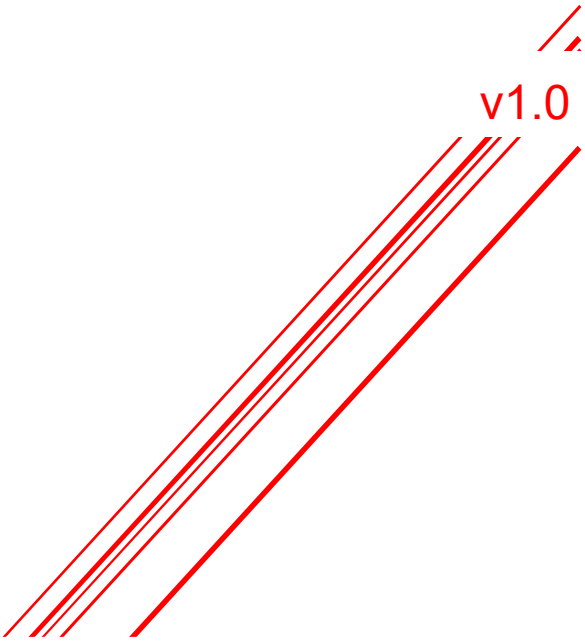
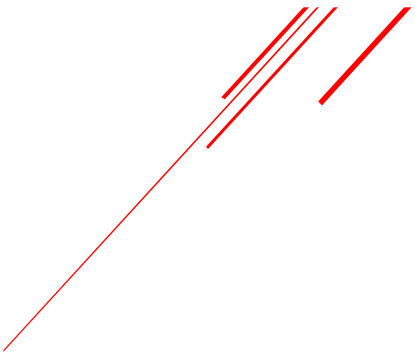
XFB3-20PS002

FA PRODUCT SECURITY GUIDELINE

v1.0



MITSUBISHI ELECTRIC CORPORATION
FACTORY AUTOMATION SYSTEMS GROUP
PRODUCT SECURITY INCIDENT RESPONSE TEAMS



Contents

Terms and Definitions

Term	Description
IT	Information Technology. A generic term for all technologies related to computers and networks.
IoT	Connecting various objects such as cars, home appliances, robots, and facilities to the Internet enabling them to exchange information, accelerating digital transformation of objects and automation to deliver added value.
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.
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 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.
Factory maintenance	Maintenance in a factory. It is performed to sustain the "Industrial health", "Safety", "Environmental load reduction", and "Operating rate improvement" of the factory.
Security accident	In operations of information and control system, the system is threatened by an event considered as a security problem. It is also called security incident.
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.
PDCA cycle	A continuous loop of "Plan", "Do", "Check", and "Action" steps.
Security key authentication	A function implemented in the PLC CPU to prevent unauthorized browsing and execution of programs. The project data locked with a security key can be viewed only with the engineering tool registered with the same security key. In addition, a program locked with a security key can be executed only with a module to which the same security key is registered.
File password	A function that prevents unauthorized reading/wiring of files using a password.
Remote password	A password that prevents unauthorized access to the PLC CPU from remote users.
Block password	A function that prevents unauthorized browsing of programs using a password.
Service setting function	A function that sets Enable/Disable for services on 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
[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, the use of IT in FA systems is growing to improve productivity in factories. FA systems have been generally assumed to be "not infected with malware and not subject to cyber-attacks because they are 'private' and 'closed'". However, the growing use of IT increases security risks in FA systems. In 2017, a major security incident was caused by malware called WannaCry[8] which initially targeted IT systems, and subsequently brought the factories of multiple companies to a halt. (Figure 1)

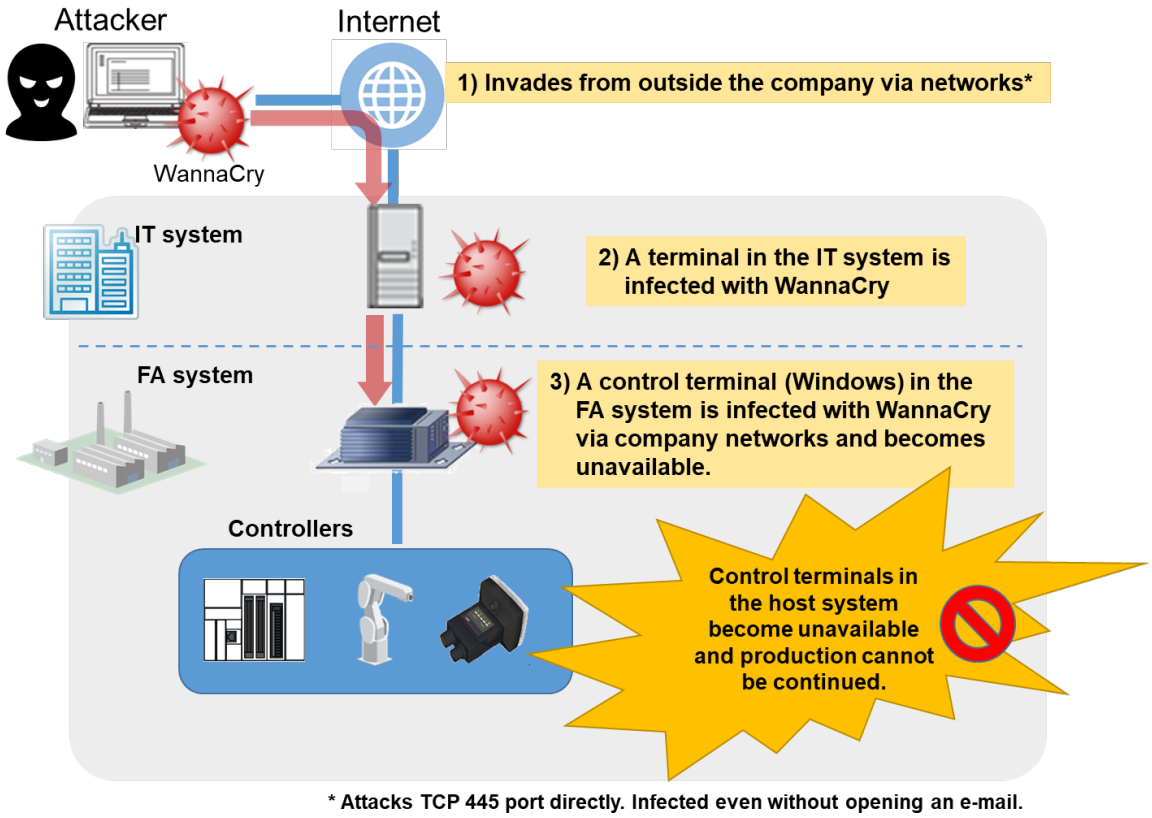


Figure 1 Examples of infection route of WannaCry into the FA system and security incident

To protect FA systems from such threats, it is important to hierarchically combine multiple security measures from physical security for factories such as access control to cyber security measures for networks and FA devices in factories. This improves security by "raising the difficulty and costs of mounting attacks " and "enhances the ability to detect and prevent attacks" thereby reducing the opportunity and influence of attacks. This concept for security measures is called "defense-in-depth", and is recommended in the international standard IEC 62443[9]. As a company manufacturing and selling FA products, Mitsubishi Electric (hereinafter referred to as "our company") has started developing FA products[10] incorporating the defense-in-depth strategy to provide customers with safe and secure FA systems.

[8] IT systems were already behind a firewall when they were infected. Therefore, firewalls alone are not enough to protect FA systems and FA systems should be “hardened” targets against potential attackers.
[9] For IEC 62443, refer to Appendix C.
[10] Programmable controller, industrial PC, FA sensor, Human-Machine Interfaces (HMIs)-GOT, servo, inverter, robot, NC, electrical discharge machine, laser processing machine, low-voltage power distribution products, power monitoring products, and related software/service

1.2. Purpose and use of this document

This document is intended to provide information about our security approach for our FA products (FA product security) and some recommendations on the use of FA products (Table 1).

Table 1 Contents and usage of this document

Chapter		Description	Usage
Chapter 2		Basic Security Policy for FA products	Read these sections to understand the security concepts and approach towards our FA products.
Chapter 3	3.1 to 3.4	Information focused on the security approach taken for our FA products	
	3.5	Security recommendations for customers using a system with the FA products	Read this section when constructing or operating a security-conscious FA system.

1.3. Disclaimer

Security-related information in this document is based on the results of our analysis and examination[11]. 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.

[11] The advice is subject to change without notice and that the reader should always ensure they have the most recent version of this document

2. Basic Security Policy for FA products

This chapter describes our basic security policy for FA products[12].

2.1. Scope of protection

Our company will strive to provide safe and secure products that conform to domestic and international security standards for control systems (such as IEC62443). In addition, our company will make continuous efforts that contribute to maintain and improve the following six elements[13] by cooperating with partner companies.

- Health: health of people working with the FA products
- Safety: safety of people working with the FA products
- Environment: environment around the FA products
- Availability: continuity of production and availability of data[14]
- Integrity: integrity of data
- Confidentiality: confidentiality of data

As a company providing FA products and services to promote factory automation, our company will enhance cyber security to create safe and secure environment for your customers. We will make continuous efforts for "Enhancement of FA Cyber Security" which refers to maintain Health, Safety, and Environment and to maintain and improve Availability, Integrity, and Confidentiality (Figure 2).

