XFB3-20PS002-B

FA SYSTEM SECURITY GUIDELINE

- FOR SAFE USE OF MITSUBISHI ELECTRIC FA PRODUCTS -

V2.0

MITSUBISHI ELECTRIC CORPORATION

Revision history

Date	Document number	Notes
Sep, 2020	XFB3-20PS002	First edition
Apr, 2021	XFB3-20PS002-A	Appendix “Inquiries about this document” is added
Jun, 2022	XFB3-20PS002-B	Detail descriptions of security risk assessment are added

Contents

Terms and Definitions

Term	Description
Availability[1]	The state that exists when data can be accessed, or a requested service provided within an acceptable period of time.
Confidentiality[2]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
DoS[3]	Denial of Service. The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided).
ERP[4]	Enterprise Resource Planning. A method/concept of managing an entire corporation in an integrated manner from the standpoint of effective utilization of enterprise resources to improve business efficiency.
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.
IDS[5]	Intrusion Detection System. Software that looks for suspicious activity and alerts administrators.
IEC62443[6]	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).
Integrity[7]	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
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.
IPS[8]	Intrusion Prevention System. System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
IT	Information Technology. A generic term for all technologies related to computers and networks.
MES	Manufacturing Execution System. An integrated manufacturing information system for managing production processes.
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[9]	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.
VPN[10]	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability[11]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[1] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/availability

[2] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/confidentiality

[3] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/denial_of_service

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

[5] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/ids

[6] International Society of Automation(ISA), https://www.isa.org/intech/201810standards/

[7] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/integrity

[8] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/ips

[9] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/supply_chain

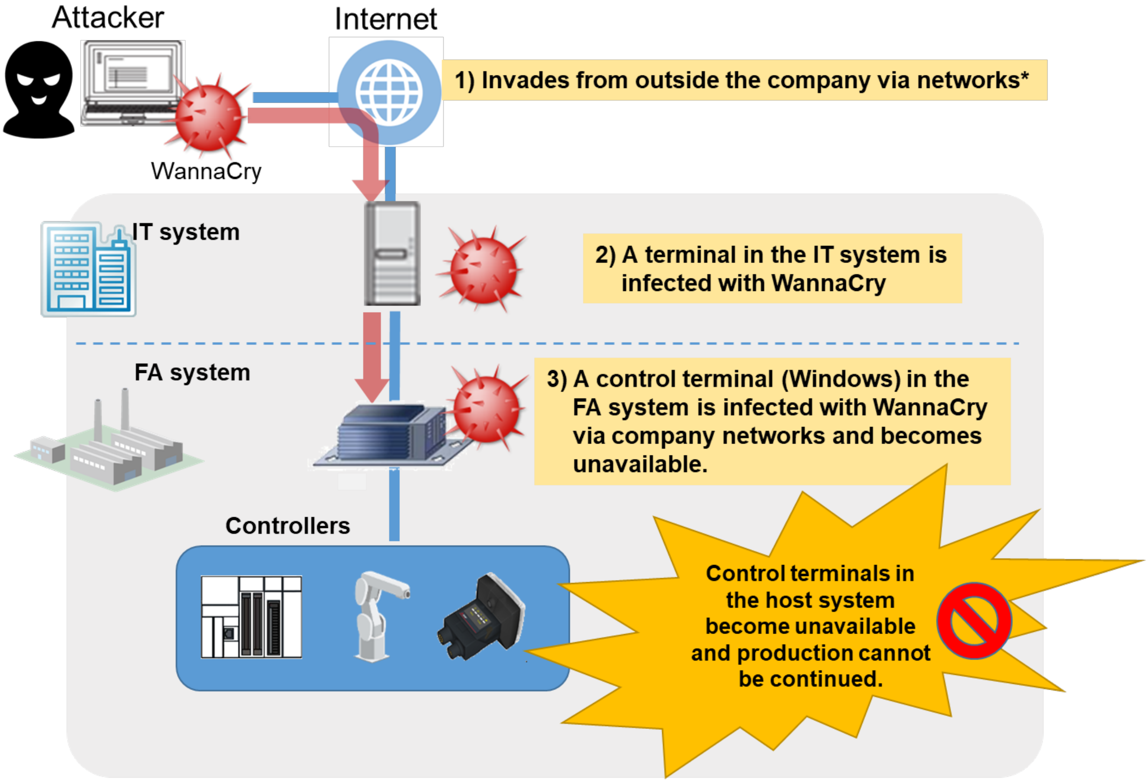
[10] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/vpn

[11] 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[12] which initially targeted IT systems, and subsequently brought the factories of multiple companies to a halt. (Figure 1)


Attacker
Internet
WannaCry
1) Invades from outside the company via networks*
IT system
2) A terminal in the IT system is infected with WannaCry
FA system
3) A control terminal (Windows) in the FA system is infected with WannaCry via company networks and becomes unavailable.
Controllers
Control terminals in the host system become unavailable and production cannot be continued.

* Attacks TCP 445 port directly. Infected even without opening an e-mail.

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[13]. As a company manufacturing and selling FA products, Mitsubishi Electric (hereinafter referred to as "our company") has started developing FA products[14] incorporating the defense-in-depth strategy to provide customers with safe and secure FA systems.

[12] 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.

[13] For IEC 62443, refer to Appendix C.

[14] 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	Security Approaches of Mitsubishi Electric	Read this chapter to understand the security concepts and approaches towards our FA products.
Chapter 3	Construction and Operation of a Secure FA System	Read this chapter when constructing or operating a security-friendly FA system.

1.3. Disclaimer

Security-related information in this document is based on the results of our analysis and examination[15]. 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.

[15] 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. Mitsubishi Electric’s Approach to FA Security

2.1. Basic security policy for Mitsubishi Electric’s FA products

This chapter describes our basic security policy as applied to FA products[16].

Our company strives to provide safe and secure products that conform to domestic and international security standards for control systems (such as IEC62443). In addition, our company makes continuous efforts that contribute to maintain and improve the following six elements[17] 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[18]
- 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 a safe and secure environment for all customers. We will make continuous efforts in the "Enhancement of FA Cyber Security" with reference to ensuring the key elements of Health, Safety, and Environment in order to protect Availability, Integrity, and Confidentiality (Figure 2).

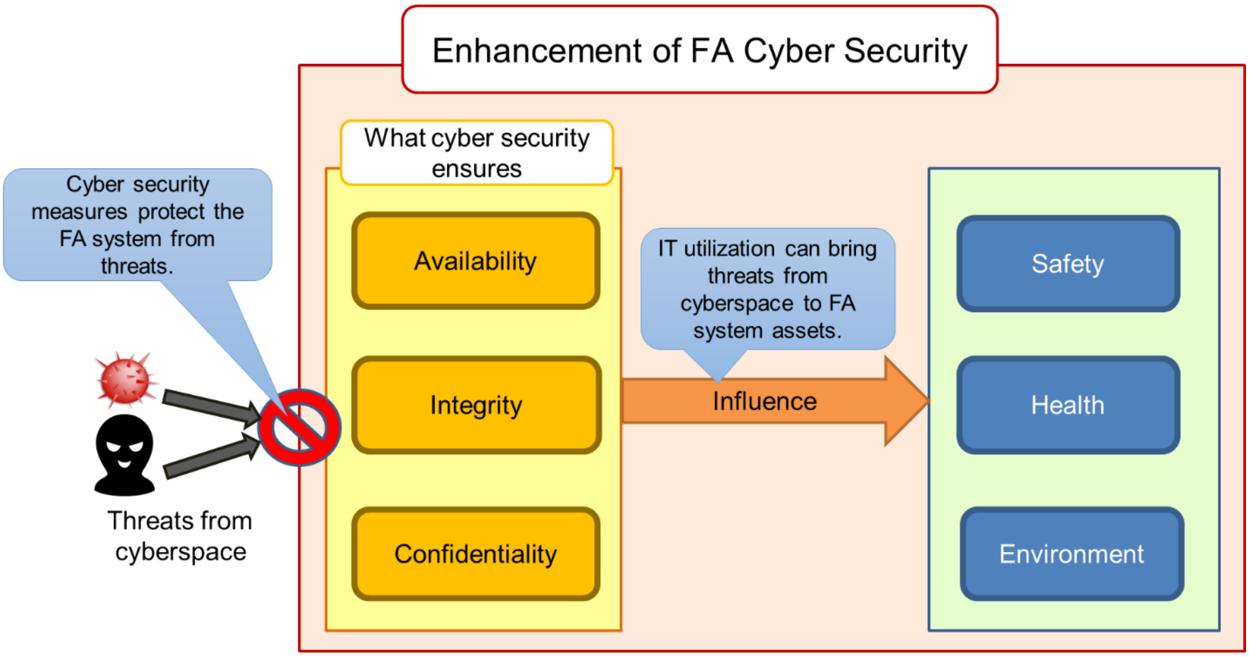

Enhancement of FA Cyber Security
What cyber security ensures
Cyber security measures protect the FA system from threats.
Availability
Integrity
Confidentiality
IT utilization can bring threats from cyberspace to FA system assets.
Influence
Safety
Health
Environment
Threats from cyberspace

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

We believe that protecting a Factory system from cyber-attacks which compromise Availability, Integrity and Confidentiality, is necessary in order to reduce the risk of causing incidents related to Health, Safety and the

[16] 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)

[17] 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.

