resulting from misuse or incorrect configuration can be prevented.

For most applicable products, this function cannot be disabled, nor can operation without a configured password be enabled.

3.4.1.1 Password Entry and Release

By entering the correct password, users can modify, access, or export data protected by access controls.

3.4.1.2 Precautions

The following precautions should be observed when using the authentication function:

- A default password is configured. Change it to a strong password that is difficult to guess before use.
- Do not share passwords with individuals who do not require access for legitimate business purposes.

3.4.2 Operation History

The Operation History function records operating information and historical events for troubleshooting and analysis purposes.

History records are stored as data files in chronological order based on date and time.

These records may help identify the date, time, and circumstances surrounding failures, abnormalities, or security incidents.

Table 9. Examples of Historical Data

History Data	Description
Operation Log	Records normal equipment operations and events.
Communication Error Log	Records communication-related errors.
Access Log	Records authentication and communication access from external systems.
Audit Trail	Records configuration changes performed through communication interfaces.
OS Event Log	Logs stored by PCs running related software, including startup, shutdown, and authentication events.
Time-Stamped Measurement Data	Measurement values recorded together with timestamps.

3.4.2.1 Precautions

The following precautions should be observed when using the Operation History function:

- Data logs have maximum storage capacities. When the capacity limit is reached, older records may be overwritten or deleted.
- For products that support exporting log data, regularly save log files to a secure location.
- In addition to the logs listed in Table 9, some products may provide other diagnostic logs intended for operators or maintenance personnel.

3.5 Supplier Risk Management Activities

As described above, Mitsubishi Electric ensures product security by working with suppliers and partners to manage risks, including those related to externally sourced hardware and software. Examples of supplier risk management activities include:

(1) Production Management: Reducing security risks through supplier assessments, improving supplier security awareness, and preventing vulnerability introduction or product tampering through delivery inspections.

(2) Product Management: Maintaining traceability and centralized management of externally procured hardware and software, including vulnerability management.

(3) Preparing product updates and external communications for product vulnerabilities and delivering them at appropriate times based on customer requirements and operational considerations.

(4) Taking necessary actions in accordance with Mitsubishi Electric quality assurance procedures in the event of security incidents caused by vulnerabilities.

3.6 Security Support Policy

Mitsubishi Electric provides security support to help customers use products safely and securely.

This section describes the scope of support and the support period.

3.6.1 Scope of Support

If a product security vulnerability is discovered during the support period, or if a security incident attributable to product security occurs, Mitsubishi Electric will assess the associated risks and impacts and, as appropriate, take the following actions.

(1) Products Supporting Software/Firmware Updates:

Providing information and guidance to customers, as well as developing and delivering software updates to address identified vulnerabilities or issues.

(2) Products Not Supporting Software/Firmware Updates:

Providing information and guidance to customers and, when deemed necessary in accordance with Mitsubishi Electric quality assurance procedures, updating or replacing affected products through Mitsubishi Electric or its authorized service providers under Mitsubishi Electric's responsibility.

3.6.2 Support Period

The support period for Mitsubishi Electric products shall be the longest period determined by the following criteria:

(1) Reasonable Product Service Life:

The support period is determined based on factors such as parts availability, technological advancements, and changes in the product operating environment.

(2) A period that includes at least the minimum support duration required by applicable laws and regulations (e.g., five years under the European CRA).

4 Secure System Construction and Operation by Customers

The previous chapters described Mitsubishi Electric's product security initiatives. However, customers must also implement appropriate security measures to build and maintain secure systems. For general guidance on secure system design and operation, refer to Section 3 of the FA System Security Guideline (XFB3-20PS001). This chapter also outlines customer responsibilities and recommended practices for power distribution and control equipment based on the security concepts in Chapter 3.

4.1 Installation of Power Distribution and Control Equipment

To ensure secure operation of the products, Table 10 lists important considerations when using the security functions provided by the products.