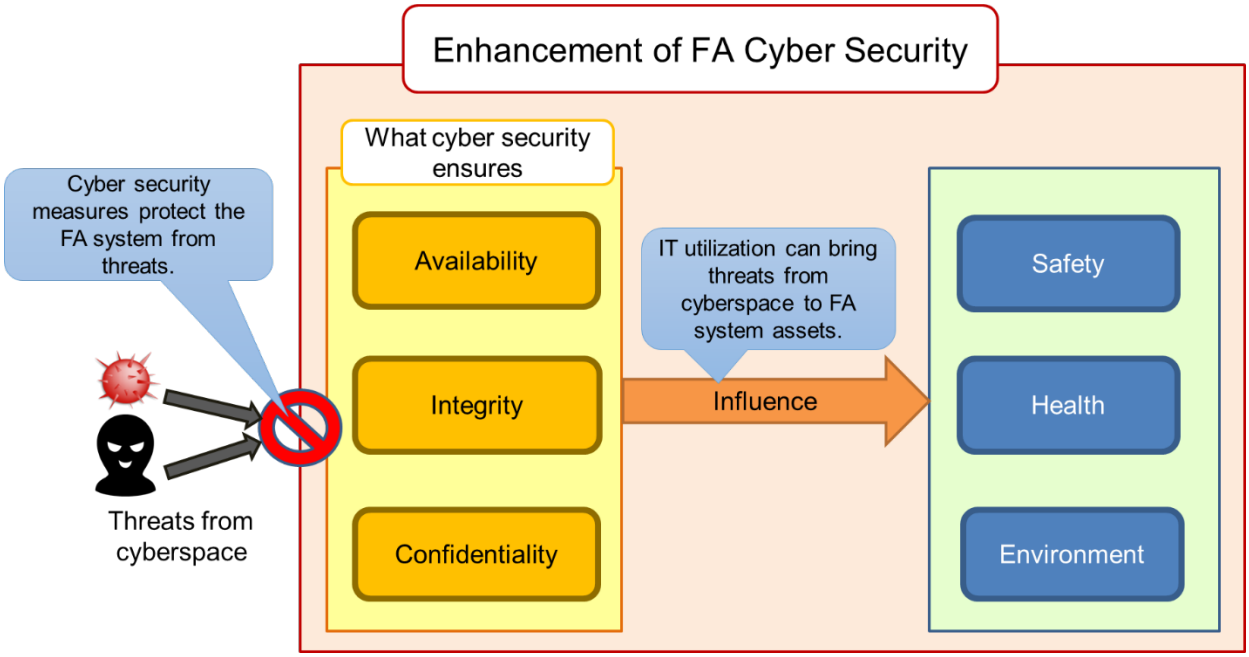


Figure 2 Conceptual diagram of "Enhancement of FA Cyber Security"

[12] For the latest information related to the security of our FA products, refer to the "Basic Policy on Product Security" on our website.
(https://www.mitsubishielectric.com/fa/business/psirt/index.html)

[13] The elements Health, Safety, Environment, and Availability are the goal of traditional FA systems. Availability, Integrity, and Confidentiality are assets in cyberspace. We integrated both ideas and defined the six elements as the target to be protected.

[14] Although it is different from the availability in terms of factory maintenance (continuity of production), it is included in this element based on the idea that the loss of data availability brings production to a halt.

2.2. Toward Realization of Enhancement of FA Cyber Security

From our point of view, to realize "Enhancement of FA Cyber Security" for safe and secure FA systems, it is necessary to not only implement cyber security measures to the FA products, but also to take a comprehensive that includes points (1) to (5) including the Asset Owner's FA system and supply chain (Figure 3).

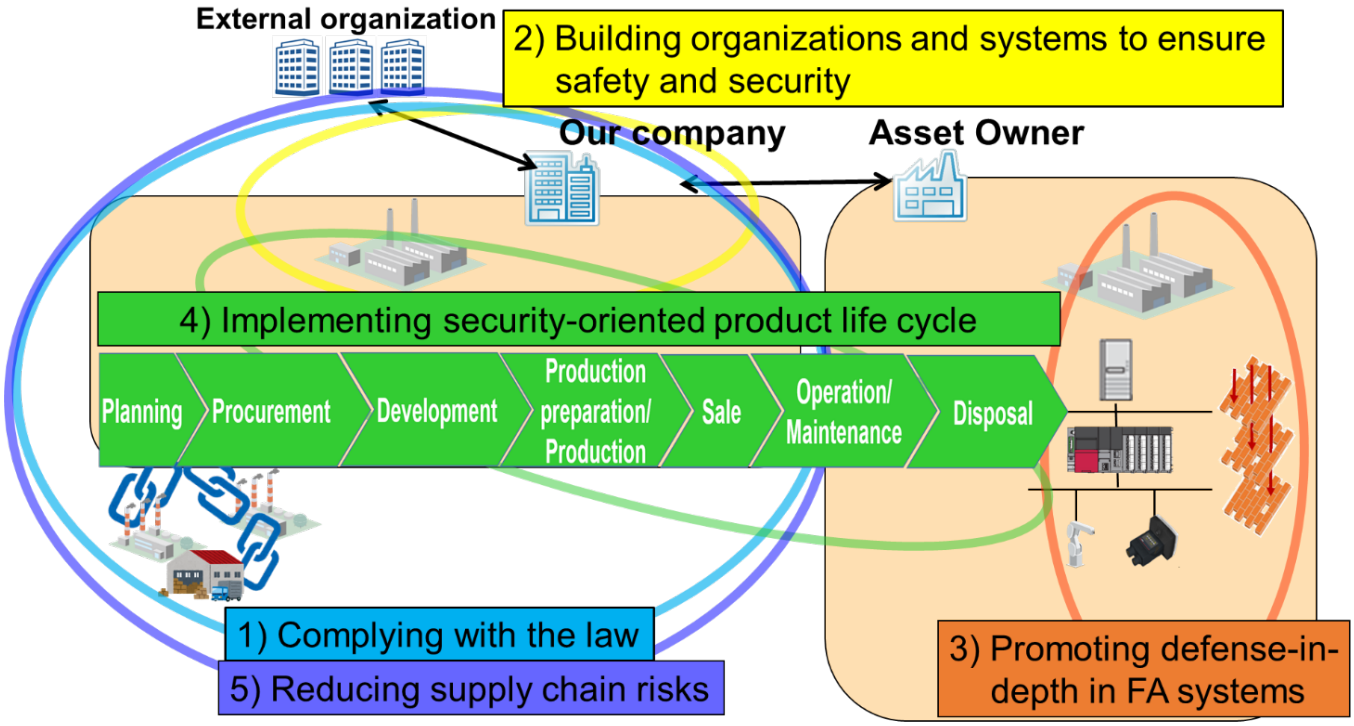


Figure 3 Approaches for "Enhancement of FA Cyber Security" related to our FA products

1) Complying with the law
   Our company complies with the law of each country and area related to FA product security. (For details, refer to 3.1.)
2) Building organizations and systems to ensure security and safety
   Our company has established a Product Security Incident Response Team (PSIRT)[15], which is responsible for activities pertaining to the security of our FA products, and to enhance and promote technical measures to prevent vulnerabilities in FA products. In case of any vulnerability problems, we will immediately investigate the cause and take corrective actions. (For details, refer to 3.2.)
3) Promoting defense-in-depth in FA systems
   From our point of view, it is necessary to take a "defense-in-depth" approach which is a combination of measures in various layers covering human, physical, network, and device layers to enhance the security of the Asset Owners' FA systems. Therefore, we work with our partner companies to enhance the security of FA products and assist with the introduction of security measures for FA systems built by Asset Owners. The provision of this guideline is a part those efforts. (For details, refer to 3.5.)

[15] Mitsubishi Electric has a corporate PSIRT serving as a coordination function at the head office, supported by main PSIRT in each group, and PSIRT in all factories working together to strive for secure quality products and services on a company-wide basis.

4) Implementing secure product development lifecycle
   Our company strives to continuously secure FA products in each phase of their lifecycle (planning, development, production preparation, procurement, production, sale, operation, maintenance, and disposal), making sustained efforts to protect our FA products from evolving attacks. (For details, refer to 3.4.)
5) Reducing supply chain risks[16]
   To enhance the security level of our FA products throughout the entire supply chain, related to our company, we strive to construct and maintain a mechanism to keep everyone, involved with the product development lifecycle, including the management layer informed and educated about the security of FA products. (For details, refer to 3.3.)

To reduce the possibility of security issues in our customers' FA systems and to quickly respond to and recover from security incidents, our company continuously makes the efforts described in 1) to 5).

[16] This document handles security-related risks such as unauthorized hardware modification and mixture of unauthorized programs in] a supply chain.

3. Approaches for Enhancement of FA Cyber Security

This chapter describes our approaches and recommended approaches for our customers for Enhancement of FA Cyber Security based on the basic security policy.