[18] 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.

Environment. For this reason, this document mainly describes measures related to Availability, Integrity, and Confidentiality.

2.2. Approaches for the Enhancement of FA Cyber Security

2.2.1. Basic Considerations for Realizing the 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 approaches that includes points 1) to 5) including the customer's FA system and supply chain (Figure 3).

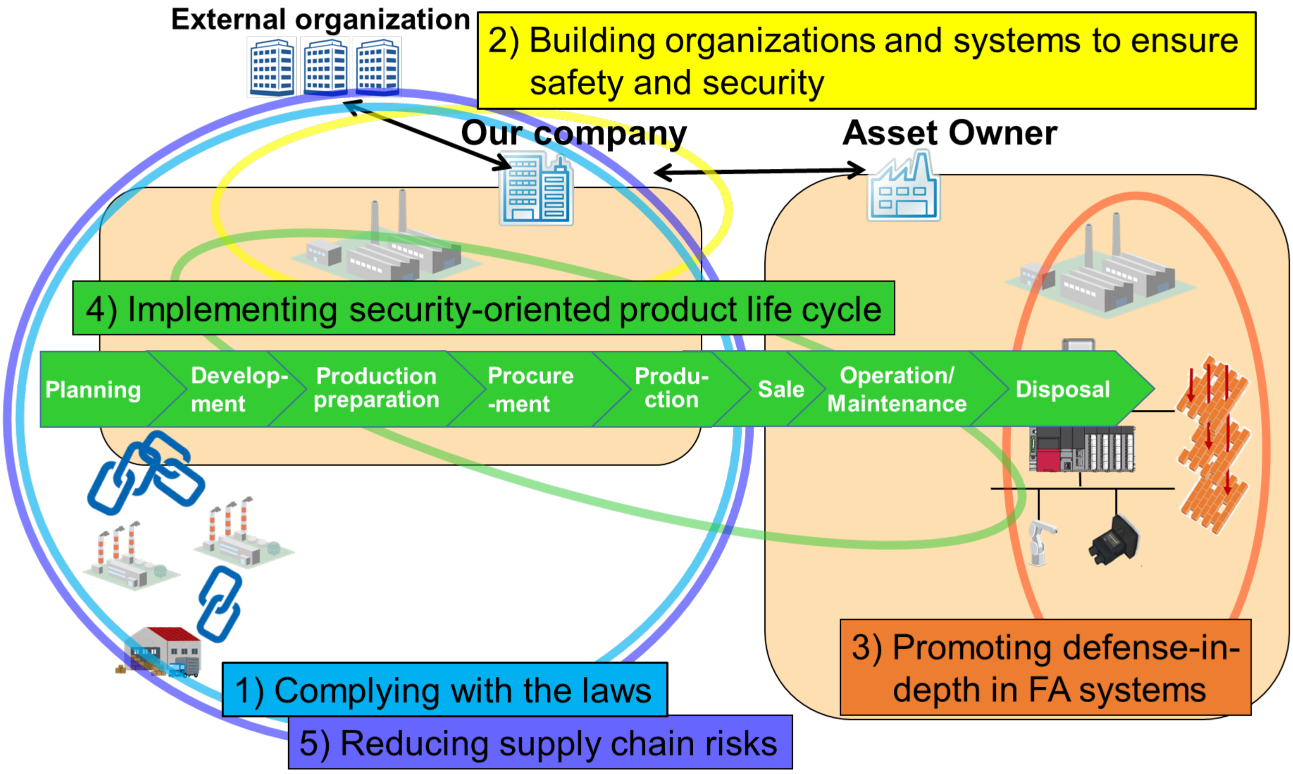

External organization
2) Building organizations and systems to ensure safety and security
Our company
Asset Owner
4) Implementing security-oriented product life cycle
Planning
Develop-ment
Production preparation
Procure-ment
Produ-ction
Sale
Operation/ Maintenance
Disposal
3) Promoting defense-in-depth in FA systems
1) Complying with the laws
5) Reducing supply chain risks

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

1) Complying with the law

   We will comply with all relevant laws and regulations related to the security of our FA products. (For details, refer to 2.2.2.) In addition, we take appropriate measures to protect personal information in accordance with our "Personal Information Protection Policy".

2) Building organizations and systems to ensure security and safety

   Our company has established a Product Security Incident Response Team (PSIRT), 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 2.2.3.)

   In addition, we will communicate with our customers swiftly, appropriately, and actively regarding security improvement of FA products.

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 customers' 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 customers. The provision of this guideline is a part those efforts. (For details on the concept of defense-in-depth, refer to 3.2.1.)

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 2.2.5.)
5) Reducing supply chain risks[19]
   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 2.2.4.)

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).

2.2.2. 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)

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

2.2.3. 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.

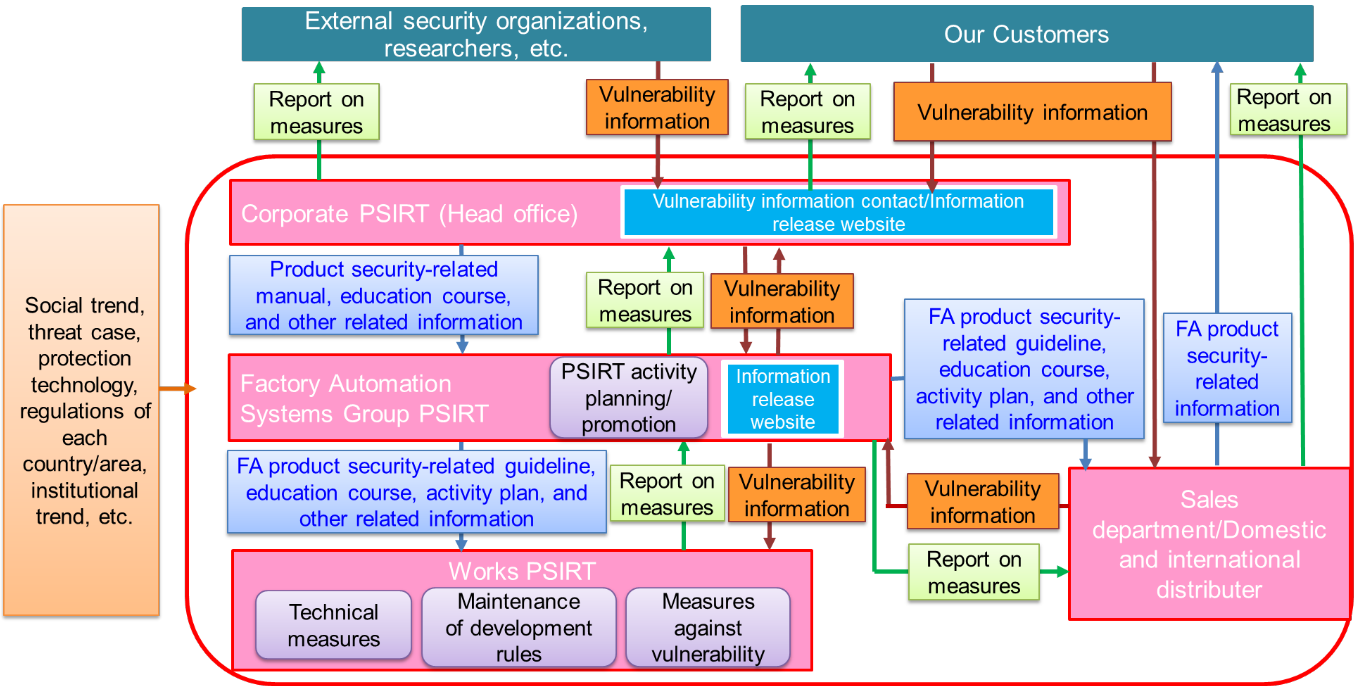

External security organizations, researchers, etc.
Our Customers
Report on measures
Vulnerability information
Report on measures
Vulnerability information
Report on measures
Social trend, threat case, protection technology, regulations of each country/area, institutional trend, etc.
Corporate PSIRT (Head office)
Vulnerability information contact/Information release website
Product security-related manual, education course, and other related information
Report on measures
Vulnerability information
FA product security-related guideline, education course, activity plan, and other related information
FA product security-related information
Factory Automation Systems Group PSIRT
PSIRT activity planning/ promotion
Information release website
FA product security-related guideline, education course, activity plan, and other related information
Report on measures
Vulnerability information
Vulnerability information
Report on measures
Sales department/Domestic and international distributer
Works PSIRT
Technical measures
Maintenance of development rules
Measures against vulnerability

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 products from external security organizations[20], 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[21] we can 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.