An overview of these functions is provided in Section 3.4. For detailed information, refer to the instruction manual for the applicable product.

Table 10. Security Function Configuration Recommendations

No.	Function	Recommendation	Reference
1	Authentication Screen	A default password is configured. Change it to a strong password that is difficult to guess before use.	3.4.1
2	Operation History	Because older entries may be overwritten when storage capacity is exceeded, periodically export and back up operation history data.	エラー! 参照元が見つかりません。
3		Configure correct date and time settings to ensure timestamps are recorded accurately.	

4.2 Operation and Maintenance of Power Distribution and Control Equipment

4.2.1 Examples of Secure Operation

As a physical security measure, restrict access to factory areas as required and install products in secure, monitored locations, such as equipment enclosures or locked cabinets. Protect rooms containing network management equipment or devices critical to control-system operation with strict access controls, separate them from general factory areas, and limit entry to authorized personnel.

Products communicate over networks with maintenance and production management PCs, some of which can manage files stored in the products. To prevent file leakage and unauthorized files from being written to products through compromised PCs, implement the following measures on all connected PCs:

- Protect PCs against theft using measures such as cable locks.
- Implement access control for PC users.
- Ensure that only authorized individuals can log in.
- Strictly manage authentication credentials.
- Implement biometric authentication, such as fingerprint authentication.
- Install and maintain antivirus software.

Storage media such as SD memory cards and USB memory devices may expose customer assets if lost or stolen. In addition, malicious parties may intentionally connect storage devices containing unauthorized files, potentially affecting control of customer equipment.

Therefore, the following security measures are recommended:

- Store removable media in locked cabinets or other secure locations.

- Restrict who may use removable media.
  ★Establish rules governing removal and transport of storage media.
  ★Restrict which PCs may write data to the storage media.
- Physically restrict access to LAN interfaces, SD card interfaces, and USB interfaces through access control and locking mechanisms.

To protect factory networks and connected PCs from unnecessary external access, install firewalls, routers, or equivalent network security devices at:

- The boundary between the Internet and the factory network.
- Server rooms and other critical network segments.

As part of ongoing security operations, customers should establish plans for regularly reviewing and verifying the items listed in Table 11.

Table 11. Periodic Security Verification Items

No.	Area	Verification Item
1	Secure Communications	When communication with external systems is required, use security mechanisms such as VPN connections.
2	Network Environment	Properly manage network traffic to prevent communication overload within environments where Mitsubishi Electric products are connected.
3	Passwords	For products and peripheral devices with user authentication functions, periodically change the configured passwords and use strong passwords that are difficult to guess.
4	Data Minimization	Retain only the minimum data necessary within products and periodically review stored information. Remove unnecessary personal or confidential information.
5	Operation History Review	Regularly review logs collected through the operation history function to detect suspicious activities. Verify that product date and time settings remain correct. For checking and configuring the date and time, refer to the relevant section of the applicable instruction manual.
6	Unauthorized Access Monitoring	Most Mitsubishi Electric application products do not include dedicated access-monitoring functions. Review Windows access logs or equivalent logs to detect unauthorized access attempts.
7	Prevention of Unauthorized Access from Higher-Level Systems	Implement user authentication on systems that access Mitsubishi Electric products and provide notification during authentication. Notifications should clearly indicate that access information is logged, unauthorized access is prohibited and subject to penalties, and that authentication constitutes consent to monitoring and logging.
8	Backup	If backup and restore functionality is provided, regularly back up or otherwise record user programs, settings, and other necessary data.
9	Backup Data Management	Customers are responsible for managing backup data created by backup and restore functions.
10	Security Updates	Regularly review security advisories and other information published through Mitsubishi Electric websites and services and apply necessary countermeasures.
11	Product Data and Software/Firmware Updates	When applying externally downloaded data or software to products, customers are responsible for taking measures to prevent abnormalities in downloaded data and verifying that the data is valid.