3.1. Complying with the law

Our company will endeavor to keep updated with the latest information on the laws of each country and area related to FA product security. Furthermore, we will conduct business activities properly complying with them and the regulations of our company. Regarding personal information protection, our company complies with the laws exemplified as follows:

- Act on the Protection of Personal Information in Japan
- General Data Protection Regulation (GDPR) (EU)

3.2. Building organizations and systems to ensure security and safety

As shown in Figure 4, PSIRT, which is responsible for security activities for our FA products, conducts the following activities in conjunction with the corporate PSIRT, Factory Automation Systems Group PSIRT, each factory PSIRT, sales department, and domestic/international distributors.

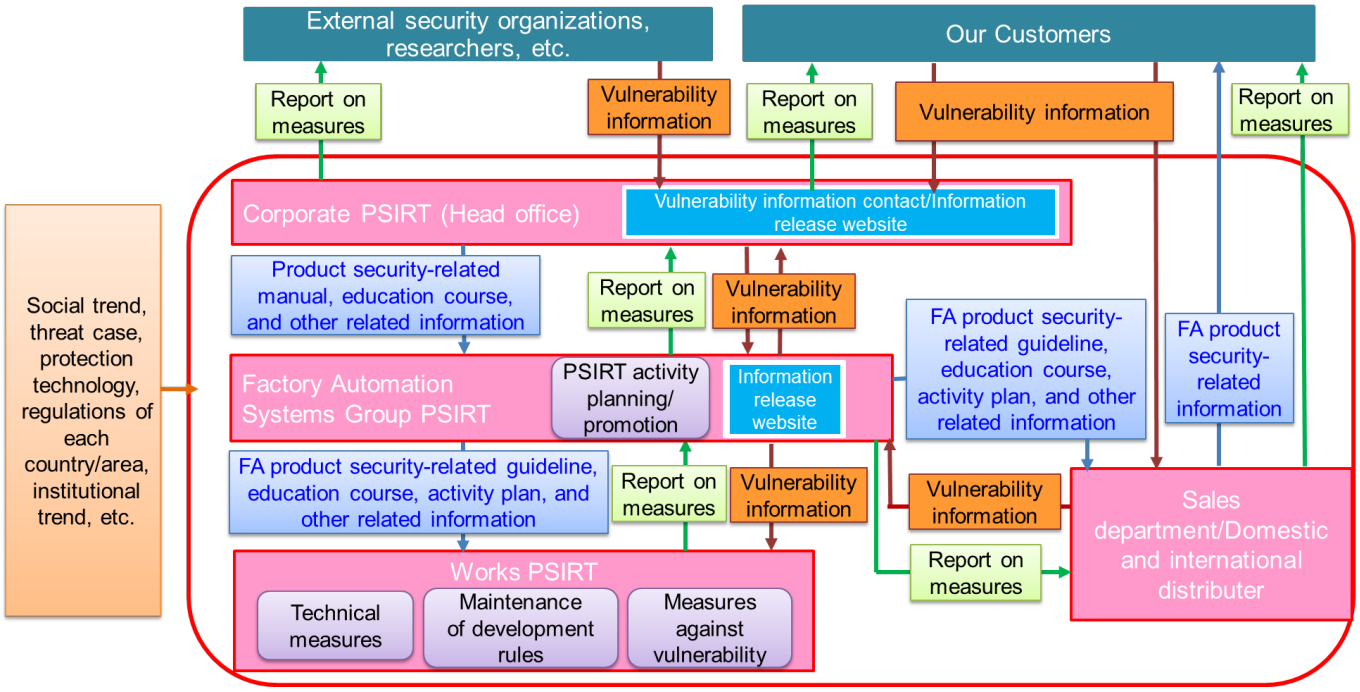


Figure 4 Organizations and systems for security on our products

(1) Enhancement and promotion of technical efforts to prevent vulnerabilities

A) Collecting and sharing information related to product security

Each of the corporate PSIRT, Factory Automation Systems Group PSIRT, and individual factory PSIRT collects and shares information related to the latest threat cases, protection technologies, regulations of each country/area, institutional trend, etc. The vulnerability information of our FA products, Open Source Software (OSS), or others reported to the corporate PSIRT is quickly distributed to the related departments in Factory Automation Systems Group via the Factory Automation Systems Group PSIRT and each factory PSIRT.

B) Well-planned activities based on the latest information

The corporate PSIRT develops a company-wide basis plan for product security activities based on the collected information. Receiving the company-wide basis plan, Factory Automation Systems Group makes and promotes plans for preparing activities including technology measures, documents and regulations for realizing the security of FA products.

C) Preparing technology measures, documents and regulations etc.

The corporate PSIRT prepares education courses and guidelines related to product security that cover all Mitsubishi Electric products not only the products of the Factory Automation Systems Group. The Factory Automation Systems Group distributes the company-wide basis measures and promotes preparing guidelines and education courses dedicated to security of FA products. Receiving the plan made by Factory Automation Systems Group, the factory PSIRT introduces concrete technological measures and prepares related rules to establish secure development processes.

(2) Quick response and information provision related to vulnerability

The corporate PSIRT has a dedicated point of contact for receiving vulnerability reports related to all of our company's products from external security organizations[17], researchers, and customers. The corporate PSIRT centralizes and manages measures including information related to vulnerabilities so that when customers inquire to the sales department or domestic/international distributors[18] we are able to respond consistently about any vulnerability.

The Factory Automation Systems Group PSIRT and each factory PSIRT determine the cause, analyze the influence, and take measures based on the vulnerability information shared with the corporate PSIRT, sales department, and domestic/international distributers as the response to the vulnerability. The results of the measures are fed back as security measures for the products, and the information is quickly and appropriately provided to the external security organizations and customers via the corporate PSIRT, sales department, and domestic/international distributers.

(3) Communication related to security improvements of FA products to customers

The Factory Automation Systems Group PSIRT will publish dedicated web pages about the security of FA products and services on our company's official website. Through these activities, we strive to quickly and appropriately communicate with customers about security improvements for FA products so that customers can use our products and services with confidence.

[17] Domestic and international public institutions (such as IPA and JPCERT/CC), pure-play security companies, etc.

[18] For contacts, refer to Appendix D.

3.3. Reducing supply chain risks

The efforts to reduce supply chain risks related to our FA products can be separated into two groups: risk management by our company as an OEM (Original Equipment Manufacturer) of Asset Owners, and risk management by OEM partners as suppliers to our company (hereinafter referred to as "Supplier risk management") (Figure 5). Through our risk management and Supplier risk management, we strive to reduce security risks to the FA products and supply chain risks to customers who procure the FA products.

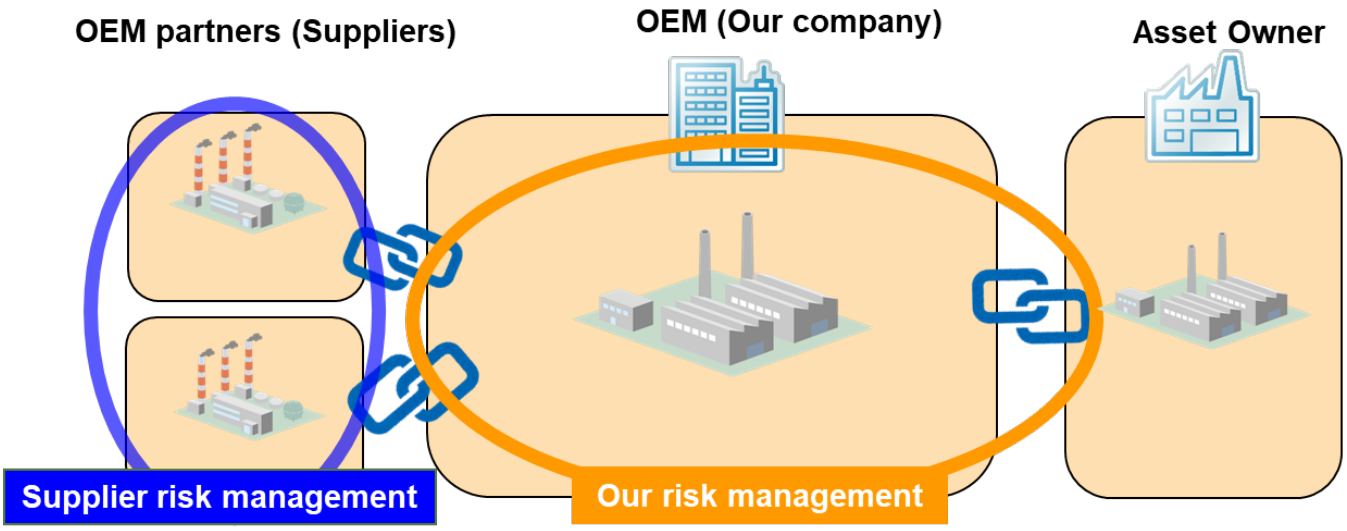


Figure 5 Scope of our approaches to reduce supply chain risks

3.3.1. Our risk management approaches

Our company implements six approaches to risk management (compliance, asset management, procured item management, production management, product management, and sales management) to reduce supply chain and security risks related to our FA products. The following shows examples of our approaches to risk management.