2.2.4. 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.

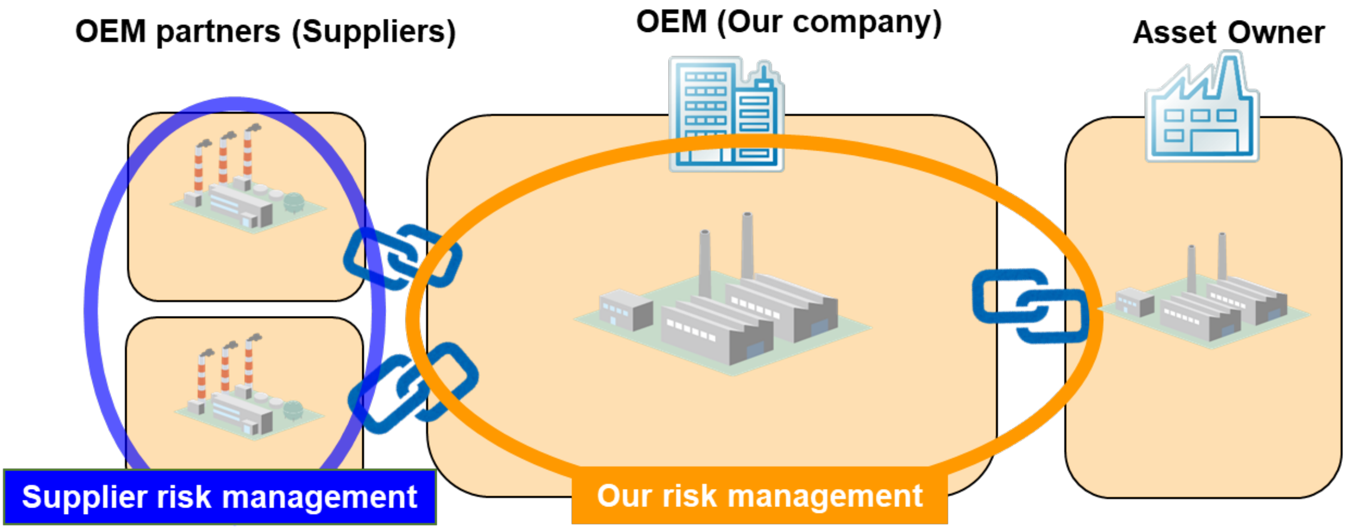


Figure 5 Scope of our approaches to reduce supply chain risks

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

[21] For contacts, refer to Appendix D.

- **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)[22]

(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

- **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

2.2.5. 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.

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

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.

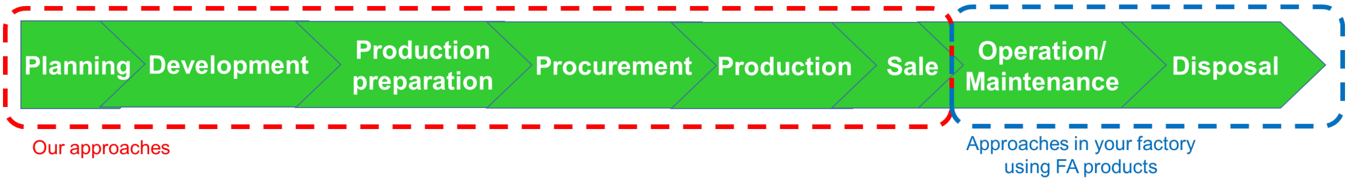


Figure 6 Product development lifecycle

Our 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 3.2.1 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[23] 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.

[23] 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.

(5) Sale

As the supplier of the FA products, our company strives to reduce customers' security risks as shown in 2.2.4. 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. Construction and Operation of a Secure FA System

3.1. Security risk assessment

3.1.1. What is security risk assessment?

When taking security measures, it is important to select effective measures that reduce risks. Effective measures can be identified by implementing a "security risk assessment" that identifies threats to the FA system to be protected and the appropriate measures against these threats. A security risk assessment clarifies the extent of the FA system to be protected, the required security measures, and allows prioritizing and the taking of effective actions for risk reduction.

Attackers use vulnerabilities in FA systems to execute their cyber-attacks. Therefore, even if you introduce high cost measures, they may NOT always be effective. Also, introducing all possible measures is NOT feasible either, due to the enormous costs and demands on resources. In order to introduce effective and targeted measures within a limited budget, it is necessary to carry out a security risk assessment.

3.1.2. Procedure of security risk assessment

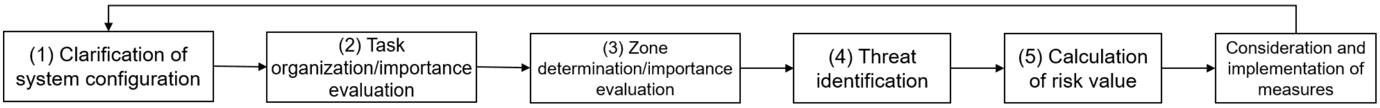

(1) Clarification of system configuration
(2) Task organization/importance evaluation
(3) Zone determination/importance evaluation
(4) Threat identification
(5) Calculation of risk value
Consideration and implementation of measures

Figure 7 Procedure of security risk assessment

A security risk assessment has the following five phases.

(1) Determination of the scope and clarification of the system configuration

A key part of the security risk assessment is the definition of the FA system to be assessed. In this phase it is helpful to check and organize devices and their roles in the FA system, the network connection relationships, and division of physical area of each system of the FA system as figures and tables.

(2) Organization and evaluate the importance of tasks

For each FA system organized in (1) above, identify the operations related to that system. In addition, evaluate the importance of each task based on factors such as the amount of financial damage in case of stoppage, or the impact on production operations.

(3) Determination of operational zones and the importance of the zones

For the FA system under evaluation in (1), divide the FA system into logical zones based on the information about tasks and asset locations/use. In addition, for those tasks associated with each zone evaluate the importance of each zone based on the result of the assessment of task importance performed in (2).

(4) Threat identification

Potential threats are enumerated, examining factors such as the function of the zone, the devices and their roles in the FA system identified in (1), the network connection relationships and physical division of each area as defined in (2), assumptions of the attack method and review with a list of possible threats.

(5) Calculation of risk value

Risk values are quantitively calculated based on the importance of the zone, the likelihood (level) of threat occurrence as organized in phases (3) and (4).

A risk value for each threat can be calculated in the above procedure. According to this calculation, high-risk threats can be prioritized for risk reduction measures, and security measures can be implemented in a cost-effective manner. The method of considering security measures is described in 3.2.

Security risk assessments should be performed continuously as new risks may emerge over time. Repeatedly performing security risk assessments can help mitigate risks by re-evaluating remaining risks from the last assessment and considering potential measures against new risks.

3.1.3. Determination of the scope of analysis and the clarification of the FA system configuration

In preparation for a security risk assessment, the scope of the analysis should be clearly defined. It is necessary to define which parts of the information system, production management system, control system or any other office systems where the analysis should be performed. It is recommended that the analysis is conducted on systems for which there are devices or servers that may affect the control or monitoring of the factory.

Next, for the determined scope of analysis, clarify the system configuration as a diagram or table. The following information is needed when defining the system configuration.

- Devices in the system and their roles

  Organize devices according to their role in the system, for example if a personal computer is connected to the system, what is its role? Is it is used for control, maintenance, or for other purposes?
- Network connections and the flow of information

  It is important to understand which devices are connected to each other, by what communication method, and from which devices information flows.

  It is also important to clarify the connection between networks. Devices such as firewalls, routers, and VPN devices are often installed at the points where connection between the networks is made. They can be used as definitions of the system boundaries and can clarify its connection points.
- Define the physical area of each system

  In addition to the logical definition of each system, a definition of the physical aspects is also required, for example, what kind of physical security measures are in place, in which areas, and containing which devices. The area’s should be listed up by factors such as if the system elements are in a common area, where any staff member can access them, or in a restricted area.