Customers should designate appropriate personnel as administrators and ensure that all users receive sufficient education and training to properly configure, manage, and operate the products.

Products should always be operated in accordance with the applicable instruction manuals and this guideline.

4.2.2 Periodic Maintenance

To maintain a secure system, periodic maintenance should be performed on Mitsubishi Electric products and associated equipment.

Maintenance is recommended at least once per year.

For products equipped with the security functions listed in Table 12, maintenance activities should include verification that those security functions continue to operate correctly.

Records of maintenance activities should be retained and managed by the customer.

Table 12. Security Function Verification Items

No.	Function	Verification Item
1	Protected Configuration Screen (Login Screen, etc.)	Verify that a password is required when attempting to modify protected data such as machine parameter data.
2	Operation History (Operation Logs, etc.)	Verify that enabled operation history records are being stored correctly and that recorded timestamps are accurate.

4.3 Removal and Disposal of Power Distribution and Control Equipment

If products are not properly disposed of, transferred, or retired from service, residual data remaining within the products may be disclosed to unauthorized parties.

To prevent information leakage, observe the following recommendations when discontinuing use of a product.

- Determine whether asset data remains within the product and delete it if present.
- If the product provides a data deletion function, use the function to securely erase the data.
- Also process any residual data stored in connected upstream devices or peripheral equipment using their respective functions.

If the product provides a backup function and backup data must be retained before erasing the product, perform an appropriate backup prior to data deletion.

Backup data exported from the product to SD memory cards, USB memory devices, computers, or other media must also be properly managed during disposal or transfer.

Before disposing of or transferring equipment:

- Remove installed SD memory cards and USB memory devices.
- Manage or dispose of those media appropriately.
- Follow the general disposal precautions described in the maintenance manual under "Safety Precautions."

When removing equipment connected to the product within a system, note that protected assets may also remain on those devices. Such equipment should be processed appropriately, including deletion of stored data where necessary, before removal from service.

5 Security Contacts

To improve the information security quality of its products, Mitsubishi Electric collects information regarding product vulnerabilities from external security researchers and coordination organizations, including domestic and international CERTs.
If you become aware of a vulnerability affecting a Mitsubishi Electric product, please report it through an appropriate coordination organization or by using the contact forms listed below.

Mitsubishi Electric Product Vulnerability Reporting Contact

Japanese
https://www.mitsubishielectric.co.jp/psirt/contact/
English
https://www.mitsubishielectric.com/psirt/contact/

5.1 Disclosure of Vulnerability Information

When vulnerabilities affecting Mitsubishi Electric products are identified, information regarding the vulnerabilities and the required countermeasures is published on the websites listed below.
Customers are encouraged to periodically review these sites and take appropriate action for any affected products.

Vulnerability Information

Japanese
https://www.mitsubishielectric.co.jp/psirt/vulnerability/index.html
English
https://www.mitsubishielectric.com/psirt/vulnerability/index.html

FA Product Vulnerability Response Status

Japanese
https://www.mitsubishielectric.co.jp/fa/about-us/security/vulnerability/
English
https://www.mitsubishielectric.com/fa/about-us/security/vulnerability/

If a software/firmware update is required for a product, please contact the machine manufacturer or distributor from whom the product was purchased.
In some cases, updates may be available for download from Mitsubishi Electric websites. Refer to the applicable instruction manual for details.
If the sales channel of the product is unknown, please contact a Mitsubishi Electric branch office or authorized distributor.
For service center contact information, refer to the end of the applicable product instruction manual.

Appendix A Inquiries Regarding This Document

For questions or inquiries regarding this document:

- Customers in Japan should contact the nearest Mitsubishi Electric branch office through the FA website.
- Customers outside Japan should contact the Mitsubishi Electric office responsible for their region through the FA Global Website.

FA Website

https://www.mitsubishielectric.co.jp/fa/

FA Global Website

https://www.mitsubishielectric.com/fa/