(1) Compliance: compliance with domestic and international laws and guidelines related to our company and customers, etc.

(2) Asset management: reduction in information leakage risk by managing product-related assets and information (such as product design drawings)[19]

(3) Procured item management: reduction in vulnerability risk by inspecting procured items and any associated tampering risk by managing stored items

(4) Production management: reduction in fraud and vulnerability risks by managing and educating operators and monitoring production sites and inspecting products respectively

(5) Product management: traceability management of shipped products and vulnerability management of our products

(6) Sales management: security enhancement at domestic/international distributors and carrier risk management

[19] Product design drawings and other product-related information must be protected because they can be exploited by attackers to find vulnerabilities in the product.

3.3.2. Supplier risk management approach

Our company implements two approaches to supplier risk management, production management and product management. These approaches reduce risks related to externally procured hardware and software to be incorporated into FA products. The following shows examples of OEM partners' approaches to risk management.

(1) Production management: security risk reduction using a check list review of said partner' measures, improvement of OEM partners' security awareness, and reduction in vulnerability and tampering risks by delivery checks

(2) Product management: traceability management of delivered products and vulnerability management of externally procured hardware and software

3.4. Implementing secure product development lifecycle

Our development is based on international standards (such as IEC 62443) to ensure reliability of our FA products. This section describes the measures incorporated in the product development lifecycle of our FA products. To protect the FA products, it is important to reduce the possibility of threats by taking required security measures in each phase of the lifecycle of the FA products (planning, development, production preparation, procurement, production, sale, operation, maintenance, and disposal) as defined in IEC 62443-4. As shown in Figure 6, our company divides our approach to product development into "actions related to the lifecycle of the FA products", which are conducted by our company, and "actions for Asset Owners using our FA products" which are recommendations to customers.

Figure 6 Product development lifecycle

3.4.1. Our approach: security measures for the lifecycle of FA products

Out company incorporates the following measures into the lifecycle of FA products (planning through sale refer to Figure 6).

(1) Planning

In the planning phase, security requirements shall be defined, with attention to the performance and functionality expected in the product, through clearly specified security functionality and performance metrics.

(2) Procurement

For procurement of the components (hardware and software) required for product development and manufacturing, specifications according to the product requirements shall be offered to the supplier. An agreement which can guarantee the compliance with the requirements shall be concluded as necessary. In addition, procured products shall be confirmed to meet the requirements including security requirements at the delivery process.

(3) Development

Each process in the development lifecycle of the FA products shall be built in a thought-out manner considering the security requirements to prevent vulnerabilities. For the development lifecycle of the FA products, refer to Appendix A.

(4) Production preparation/Production

In the preparation phase before manufacturing, introduction of measures in each layer described in 3.5.1 into the production site shall be considered for manufacturing compliant with the security requirements. At this time, the contents of the maintenance agreement and the operation/maintenance method of the externally procured production equipment[20] shall be checked they comply with the security requirements, and additional measures shall be taken as necessary.

In the manufacturing processes, measures to prevent unauthorized hardware and software from being incorporated shall be taken, such as prevention of entry of unauthorized persons to the production area by use of entry and exit control for operators, prevention of fraud by identification of the operator in charge, and prevention of mistakes by following the instructions thoroughly.

(5) Sale

As the supplier of the FA products, our company strives to reduce customers' security risks as shown in 3.3.1. When selling products, our company distributes documents including security specifications of the products to customers. If any vulnerability is discovered, our company provides information related to the vulnerability and measures and easing measures against it to customers as soon as possible.

3.4.2. Recommendations for Asset Owners using FA products: secure operation, maintenance, and disposal of the FA products

Our company manages security information related to operation, maintenance, and disposal of the FA products and firmware updates to help customers with the operation, maintenance and disposal. In addition to the security recommendations related to operation, maintenance, and disposal of the FA products provided in this guideline, our company provides information on individual products in manuals and other documents as necessary.

Furthermore, our company recommend the following measures to customers who have introduced our FA products for operation, maintenance, and disposal of the FA products.

To enhance the security of an entire factory, it is necessary to understand risks by implementing security risk assessments and thereafter take measures based on defense-in-depth. For the security enhancement of the entire factory based on the security risk assessment and defense-in-depth, refer to 3.5.

[20] Security updates of OS and related installation methods, local maintenance by the equipment manufacturer (including availability of external media such as USB memory or personal computers used for maintenance, availability of special remote maintenance monitoring service such as VPN, etc.), and countermeasures to be taken when equipment data is taken out by an internal engineer, etc.

(1) Operation and maintenance

Our FA products have functions that can be utilized as security measures during operation that are in addition to dedicated security functions. It is recommended to use these functions to investigate the cause in the case of a problem or when recovering the system from an error. For example, by collecting and saving the errors and abnormalities that occurred in our FA products or networks with the event history (error history) function. This can be used to investigate the cause in the case of a problem.

For customers using FA products, it is recommended to periodically check the latest firmware version and to perform firmware updates with the firmware update function. The use of the latest firmware can eliminate vulnerabilities and enhance security functionality, resulting in reduction of security risks. However, firmware updates may change the behavior of our FA products. Therefore, it is recommended to check the operational impact on the FA products and the safety of the FA system before restarting the FA system after a firmware update.

For customers using software related to the FA products such as engineering tools, it is recommended to periodically check the latest software version and to perform software updates after checking the integrity of the system.

If you have a FA product without the firmware update function or if you have any questions, please consult our company. For contacting our company, refer to Appendix D.

(2) Disposal

For customers using FA products, it is recommended to take appropriate measures such as breaking down the FA product so that data cannot be removed from the product before disposal. If it is disposed without taking appropriate measures, programs, recipe information, and others stored in it may be exploited by a third party.

3.5. Promoting defense-in-depth for FA systems

To further enhance security, our company recommends you to incorporate defense-in-depth into FA systems. To realize defense-in-depth, it is necessary to understand any risks by implementing security risk assessment[21] for the FA system and then take applicable measures based on defense-in-depth. By repeating security risk assessments for the FA system and applying countermeasures based on defense-in-depth in PDCA cycles as a part of security measures for the FA system, security can be continuously enhanced.

3.5.1. What is defense-in-depth?

The defense-in-depth security measure is a concept of taking measures from each point of view such as "human operation", "use of device/equipment", "network access", "data access", and "execution of application". Our company divides these points of view into the defense-in-depth approach related to the environment (outside the product) related to inside the product, defined as "human layer", "physical layer", "network layer", and "device layer" (Figure 7). The defense-in-depth approach increases the costs to attackers and enhances the ability to detect and prevent attacks thus reducing the influence of attacks.

The security functionality of the FA products is one of the defense-in-depth measures. To protect the FA system from cyber-attacks, our company recommends to install a firewall for the purpose of protection from cyber-attacks, install antivirus software into the personal computer, and consider installing the entry and exit control in the factory.

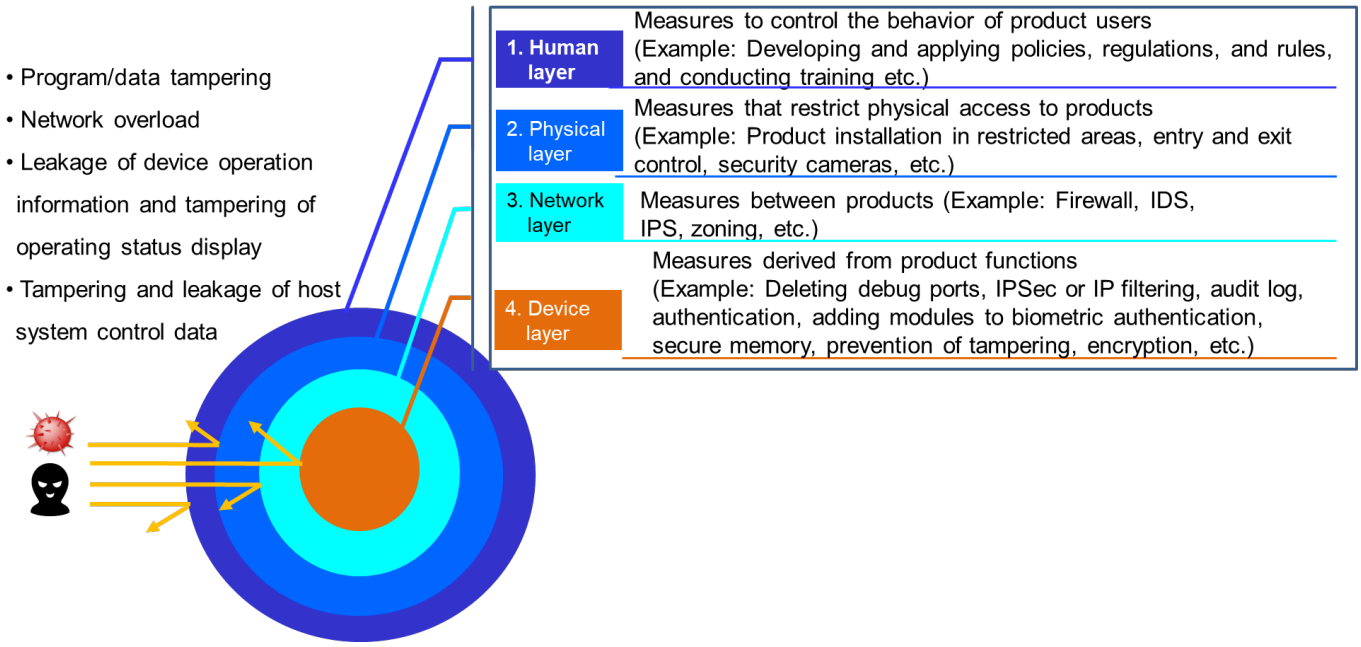


Figure 7 Defense-in-depth security measures

[21] For security risk assessment, refer to Appendix B.