Figure 8 in this guideline shows an example of a system configuration that could be used in a security risk assessment.

The figure shows how various pieces of equipment such as sequencers (PLCs), displays (HMIs), robots, NC systems, electric discharge machines, and laser machines are installed and arranged in multiple areas in the example factory. Additionally, the factory's engineers maintain/access those FA devices using personal computers installed in the office. Furthermore, a data processing server, for production control, is installed in a server room. The factory, office, and server room are all connected to the company's intranet via firewalls as well as being connected to the Internet, also via a firewall.

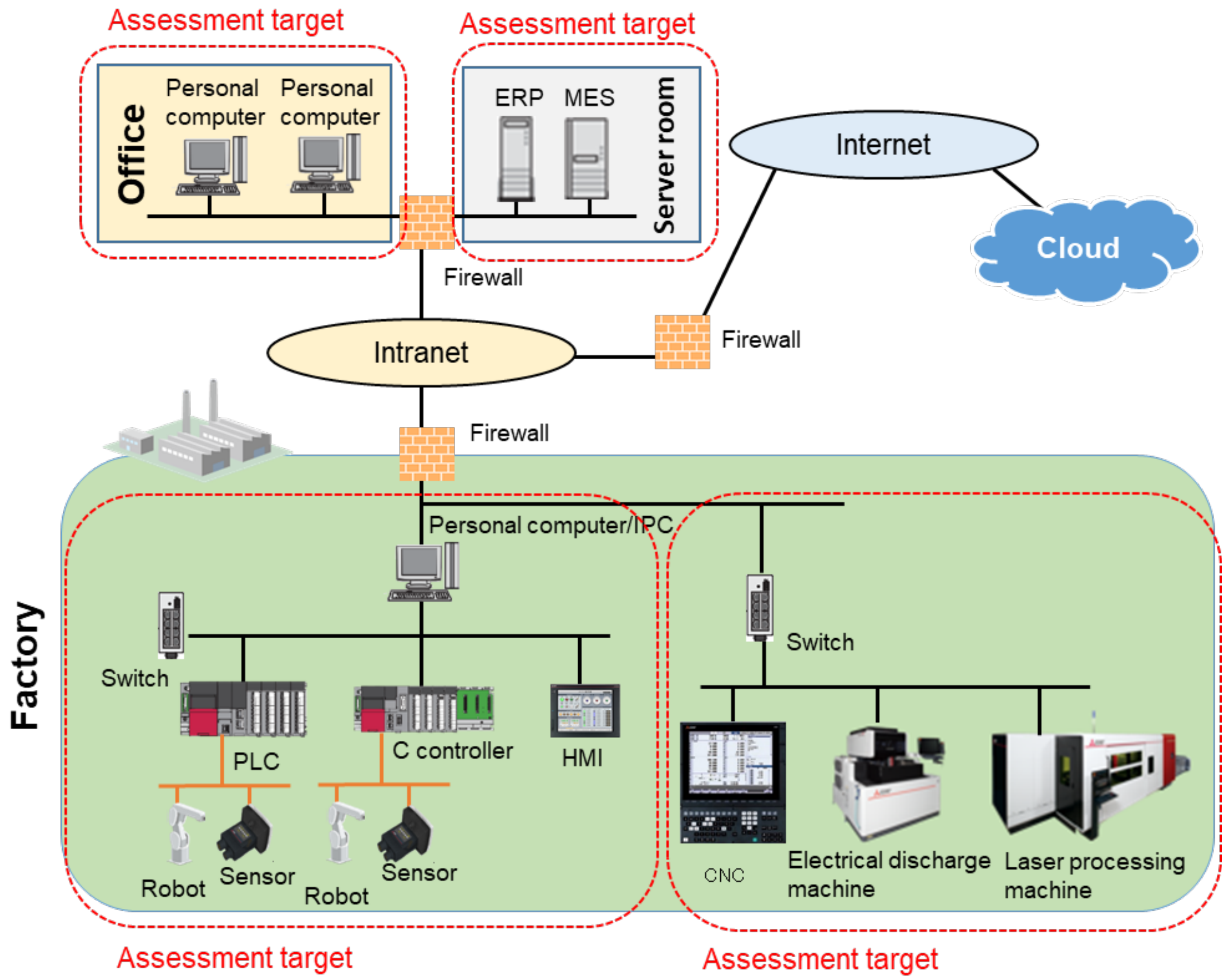


Figure 8 FA System configuration example

It is not necessary to express every single individual device and network in the FA system configuration diagram for the risk assessment. It will take too long to create the diagram, be prone to errors, and it will often be too complicated to understand. Therefore, if multiple devices with the same function, role, and communication destination are lined-up in parallel, it is a good idea to represent them as one (example) in the configuration diagram.

3.1.4. Organize operational tasks and assess their importance

This section describes the process of organizing and evaluating the importance of tasks, which is the next step in the preparation of the security risk assessment. This section utilizes the FA system structure defined in section 3.1.3 .

- Department/person in charge of the task/operation

  Clarify the department or person(s) in charge of the task. It is especially important whether a task will be performed by an internal department (or staff member) or if it will be outsourced to an external company.
- Devices used for the task

  Identify all devices required for the task, such as the equipment and/or devices to be used in the FA system.
- Information used for the task

  Organize the information related to the task, such as the input information used for the task and the output information as a result.
- Description of the task/operation

  Detail what task/operations will be performed using the equipment and information.

Next, for each of the task/operations detailed, the level of importance should be evaluated against a standard criteria list, the amount of potential damage, and/or the degree of impact on production etc.. Table 2 shows an example of an importance evaluation based on the degree of impact on production when the task/operation is stopped. For example, the importance of a precision machining process is evaluated as “high”, if as a result of the processing machine stopping, the total production line would stop. On the other hand, if production could continue despite the processing machine stopping, then the evaluation of importance would be “low”. The example shown in Table 2 identifies the result of the importance evaluation for various tasks/operations.

No	Task	Department in charge	Description	Importance
1	Production plan setting	Production management department	• Set recipes (parameters) from the personal computer to MES server.	Medium
2	Recipe setting	Production management department	• Set recipes (parameters) from the personal computer to MES server.	Low
3	Processing and assembly (+ Inspection)	Manufacturing department	• The instruction sent from the MES server to the production line, such as production model and production volume, will trigger the set-up change on the production site. The facilities acquire the recipe from the MES server and starts the production line. • Perform assembly and processing using the robot and others.	Medium
4	Precision machining (+ Inspection)	Manufacturing department	• The instructions sent from the MES server to the production line, such as production model and production volume, will trigger the set-up change on the production site. The facilities acquire the recipe from the MES server and starts the production line. • Perform the Precision machining using the laser processing machine and others.	High
5	Production status monitoring (Production site)	Manufacturing department	• The HMI acquires the production status listed in the MES server and displays it on the screen.	Medium
6	Productivity analysis	Production management department	• With the personal computer, acquire the production performance information such as past production volume and production defects stored in the MES server, and analyze the data to identify the area where improvement is required.	Low
7	Quality inspection information reference	Quality management section	• With the personal computer, acquire the quality inspection information in the MES server.	Low
8	Maintenance	Equipment vendor Production engineering department	• Physically connect the personal computer for maintenance to the equipment at the production line to upgrade programs and set parameters.	Low
9	Remote maintenance	Equipment vendor	• Connect to the equipment on the production line via the Internet to acquire the degree of deterioration of the equipment (components, etc.). Adjust parameters as necessary.	Low
10	Production program creation	Production engineering department	• Develop and test programs for operating the production facilities.	Low
11	Processing drawing creation	Design department	• Develop and test drawings for performing processing with production facilities.	Low

Table 2 Importance evaluation

3.1.5. Identifying zones and evaluating their importance

This section describes how to divide the FA system configuration into zones and evaluate each zones importance. Dividing the overall system configuration into zones makes it easy to identify threats according to the characteristics of each zone and if the threat affect shows itself inside or outside of the zone. By doing this, detailed consideration can be made of the appropriate security measures needed to achieve the target security level for each zone.

To define the zones, use the FA system configuration (as described in 3.1.3) as the basis, then create logical zones by device/equipment usage or the classification of the physical area in which the devices and equipment are placed. For example, an area where production management servers and personal computers for production control are placed could be defined as the "Production management zone", equally an area where equipment and computers for engineering would be the "Engineering zone", and finally an area in the factory where production equipment is placed could be the "Control zone". Figure 9 shows an example of how zone division can be applied to the sample FA system configuration. At an actual production site, there may be cases where devices/equipment for different purposes are physically installed in the same area, such as a server for production control installed in the factory, but in this example, it is assumed that there is no such mixing of equipment.