3.5.2. Examples of a defense-in-depth approach

To realize the defense-in-depth concept, take security measures at each appropriate layer "human layer", "physical layer", "network layer", and "device layer". Table 2 and Figure 8 show the threats derived from the security risk assessment for the FA system and examples of security measures based on defense-in-depth.

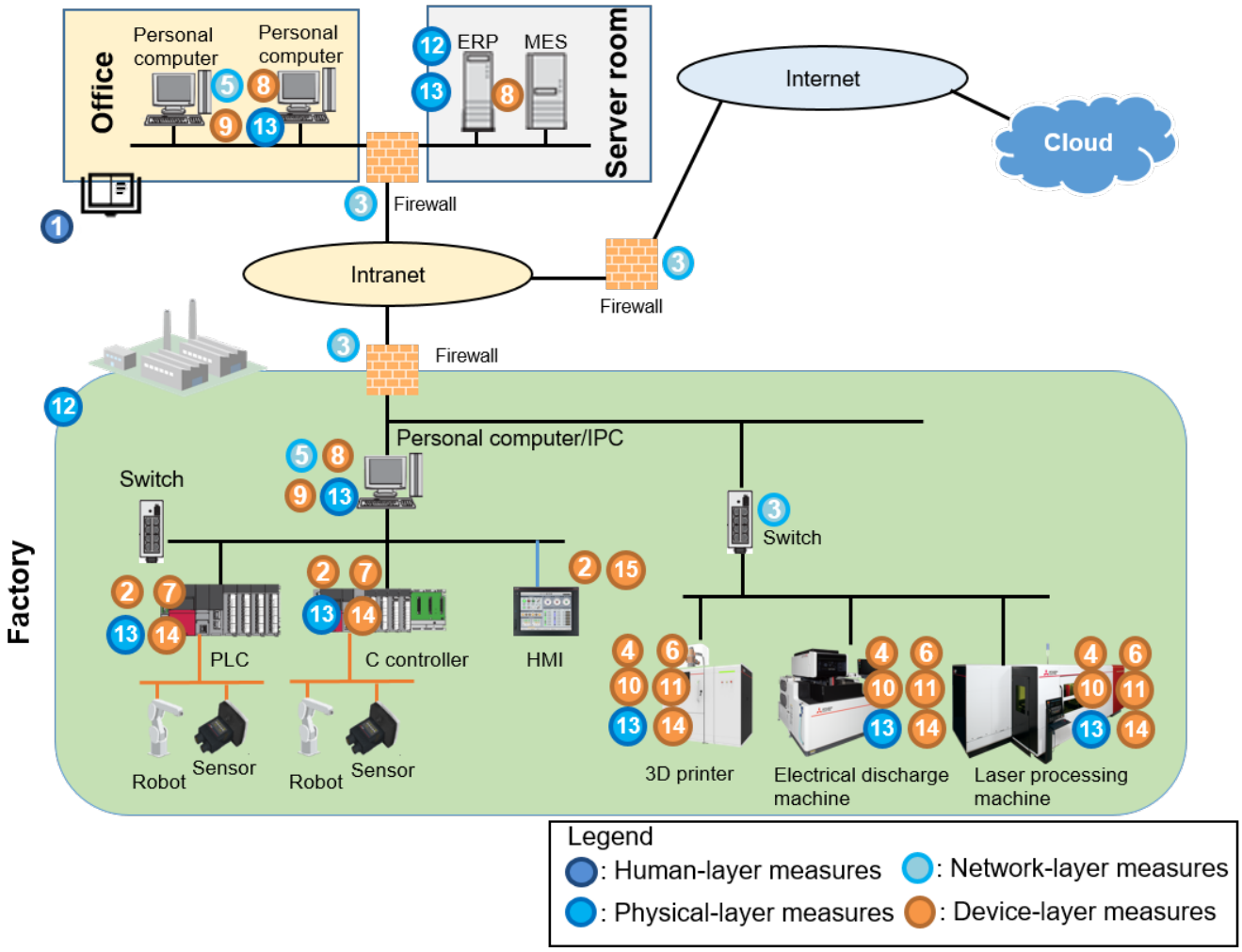


Figure 8 Threats in FA system and examples of measures

Table 2 List of threats and measure examples

Threat		Layer of defense-in-depth		Measure against threat
Common to all threats	customer's environment	Human layer	1	Prevents incorrect usage or failure to implement security measures by educating managers and users.
Overload on the network (DoS attack)	FA product	Device layer	2	Interrupts communication from unauthorized IP addresses by setting the IP filter function.
	customer's environment	Network layer	3	Restricts malicious traffic by separating the factory network and intranet, and the intranet and Internet using a firewall.
Leakage of production data due to communication interception through the intranet	FA product	Device layer	4	Prevents data leakage or tampering by mutual authentication using certificates.
	customer's environment	Network layer	5	Prevents production data leakage by protecting communication between hubs by using VPN technology.

Data leakage and tampering through the Internet	FA product	Device layer	2	Restricts the network access with an IP filter function on the FA product side.
			6	Prevents permanent connection or unauthorized access from the Internet by limiting the VPN connection from the outside to the FA product by user permission.
			7	Limits the access to programs and data in the FA product by the password authentication.
	customer's environment	Network layer	3	Limits the network access by installing a firewall at the entrance of the factory network.
		Device layer	8	Prevents program tampering by installing antivirus software or restricting login by user authentication on the personal computer for the development environment.
			9	Prevents program tampering by encrypting the programs and data on the personal computer for the development environment.
Leakage of production know-how from the FA product	FA product	Device layer	10	Prevents leakage of data due to unnecessary external communication by permitting only communication options based on license authentication.
			7	Prevents unauthorized reading and program execution with unauthorized devices from the FA product by data protection for the programs.
Fraud due to tampering of programs or data of the FA product	FA product	Device layer	2	Limits the network access by introducing an IP filter function or with a remote password function in the FA product.
			11	Prevents tampering of the FA products program or data by restricting applications that can be installed by checking the application white list of the FA product.
			7	Limits the access to programs and data in the FA product by the password authentication.
	customer's environment	Physical layer	12	Prevents programs and data from being tampered with by intruders entering the factory by access control into the factory.
			13	Prevents programs and data from being tampered with by intruders entering the factory by physically sealing free Ethernet and USB ports on the FA products or personal computer in the development environment.
		Network layer	3	Limits the network access by installing a firewall at the entrance of the factory network.
		Device layer	8	Prevents program tampering by installing antivirus software or restricting login by the user authentication in the personal computer for the development environment.
			9	Prevents program tampering by encrypting the programs and data in the personal computer for the development environment.
Fraud by attacks to unused services of the FA product	FA product	Device layer	2	Limits the network access by introducing the IP filter function or with the remote password function of the FA product.
			14	Prevents the access from unused services to the FA products by disabling unused services with the service setting function.
	customer's environment	Network layer	3	Limits the network access by installing a firewall to the entrance of the factory network.

		Device layer	8	Prevents program tampering by installing antivirus software or restricting login by user authentication on the personal computer for the development environment.
			9	Prevents program tampering by encrypting the programs and data on the personal computer for the development environment.
Leakage of device operation information or tampering of the operating status display	FA product	Device layer	2	Limits the network access with an IP filter function on the FA product side.
			15	Prevents interception or tampering of the operation informational by using user authentication while operating the FA product.
	customer's environment	Physical layer	13	Prevents information theft by intruders to the factory by physically sealing free Ethernet and USB ports on the FA product.
		Network layer	3	Limits the network access by installing a firewall at the entrance of the factory network.
Data leakage and tampering by software illegally installed to the server or personal computer	customer's environment	Device layer	8	Prevents data leakage and tampering by implementing software installation restrictions by using an application white list on the server, personal computer, and IPC.
			9	Prevents data leakage and tampering by encrypting data and protecting databases on the server, personal computer, and IPC.
Tampering and leakage of host system control data	customer's environment	Physical layer	13	Implements measures against intruders entering the server room by physically sealing free Ethernet and USB ports on the server and by access control for the server room.
		Network layer	3	Limits the network access to the server by installing a firewall for separating the Internet and intranet.
		Device layer	8	Limits the access to the server or data by installing antivirus software on the MES/ERP server or by user authentication.