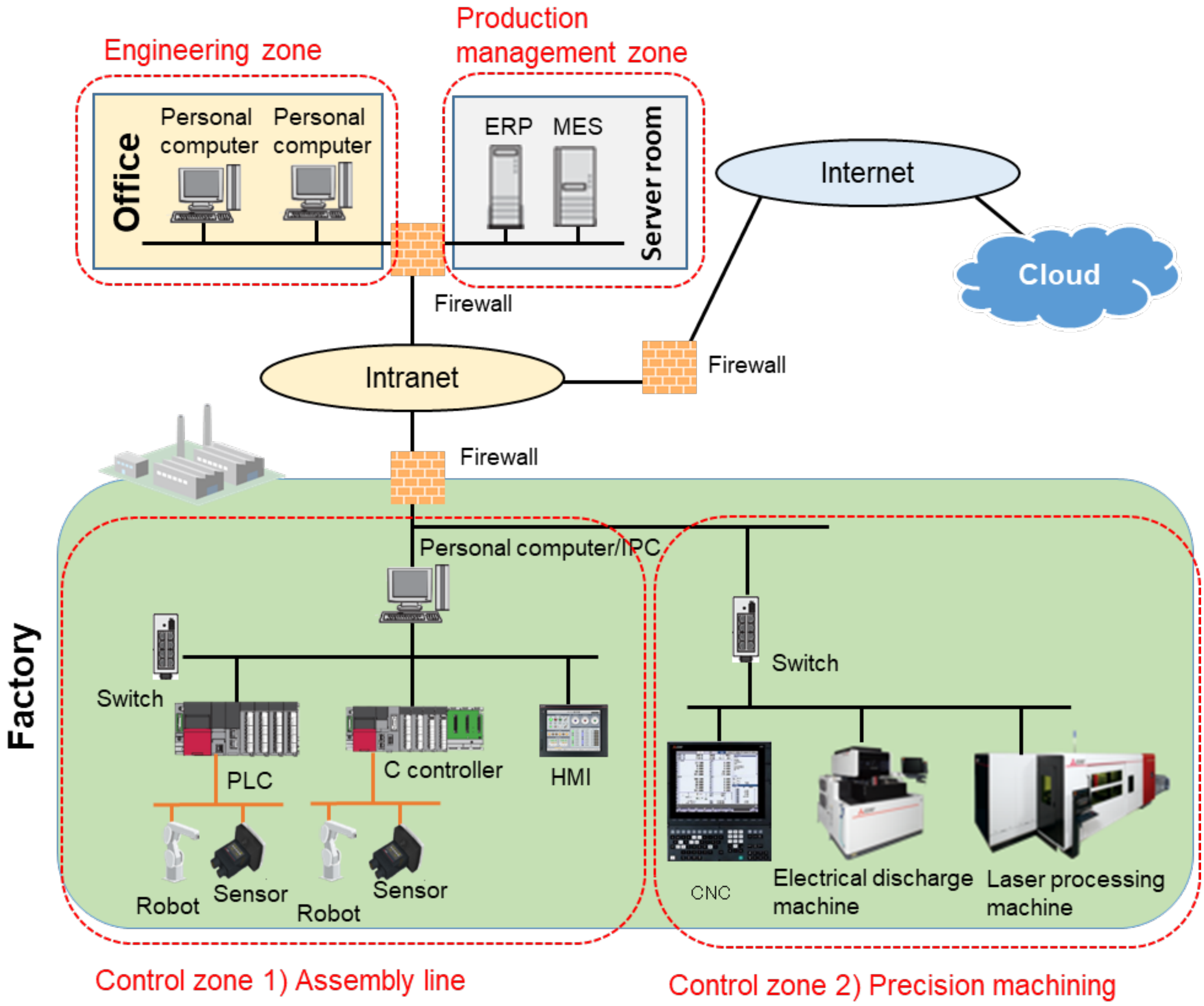


Figure 9 Example of zone division

Next, evaluate the importance of each of the divided zones. Use the importance of the tasks/operations defined in 3.1.4 and assign them to each applicable zone. To evaluate the importance of a zone, use the task/operation with the highest level of importance and apply that same level of importance to the zone itself. Table 3 shows an example of applying the evaluation of the importance of tasks to a zone.

Table 3 Example of zone importance evaluation

Name	Overview	Related task	Importance
Control zone 1) (Assembly line)	A production line for assembling products. It is a zone consisting of control devices and equipment.	• Assembly production (+ Inspection) (Medium) • Production status monitoring (Production site) (Medium) • Maintenance (Low) • Remote maintenance (Low)	Medium
Control zone 2) (Precision machining)	A production line for Precision machining. It is a zone consisting of control devices and equipment.	• Precise production (+ Inspection) (High) • Production status monitoring (Production site) (Medium) • Maintenance (Low) • Remote maintenance (Low)	High
Production management zone	A zone consisting of a group of servers that manage production plans and traceability data.	• Production plan setting (Medium) • Recipe setting (Low) • Production (+ Inspection) (High) • Production status monitoring (Production site) (Medium) • Productivity analysis (Low) • Quality inspection information reference (Low)	High
Engineering zone	A zone for developing programs for production facilities and designing drawings to be used in the production.	• Production program creation (Low) • Processing drawing creation (Low)	Low

3.1.6. Threat identification

In general, there is a vast array of threats to security. In this document, threats to the FA system are classified into "reduced availability ", "data falsification/destruction", "data theft/leakage ", and "unauthorized intrusion". For each classified threat to the FA system, it is necessary to identify the specific details of the threat by simulating how the equipment/device functions or the installation environment could be attacked. This can be done by considering the attack scenarios leading up to the occurrence of the threat, and by referring to risk assessment documents such as the ones published by Information-technology Promotion Agency (IPA)[24]. After the threats are identified, organize the threats based on their scale of impact, such as the cost of recovery and degree of impact on production. Table 4 shows an example of threat organization. In this example, the degree of impact on production is used to evaluate the impact of threat occurrence.

Table 4 Example of threat organization

Threat type	Threat description	Effect on production (Example)Intrusion
Availability degradation	• Excessive load on the network (DoS attack) • Unauthorized execution by attacking unused services of FA products	• Delayed delivery due to lower productivity • Occurrence of personal injury, disaster, and failure due to loss of facility control • Poor quality accompanied by brand defamation
Falsification/destruction of data	• Falsification of programs and data in FA products • Falsification of device operation information • Falsification of upper-level system management data in the server/personal computer	• Poor quality accompanied by brand defamation • Delayed delivery due to lower productivity • Occurrence of personal injury, disaster, and failure due to facility malfunction
Theft/leakage of data	• Leakage of Production know-how from FA products • Leakage of device operation information • Leakage of upper-level system management data from in the server/personal computer • Leakage of production data due to interception of communication via the intranet	• Leakage of production information and quality assurance know-how
Intrusion	• Physical intrusion into the zone • Intrusion into the server/personal computer via the internet • Installation of illegal software to the server/personal computer	• Leakage of production information and quality assurance know-how • Leakage of customer information accompanied by brand defamation

[24] IPA Guide for Analyzing Security Risks to Control Systems 2nd edition - Implementation and Utilization of Risk Assessment in Security Measures - (https://www.ipa.go.jp/security/controlsystem/riskanalysis.html)

3.1.7. Calculating risk values

As the final phase of the security risk assessment, this section describes how to calculate risk values.

To evaluate the potential of threat occurrence, an understanding of the zone breakdown, identified in 3.1.5, and the threat types to each zone, detailed in 3.1.6, is required. The likelihood of each threat occurring is categorized in three levels as follows.

Table 5 Evaluation standard for the possibility of threat occurrence

Possibility of threat occurrence	Determination level
3	High possibility of occurrence
2	Medium possibility of occurrence
1	Low possibility of occurrence

When evaluating the likelihood of threat occurrence, if countermeasures have already been introduced for the threat, then the countermeasures should also be considered in the evaluation. In addition, the above criteria are an “abstract” evaluation example. When considering an actual threat, the number of levels of likelihood and their associated evaluation criteria should be set according to the characteristics of each threat. The criteria for setting the appropriate evaluation measures might include several issues, for example, a focus on the attacker (source of the threat), the logical or physical arrangement of the attack target could also be a factor. For more detailed examples of evaluation criteria, please refer to documents such as the analysis guide published by the IPA. For this example, the table below defines three possible threat levels based on physical access.

Table 6 Occurrence possibility of threats based on physical access

Possibility of threat occurrence	Determination level
3	The attack target is located in a place accessible by everyone.
2	The attack target is located in a place accessible by limited persons.
1	The attack target is located in a place with strict access control, such as a room where entry is strictly limited.

Note: Since some level of knowledge and experience of security can help in threat identification and the judgment of the possibility of threat occurrence, it is highly recommended to consult dedicated security specialists/vendors.

Finally, the risk value is calculated according to the importance of a zone and the possibility of the threat occurring. The following table shows an example of how risk values are calculated. In this table, a risk value is set in each cell according to the importance of the zone in the vertical axis and the threat possibility in the horizontal axis. In this example, the threat likelihood uses the threat potential 1-3 criteria from Table 5. In addition, the risk value is set in five stages from A to E in descending order of risk.

Table 7 Example of risk value calculation

	Possibility of occurrence: 3	Possibility of occurrence: 2	Possibility of occurrence: 1
Importance of zone: High	A	B	C
Importance of zone: Medium	B	C	D
Importance of zone: Low	C	D	E

The risk values are calculated for each zone according to the risk value calculation criteria, and the results are organized into a table. Table 8 shows an example of risk value calculation for the threats in each zone.

Table 8 Risk value calculation results

Zone	Threat	Implemented measures	Possibility of occurrence	Risk value
Control zone 1) (Assembly line) Importance: Medium	Physical intrusion into the zone	Entry/exit restriction	1	D
	Intrusion via the internet	Installation of a firewall	2	C
	Installation of illegal software to the server/personal computer	None	3	B
	Leakage of Production know-how from FA products	None	3	B
	Leakage or falsification of device operation information	None	2	C
Control zone 2) (Precision machining) Importance: High	Physical intrusion into the zone	Entry/exit restriction	1	C
	Intrusion via the internet	None	3	A
	Leakage of Production know-how from FA products	None	3	A
	Leakage or falsification of device operation information	None	2	B
Production management zone Importance: High	Physical intrusion into the zone	Entry/exit restriction	1	C
	Intrusion via the internet	Installation of a firewall	2	B
	Installation of illegal software to the server/personal computer	None	3	A
	Leakage of production data due to interception of communication via the intranet	None	2	B
	Leakage of upper-level system management data from in the server/personal computer	Login authentication	2	B
Engineering zone Importance: Low	Physical intrusion into the zone	Entry/exit restriction	1	E
	Intrusion via the internet	Installation of a firewall	2	D
	Installation of illegal software to the server/personal computer	Installation of antivirus software	2	D
	Leakage or falsification of programs and data in FA products	Login authentication	2	D

The security risk assessment is complete once the risk value calculation is complete. The next chapter describes the consideration process when reviewing security measures to be implemented according to the calculated risk values.

3.2. Implementing security measures

3.2.1. Security measures for FA systems

This section describes how to implement security measures for FA systems based on the results of security risk assessment. Using that risk assessment and prioritizing measures against high-risk threats (identified by their calculated risk values) effective countermeasures can be implemented within a limited budget.

Security countermeasures against threats identified by security risk assessment should be considered within a concept called "defense-in-depth". This concept examines measures in a multilayered approach from different points of view such as "human operation", "use of device/equipment", "network access", and "execution of application". Our company divides these points of view into those related to the environment (outside of the product) and those related to the inside of the product, from the perspectives of the "human layer", "physical layer", "network layer", and "device layer" (Figure 10). The defense-in-depth approach reduces the impact of attacks by making attackers incur higher attack costs, and by enhancing the ability to detect and prevent attacks.

The security functionality of FA products can be considered as one of the defense-in-depth measures. To protect FA systems from cyber-attack, our company recommends; installing a firewall to prevent intrusion into factory networks, installing antivirus software into the personal computer, and consider installing the physical entry and exit controls in the factory.

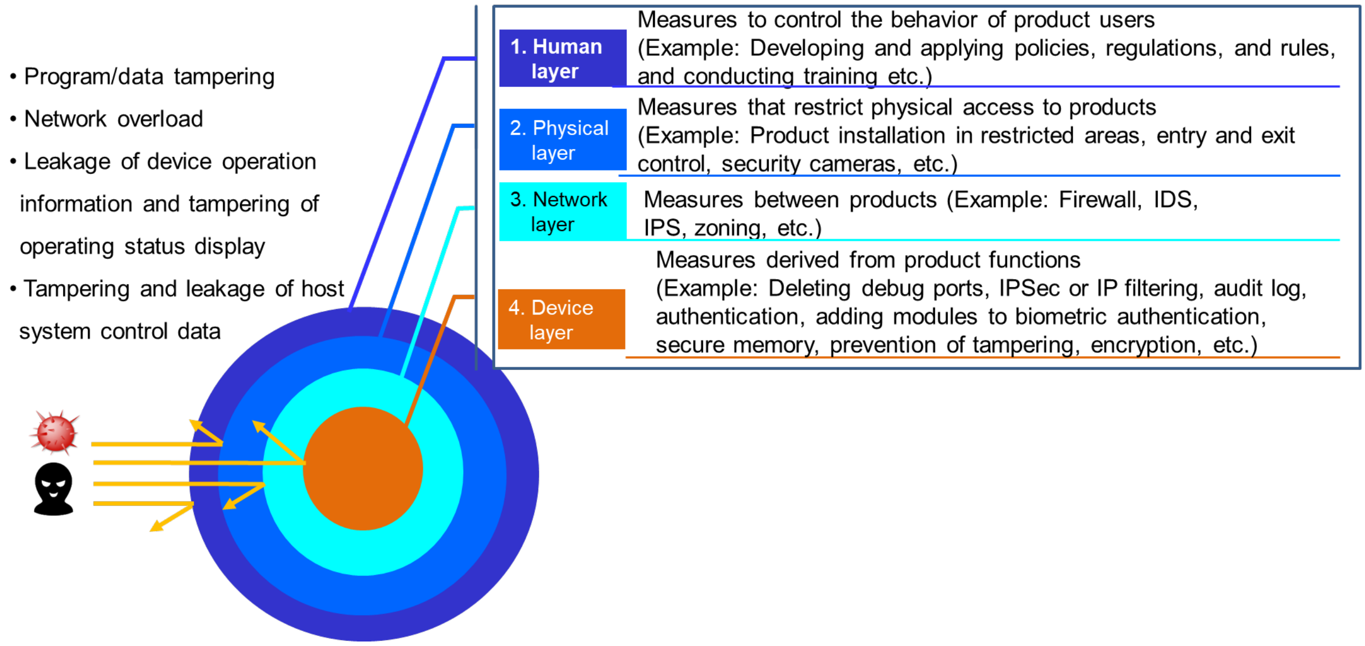

• Program/data tampering
• Network overload
• Leakage of device operation information and tampering of operating status display
• Tampering and leakage of host system control data
1. Human layer
Measures to control the behavior of product users (Example: Developing and applying policies, regulations, and rules, and conducting training etc.)
2. Physical layer
Measures that restrict physical access to products (Example: Product installation in restricted areas, entry and exit control, security cameras, etc.)
3. Network layer
Measures between products (Example: Firewall, IDS, IPS, zoning, etc.)
4. Device layer
Measures derived from product functions (Example: Deleting debug ports, IPSec or IP filtering, audit log, authentication, adding modules to biometric authentication, secure memory, prevention of tampering, encryption, etc.)

Figure 10 Defense-in-depth security measures

To realize a defense-in-depth concept, take appropriate security measures at each layer, i.e. "human layer", "physical layer", "network layer", and "device layer". Table 9 and Figure 11 show the threats derived from the security risk assessment for the example FA system, and examples of the employed security measures based on defense-in-depth.