To realize the defense-in-depth concept, it is necessary to construct an FA system in which our partner's devices and others are combined with the functions of our products. Therefore when thinking about cyber security it is important to consider the system as a whole and not only as a series of individual parts

Revision History

Date	Document number	Notes
Sep, 2020	XFB3-20PS001	First edition
Apr, 2021	XFB3-20PS001-A	Appendix D

Appendix A: Development lifecycle of FA products

As shown in Figure 9, our company implements security measures throughout the whole development lifecycle.

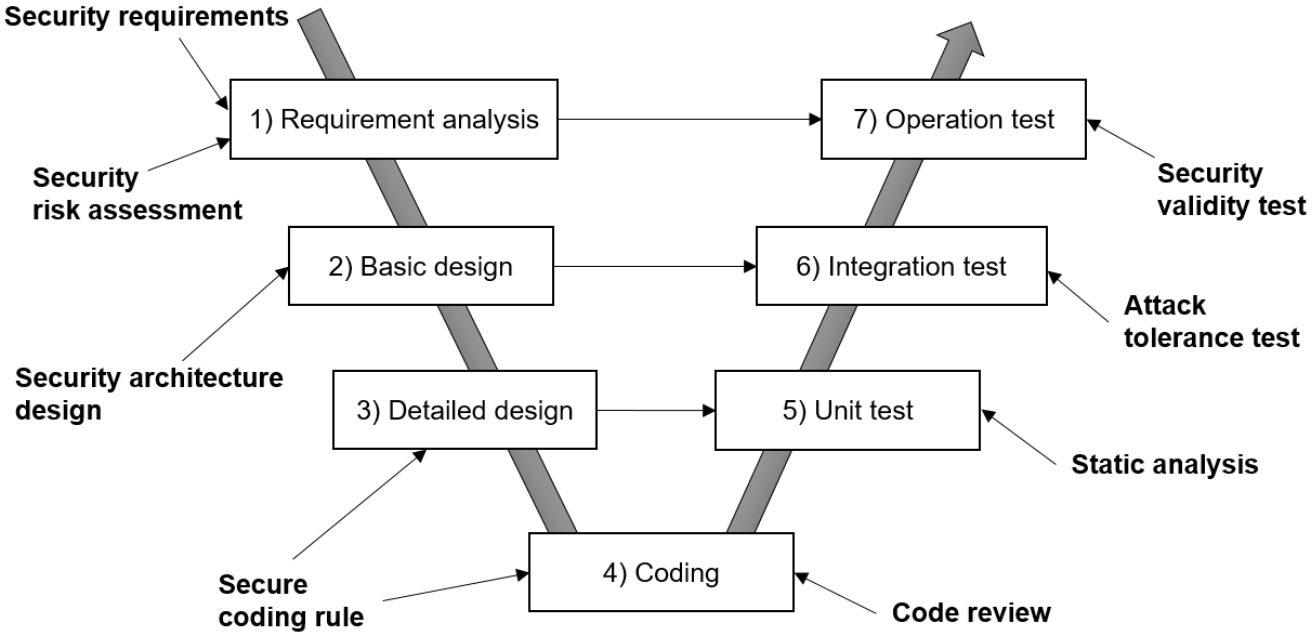


Figure 9 Security measures in the development lifecycle

The following describes the measures in each step of the development lifecycle.

1) Requirement analysis

   Before product development, product requirements are defined to clarify the functionality to be incorporated. Requirement definition involves product security risk assessment the results of which are reflected in the security requirements. In addition, whether these requirements are achieved by software or hardware is clarified. Security requirements not only apply to the requirement definition of products developed by our company, but also the selection of externally procured products (software and hardware). In this process, security requirements are documented following a ruled procedure. The documented security requirements are reviewed by related parties to confirm their validity.

2) Basic design

   This process involves software architecture design and functional design. In this process, protective design and usage considerations against malicious access via external interfaces are documented as a security architecture design. The review in this process aims to confirm that the security architecture is properly designed.

3) Detailed design

   This process involves software module design. Module division and definition, definition of variables, and other design activities are conducted according to coding rules including secure coding standards. Secure coding standards define the rules for developers to prevent vulnerabilities. The review in this process aims to check if the design follows the coding rules.

4) Coding

This process involves software creation (coding) according to the detailed design. Coding is performed according to the coding rules including secure coding standards. The review in this process aims to confirm that coding is properly performed.

5) Unit test

This process tests whether the software is coded according to the detailed design. Static analysis with a tool confirms that security functions are properly implemented according to secure coding standards.

6) Integration test

This process tests whether the software conforms to the basic design. The attack tolerance test[22] checks if the security measures selected in the security risk assessment are properly implemented.

7) Operation test

This process checks whether the software and hardware satisfy the security requirements by actual operations. Security validity test checks if the security requirements are satisfied.

[22] The attack tolerance test includes fuzzing and abuse case testing.

Fuzzing: A test that involves mechanically creating a large amount of data with invalid values as inputs to the device to check for malfunction or operational stop

Abuse case testing: A test that involves operation intended to cause harmful results to related parties such as a system and its users

Appendix B: Security risk assessment

For taking security measures, it is important to select effective measures to reduce risks. Effective measures can be selected by implementing a "security risk assessment" that Identifies threats to the system to be protected and measures against these threats.

Figure 10 shows the procedure of a security risk assessment[23, 24].

1) Check and organize the device and system status

   Check the system status such as the system configuration, roles and settings of devices, and communication flow as information required for the security risk assessment, and organize it in figures and tables. Figure 11 shows an example of organized system configuration, Table 3 lists examples of organized roles and settings of devices, and Table 4 shows an example of organized communication flow.

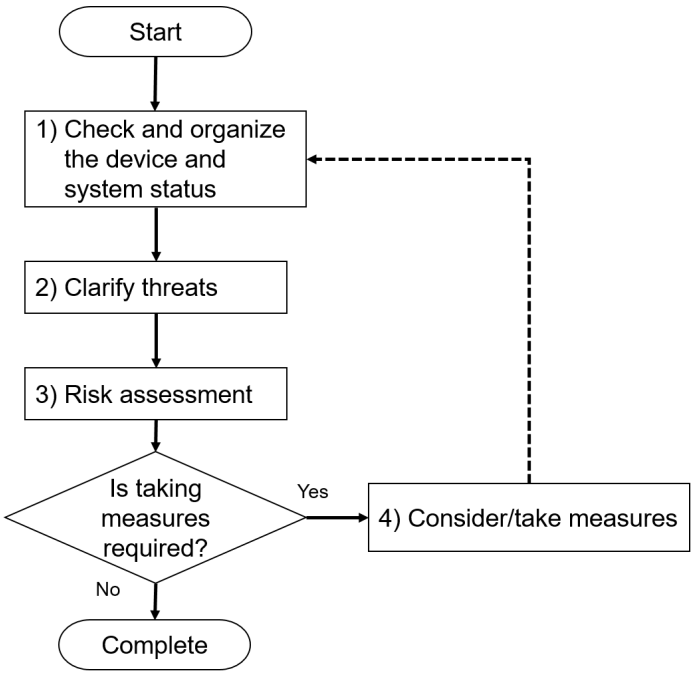


Figure 10 Procedure of security risk assessment

[23] This example describes the security risk assessment for the FA system. The test conductor and method are different from the "security risk assessment of the product" described in Appendix A.

[24] For the detailed procedures, refer to "Quick Guide to "Risk Assessment Guide for Industrial Control Systems", 2nd Edition" (https://www.ipa.go.jp/files/000078098.pdf) published by IPA.