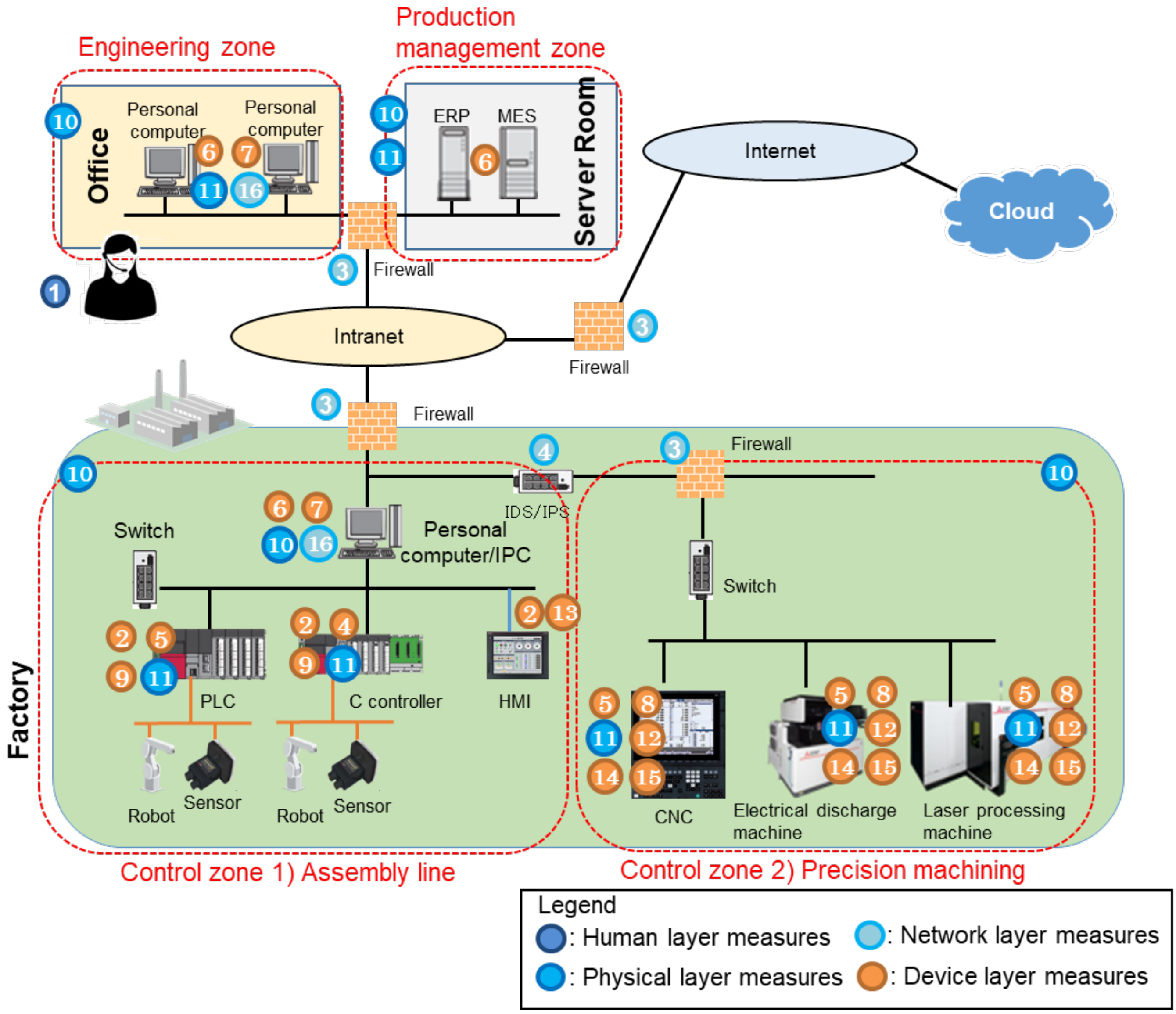


Figure 11 Threats to the example FA system and examples of countermeasures

Table 9 List of threats and measure examples

Threat	Point of countermeasure	Defense-in-depth layer		Countermeasure against threat
Common to all threats	Customer's environment	Human layer	1	Educate managers and users to prevent incorrect usage or failure to implement security measures.
Overload on the network (DoS attack)	Our FA product	Device layer	2	Setting IP filter functions interrupts communication from unauthorized IP addresses.
	Customer's environment	Network layer	3	Use firewalls to separate the factory network, intranet and internet from each other to restrict malicious traffic.
			4	Implement IDS (Intrusion Detection System) and IPS (Intrusion Prevention System), etc. to detect intrusions on networks
Unauthorized execution through attacks on unused services related to FA products	Our FA product	Device layer	2	Restrict FA products network access with IP filters and password authentication.
			5	Disable and prevent use of unused services to the FA product.

Threat	Point of countermeasure	Defense-in-depth layer		Countermeasure against threat
	Customer's environment	Network layer	3	Restrict network access by installing firewalls at “entry points” to the factory network.
		Device layer	6	Install antivirus software and restrict access by login and user authentication on development PCs to prevent program tampering.
			7	Encrypt programs and data on development PCs to prevent tampering with programs.
Fraudulent execution by falsifying programs and data related to FA products	Our FA product	Device layer	2	Apply IP filters and password authentication to FA products to restrict unauthorized network access.
			8	Implement an application whitelist for the FA product to restrict which applications can be installed, preventing tampering with the FA products program or data.
			9	Utilize password authentication to restrict access to programs and data of the FA product.
	Customer's environment	Physical layer	10	Apply access control to areas/zones (such as the ID or biometric authentication etc.) to prevent unauthorized access by intruders.
			11	Physically seal unused Ethernet and USB ports on FA products or development PCs to prevent unauthorized access and tampering by intruders.
		Network layer	3	Restrict network access by installing a firewall at the entry points to the factory network.
		Device layer	6	Install antivirus software and restrict access by login and user authentication on development PCs to prevent program tampering.
			7	Encrypt programs and data on development PCs to prevent tampering with programs.
Leakage/tampering of data as a result of intrusion from the Internet	Our FA product	Device layer	2	Apply IP filters to the FA product to restrict unauthorized network access.
			12	Restrict VPN connection from outside to the FA product by applying user permission to prevent permanent connection or unauthorized access from the internet
			9	Apply password authentication to FA products to prevent unauthorized access to the device programs and data.
	Customer's environment	Network layer	3	Apply a firewall at the network “entry point” of each zone to prevent unauthorized access.
			4	Utilize IDS (Intrusion Detection System) and IPS (Intrusion Prevention System), etc. to detect any unauthorized intrusions on networks
		Device layer	6	*Install antivirus software and restrict access by login and user authentication*

Threat	Point of countermeasure	Defense-in-depth layer	Countermeasure against threat	
				on development PCs to prevent program tampering.
			7	*Prevents program falsification by Encrypt programs and data on development PCs to prevent program tampering.*
Leakage of operational information/falsification of the operating status of devices	Our FA product	Device layer	2	*Apply IP filters to FA products to prevent unauthorized network access.*
			13	Utilize user authentication while operating FA products to prevent the interception or falsification of operational information.
	Customer's environment	Physical layer	11	Seal unused Ethernet and USB ports on FA products to prevent access and information theft by intruders.
		Network layer	3	Install a firewall at the entry points to the factory network to limit unauthorized network access.
Data leakage and falsification by means of improperly installed software on servers and personal computers	Customer's environment	Device layer	6	Utilize an application white-list on servers, personal computers, and IPCs to prevent unauthorized software installation, data leakage and tampering with data.
			7	Encrypt data and protect databases on servers, personal computers, and IPCs to prevent data leakage or data tampering.
Tampering and leakage of management data from servers and PCs	Customer's environment	Physical layer	11	Ensure that servers are located in a server room secured by physical user access controls and seal the servers unused Ethernet and USB ports as measures to prevent unauthorized access.
		Network layer	3	Install a firewall to separate the Internet and intranet and limit unauthorized network access to servers.
		Device layer	6	Install antivirus software on the MES/ERP server and apply user authentication to limit unauthorized access to the server and its data.
Leakage of production know-how from FA products	Our FA product	Device layer	14	Restrict external communications by license authentication to prevent data leakage due to unnecessary external communication.
			9	Apply data protection measures to prevent unauthorized reading of data from FA products and program execution by unauthorized devices.
Leakage of production data due to communication interception across the intranet	Our FA product	Device layer	15	Utilize mutual authentication using certificates to prevent data leakage or falsification.
	Customer's environment	Network layer	16	Protect communication between hubs by using VPN technology to prevent data leakage.
Physical intrusion into the zone	Customer's environment	Physical layer	10	Apply access control (such as the ID authentication and biometric authentication) for entry in to factory zones to prevent unauthorized access to programs and tampering with data.

Threat	Point of countermeasure	Defense-in-depth layer		Countermeasure against threat
Intrusion from the Internet	Customer's environment	Network layer	3	Install a firewall that separates the intranet from the Internet to prevent intrusion from the Internet
			4	Utilize IDS (Intrusion Detection System) and IPS (Intrusion Prevention System), etc. to detect intrusion on the network

Please refer to the "FA System Security Guideline Supplement" for the security functions of our FA products and product-specific security measures. In addition to the functions of our products, it is necessary to construct an FA system that combines our partner devices and other equipment in order to realize a multi-layered, defense-in-depth strategy.

3.2.2. Implementation of continuous security risk assessments

Security risk assessments and the consideration of measures based on assessment results are required to be performed continuously. As time passes, new risks may emerge with regard to the FA system. Performing regular security risk assessments can mitigate risks by continuously considering and implementing security measures against new risks and any remaining risks from the last assessment.
It is recommended that a security risk assessment be reperformed when:

- When an elapsed period of time has passed
  Results of the security risk assessment should be reviewed periodically. When reviewing, consider the changes in the FA system configuration and any potential new threats as described below.
- Changes in the FA system configuration, the nature of its operation (tasks), or the information it handles
  When there is a major change in the FA system configuration, its operational tasks, or the information handled in the performance of those tasks, especially if they were previously targets of the security risk assessment, it is recommended that a new security risk assessment is conducted.
- Emergence of new threats and countermeasures
  When a new threat or countermeasure is identified, which did not exist at the time of previous security risk assessment, it is recommended that the security risk assessment is repeated again.

3.2.3. Secure operation, maintenance, and disposal of the FA product

We will provide security information and firmware updates related to the operation, maintenance, and disposal of the FA products supporting our customers with their own operation, maintenance and disposal activities related to the FA products. Such security related recommendations can be found in this guideline, as well as information provided in individual product manuals and supplementary documents as necessary.
We recommend the following measures to customers who have installed our FA products;

(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 of a problem or when recovering the system from an error. For example, using the event (error) history function to collect and save details about any errors and abnormalities that occurred in our FA products or networks, can be a valuable aid to identifying the cause of the problem whether it is a systematic error or the result of some unauthorized activity

For customers using FA products, it is recommended to periodically check the latest firmware version and to perform firmware updates when necessary, with the firmware update function. The use of the latest firmware can eliminate vulnerabilities and enhance security functionality, resulting in the reduction of security risks. However, as firmware updates may change the behavior/operation of our FA products, 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.

If you have an FA product without the update function, or if you have any questions, please contact us, details how can be found in Appendix C.

(2) Disposal

For customers using FA products, it is recommended to delete all data and take appropriate disposal measures such as physically or electrically destroying the FA product so that any residual data cannot be recovered from the product after disposal. If such precautions are not taken at the time of disposal, it may be possible for third parties to exploit this and extract programs, recipe information, operational data and others useful information such as network setting etc. which may aid nefarious entities to create future attacks on the customers systems.

Appendix A: Development lifecycle of FA products

As shown in Figure 12, our company implements security measures throughout the whole development lifecycle.

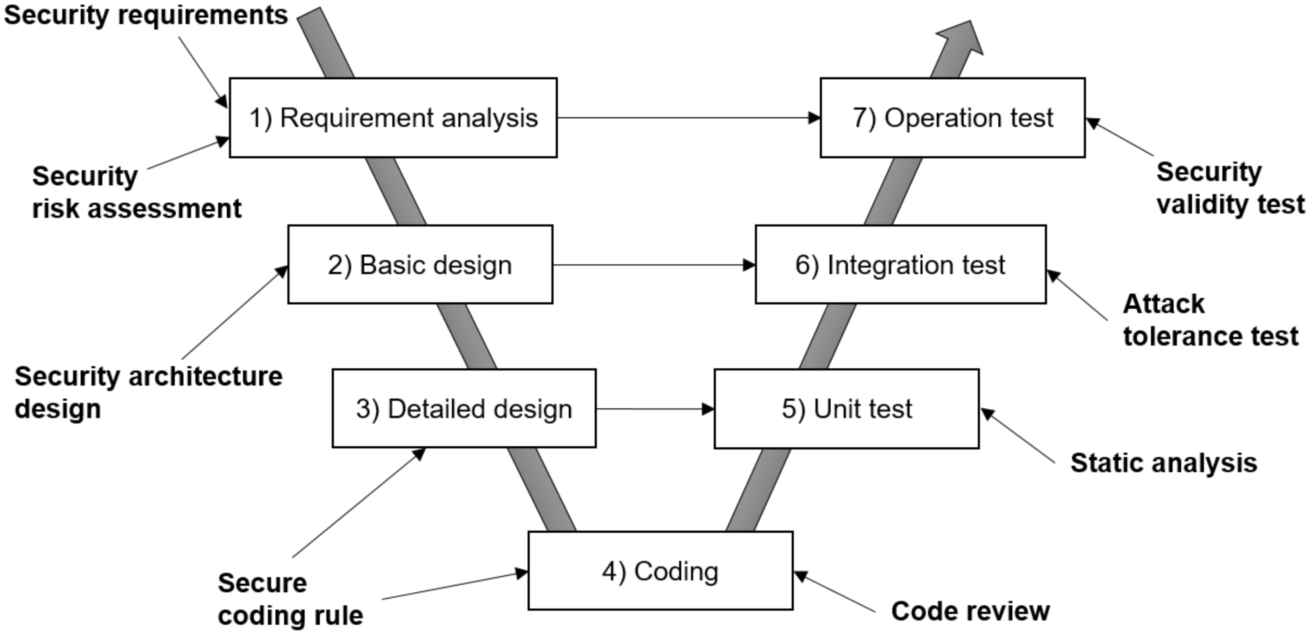


Figure 12 Security measures in the development lifecycle

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[25] 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.

[25] 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: 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.

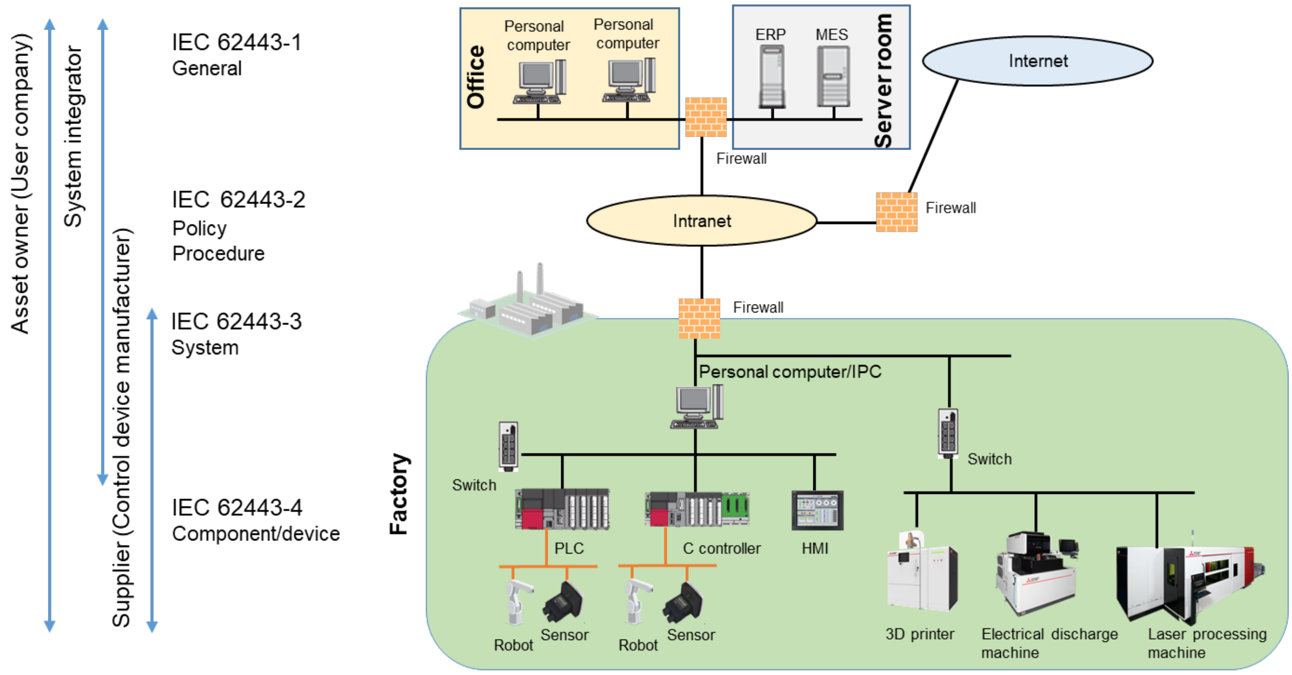


Figure 13 IEC 62443 compliance

[26] Industrial Automation and Control System

Appendix C: Inquiries about this document

For questions and inquiries on this document, contact your local sales office listed in Table 10. For the customers overseas, contact your local sales office listed in Table 11.

Table 10 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 11 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

Country /Region	Sales office/Address	Tel	Fax
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