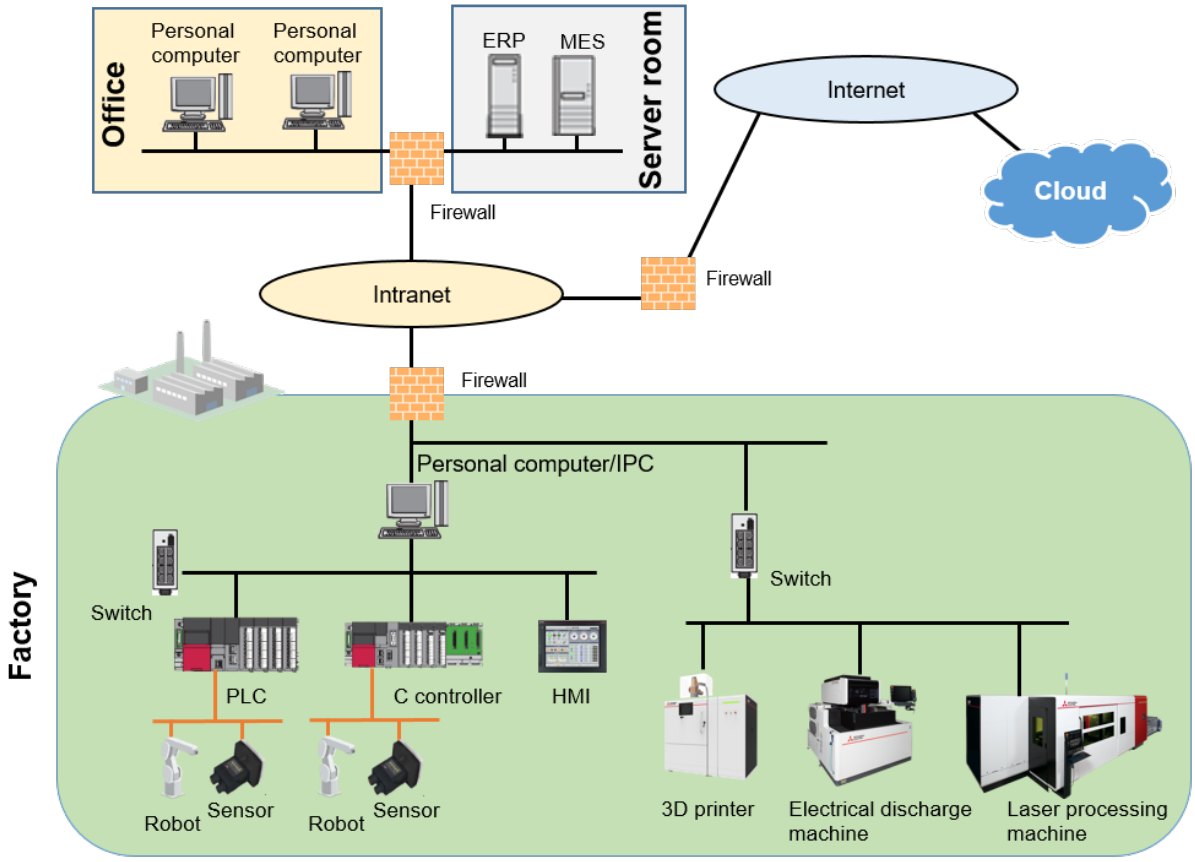


Figure 11 System configuration (example)

Table 3 Organizing roles and settings of devices (example)

Name	Role	Setting	Remarks
Personal computer/IPC	Writes programs and settings in the programmable controller and C controller.	・The latest versions of the OS and software are used. ・User authentication restricts operators. ・An engineering tool is installed and security functions are properly set.	Usage other than writing programs and settings such as browsing the web or using e-mails is prohibited.
Programmable controller	Controls robots and sensors.	・The latest version of the firmware is used.	-
HMI	Allows on-site workers to check the device operating information and to change the device settings.	・The latest version of the firmware is used. ・The wireless network (Wi-Fi) for connecting to the factory network is available.	-
Firewall	Blocks external communications.	・Communications outside the Intranet are blocked. ・Communications among the server room, office, and factory are allowed.	It is desirable to allow only the communications permitted by the administrator.
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

Table 4 Organizing communication flow (example)

Source	Destination	Content of communication
Personal computer/IPC	Programmable controller	Program and setting information
HMI	Programmable controller	Setting change by on-site workers
Programmable controller	HMI	Device information to be displayed on the display device
Personal computer/IPC	Internet	Acquisition of update software and others
• • •	• • •	• • •

2) Threat Modeling

Identify the potential threats. Based on the information organized in 1), list the threat by simulating how the device functions and installation environment can be attacked or considering the scenarios of attacks that bring threats[25]. In addition, assess the threats on a uniform scale such as estimated financial damage including loss due to production stop and recovery costs. Table 5 lists examples of identified threats.

Table 5 Identifying of threats (example)

Threat	Area		Cause	Possible damage	Possible financial damage
	Device	Communication path			
The program of the programmable controller is tampered with a personal computer or IPC operated by an inside criminal.	Programmable controller	Programmable controller | Personal computer/IPC	Inside criminal	The robot or sensor controlled by the programmable controller operates unexpectedly, and the production stops.	XXX hundred-million yen
Data leaks due to illegally installed software.	Personal computer/IPC	Personal computer/IPC | Internet	Illegal software	Any programs or settings of the programmable controller or C controller leak, and a counterfeit is produced.	YYY hundred-million yen
The display device is operated by an illegal person, and the device operation information leaks.	HMI	HMI | Programmable controller	Illegal person	Device operation status leaks outside.	ZZZZ hundred-million yen
• • •	• • •	• • •	• • •	• • •	• • •

[25] Typically, threats can be listed by the approach based on assets such as equipment and devices or on scenarios of attack to the system.

3) Risk assessment

Assess the risks from the threats, and determines whether taking security measures is required. Considering the possible amount of damage by each threat identified in 2), examine if the measures against the risks are sufficient. For example, consider the following.

a) Rank the amount of damage with easily understandable values (such as financial damage), and set the priority.
b) Check whether effective measures are taken to the risks with high priorities, and list risks with insufficient measures.
c) Make sure that the cost of measures (such as equipment cost and operation cost) does not exceed the effect of measures (such as amount of damage to be reduced) in order to select cost-effective measures.

4) Consider/take measures

As a result of risk assessment, if the measures against a certain risk are judged as insufficient, consider and take additional measures by using the defense-in-depth approach. For considering and taking defense-in-depth measures, refer to 3.5.2.

Appendix C: Overview of IEC 62443

IEC 62443 is a standard that specifies measures against security problems in the industrial automation and control system. Focusing on the security of control systems, it involves many basic and important concepts related to safety of the current control system. IEC 62443 prioritizes the availability, integrity, and confidentiality in this order. In addition, one of its features is that it requires consideration for human health and safety and influence on the environment.

IEC 62443 is systematically divided into four parts from Part 1 to Part 4.

- IEC 62443-1: Definition of terms, concepts, and models of Industrial Automation And Control System (IACS[26]) security
- IEC 62443-2: Security policies and operation rules required for Asset Owners and methods of management and maintenance
- IEC 62443-3: Definition of security levels through the risk assessment process by dividing the network of the control system per security zone
- IEC 62443-4: Requirements for developing safe IACS products and solution and detailed technical requirements of IACS component levels as specific development and technical requirements of control system products

IEC 62443 is widely adopted mainly by Asset Owners (user companies), system integrators, suppliers (control device manufacturers). It is an important standard for designing and implementing security measures for control systems.

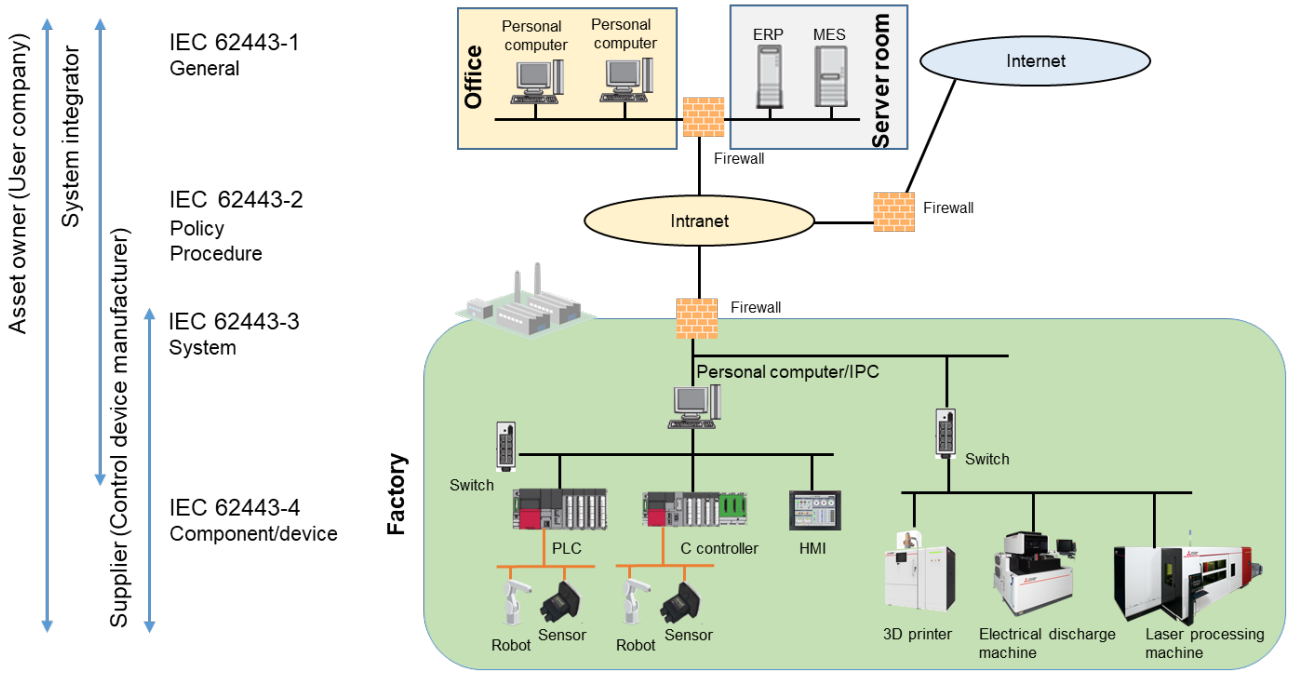


Figure 12 IEC 62443 compliance

[26] Industrial Automation and Control System

Appendix D: Inquiries about this document

For questions and inquiries on this document, contact your local sales office listed in Table 6. For the customers overseas, contact your local sales office listed in Table 7.

Table 6 Contact list of sales offices in Japan

Branch	Address		Tel
Equipment Sales Dep. in Head Office	1-30-7 Taitou, Taitou-ku, Tokyo 110-0016, Japan	Akihabara i-MARK Building	+81 -3-5812-1450
Industrial Mechatronics Sales Dep. in Head Office	1-18-6, Kagenuma, Minami-ku, Saitama, Saitama 336-0027, Japan		+81 -48-710-5750
Hokkaido Branch	4-1 Kitanijyounishi, Chuo-ku, Sapporo, Hokkaido 060-8693, Japan	Hokkaido Building	+81 -11-212-3794
Tohoku Branch	1-1-20 Kakyoin, Aoba-ku, Sendai, Miyagi 980-0013, Japan	Kakyoin Square	+81 -22-216-4546
Kanto Branch	11-2 Shintoshin, Chuo-ku, Saitama, Saitama 330-6034, Japan	Meiji Yasuda Life Saitama Shintoshin Building	+81 -48-600-5835
Niigata Branch	2-4-10 Higashiodori, Chuo-ku, Niigata, Niigata 950-8504, Japan	Nippon Life Building	+81 -25-241-7227
Kanagawa Branch	2-2-1 Minatomirai, Nishi-ku, Yokohama, Kanagawa 220-8118, Japan	Yokohama Landmark Tower	+81 -45-224-7227
Hokuriku Branch	3-1-1 Hirooka, Kanazawa, Ishikawa 920-0031, Japan	Kanazawa Park Building	+81 -76-233-5502
Chubu Branch	3-28-12 Meieki, Nakamura-ku, Nagoya, Aichi 450-6423, Japan	Dai Nagoya Building	+81 -52-565-3314
Toyota Branch	1-5-10 Kosakahonmachi, Toyota, Aichi 471-0034, Japan	Yahagi Toyota Building	+81 -565-34-4112
Kansai Branch	4-20 Ofukacho, Kita-ku, Osaka, Osaka 530-8206, Japan	Grand Front Osaka Tower A	+81 -6-6486-4122
Chugoku Branch	7-32 Nakamachi, Naka-ku, Hiroshima, Hiroshima 730-8657, Japan	Nippon Life Hiroshima Building	+81 -82-248-5348
Shikoku Branch	1-1-8 Kotobukicho, Takamatsu, Kagawa 760-8654, Japan	Nippon Life Takamatsuekimae Building	+81 -87-825-0055
Kyusyu Branch	2-12-1 Tenjin, Chuo-ku, Fukuoka, Fukuoka 810-8686, Japan	Tenjin Building	+81 -92-721-2247

Table 7 Contact list of overseas sales offices

Country /Region	Sales office/Address	Tel	Fax
USA	MITSUBISHI ELECTRIC AUTOMATION, INC. 500 Corporate Woods Parkway, Vernon Hills, IL 60061, U.S.A.	+1-847 -478-2100	+1-847 -478-2253
Mexico	MITSUBISHI ELECTRIC AUTOMATION, INC. Boulevard Miguel de Cervantes Saavedra 301, Torre Norte Piso 5, Ampliacion Granada, Miguel Hidalgo, Ciudad de Mexico, Mexico, C.P.11520	+52 -55-3067-7500	-
Brazil	MITSUBISHI ELECTRIC DO BRASIL COMÉRCIO E SERVIÇOS LTDA. Avenida Adelino Cardana, 293, 21 andar, Bethaville, Barueri SP, Brazil	+55 -11-4689-3000	+55 -11-4689-3016
Germany	MITSUBISHI ELECTRIC EUROPE B.V. German Branch Mitsubishi-Electric-Platz 1, 40882 Ratingen, Germany	+49 -2102-486-0	+49 -2102-486-1120
UK	MITSUBISHI ELECTRIC EUROPE B.V. UK Branch Travellers Lane, Hatfield, Hertfordshire, AL10 8XB, U.K.	+44 -1707-28-8780	+44 -1707-27-8695
Ireland	MITSUBISHI ELECTRIC EUROPE B.V. Irish Branch Westgate Business Park, Ballymount, Dublin 24, Ireland	+353 -1-4198800	+353 -1-4198890
Italy	MITSUBISHI ELECTRIC EUROPE B.V. Italian Branch Centro Direzionale Colleoni - Palazzo Sirio, Viale Colleoni 7, 20864 Agrate Brianza (MB), Italy	+39 -039-60531	+39 -039-6053-312
Spain	MITSUBISHI ELECTRIC EUROPE, B.V. Spanish Branch Carretera de Rubí, 76-80-Apdo. 420, 08190 Sant Cugat del Vallés (Barcelona), Spain	+34 -935-65-3131	+34 -935-89-1579
France	MITSUBISHI ELECTRIC EUROPE B.V. French Branch 25, Boulevard des Bouvets, 92741 Nanterre Cedex, France	+33 -1-55-68-55-68	+33 -1-55-68-57-57
Czech Republic	MITSUBISHI ELECTRIC EUROPE B.V. Czech Branch Avenir Business Park, Radlicka 751/113e, 158 00 Praha 5, Czech Republic	+420 -251-551-470	+420 -251-551-471
Poland	MITSUBISHI ELECTRIC EUROPE B.V. Polish Branch ul. Krakowska 50, 32-083 Balice, Poland	+48 -12-347-65-00	+48 -12-630-47-01
Sweden	MITSUBISHI ELECTRIC EUROPE B.V. (Scandinavia) Fjelievägen 8, SE-22736 Lund, Sweden	+46 -8-625-10-00	+46 -46-39-70-18
Russia	MITSUBISHI ELECTRIC (RUSSIA) LLC St. Petersburg Branch Piskarevsky pr. 2, bld 2, lit “Sch”, BC “Benua”, office 720; 195027 St. Petersburg, Russia	+7 -812-633-3497	+7 -812-633-3499
Turkey	MITSUBISHI ELECTRIC TURKEY A.Ş Ümraniye Branch Serifali Mahallesi Nutuk Sokak No:5, TR-34775 Umraniye/Istanbul, Turkey	+90 -216-526-3990	+90 -216-526-3995
UAE	MITSUBISHI ELECTRIC EUROPE B.V. Dubai Branch Dubai Silicon Oasis, P.O.BOX 341241, Dubai, U.A.E.	+971 -4-3724716	+971 -4-3724721
South Africa	ADROIT TECHNOLOGIES 20 Waterford Office Park, 189 Witkoppen Road, Fourways, South Africa	+27 -11-658-8100	+27 -11-658-8101
China	MITSUBISHI ELECTRIC AUTOMATION (CHINA) LTD. Mitsubishi Electric Automation Center, No.1386 Hongqiao Road, Shanghai, China	+86 -21-2322-3030	+86 -21-2322-3000
Taiwan	SETSUYO ENTERPRISE CO., LTD. 6F, No.105, Wugong 3rd Road, Wugu District, New Taipei City 24889, Taiwan	+886 -2-2299-2499	+886 -2-2299-2509
	MITSUBISHI ELECTRIC TAIWAN CO., LTD No.8-1, Industrial 16th Road, Taichung Industrial Park, Taichung City 40768, Taiwan, R. O. C.	+886 -4-2359-0688	+886 -4-2359-0689
Korea	MITSUBISHI ELECTRIC AUTOMATION KOREA CO., LTD. 7F-9F, Gangseo Hangang Xi-tower A, 401, Yangcheon-ro, Gangseo-Gu, Seoul 07528, Korea	+82 -2-3660-9530	+82 -2-3664-8372

Singapore	MITSUBISHI ELECTRIC ASIA PTE. LTD. 307 Alexandra Road, Mitsubishi Electric Building, Singapore 159943	+65 -6473-2308	+65 -6476-7439
Thailand	MITSUBISHI ELECTRIC FACTORY AUTOMATION (THAILAND) CO., LTD. 12th Floor, SV.City Building, Office Tower 1, No. 896/19 and 20 Rama 3 Road, Kwaeng Bangpongpang, Khet Yannawa, Bangkok 10120, Thailand	+66 -2682-6522	+66 -2682-6020
Vietnam	MITSUBISHI ELECTRIC VIETNAM CO., LTD. Unit 01-04, 10th Floor, Vincom Center, 72 Le Thanh Ton Street, District 1, Ho Chi Minh City, Vietnam	+84 -8-3910-5945	+84 -8-3910-5947
Indonesia	PT. MITSUBISHI ELECTRIC INDONESIA Gedung Jaya 8th Floor, Jl MH.Thamrin No 12 Jakarta Pusat 10340 Indonesia	+62 -21-3192-6461	+62 -21-3192-3942
India	MITSUBISHI ELECTRIC INDIA PVT. LTD. Pune Branch Emerald House, EL-3, J Block, M.I.D.C., Bhosari, Pune-411026, Maharashtra, India	+91 -20-2710-2000	+91 -20-2710-2100
Australia	MITSUBISHI ELECTRIC AUSTRALIA PTY. LTD. 348 Victoria Road, P.O. Box 11, Rydalmere, N.S.W 2116, Australia	+61 -2-9684-7777	+61 -2-9684-7245