

Security Guideline for Factory Automation System

Introduction

Background and Objectives

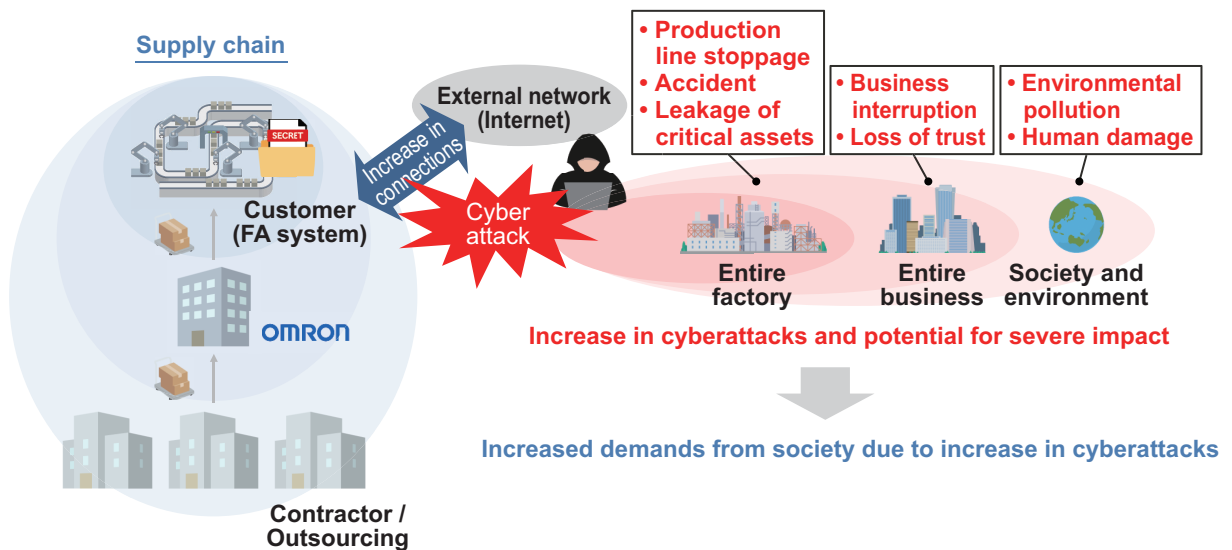
In recent years, manufacturers have been promoting initiatives to utilize IT/IoT technologies and data in their manufacturing sites with the aim of improving productivity and quality. With the increase in the number of connections to the outside world including the Internet, complexity of the supply chain, and ever increasing importance of product safety and quality and data in factory automation (hereinafter referred to as *FA*) devices, there has been an increase in the number of attacks targeting FA systems themselves, or using organizations and FA systems with inadequate security measures in the supply chain as a springboard.

Accordingly, countries are enacting cybersecurity-related laws and regulations, which cover FA system manufacturers and operators, FA systems and FA system components, whereas industries such as control system industry*¹, semiconductor industry*², and automotive industry*³ are standardizing their security requirements. Thus, social demands for cybersecurity are increasingly growing.

*1. IEC 62443 series

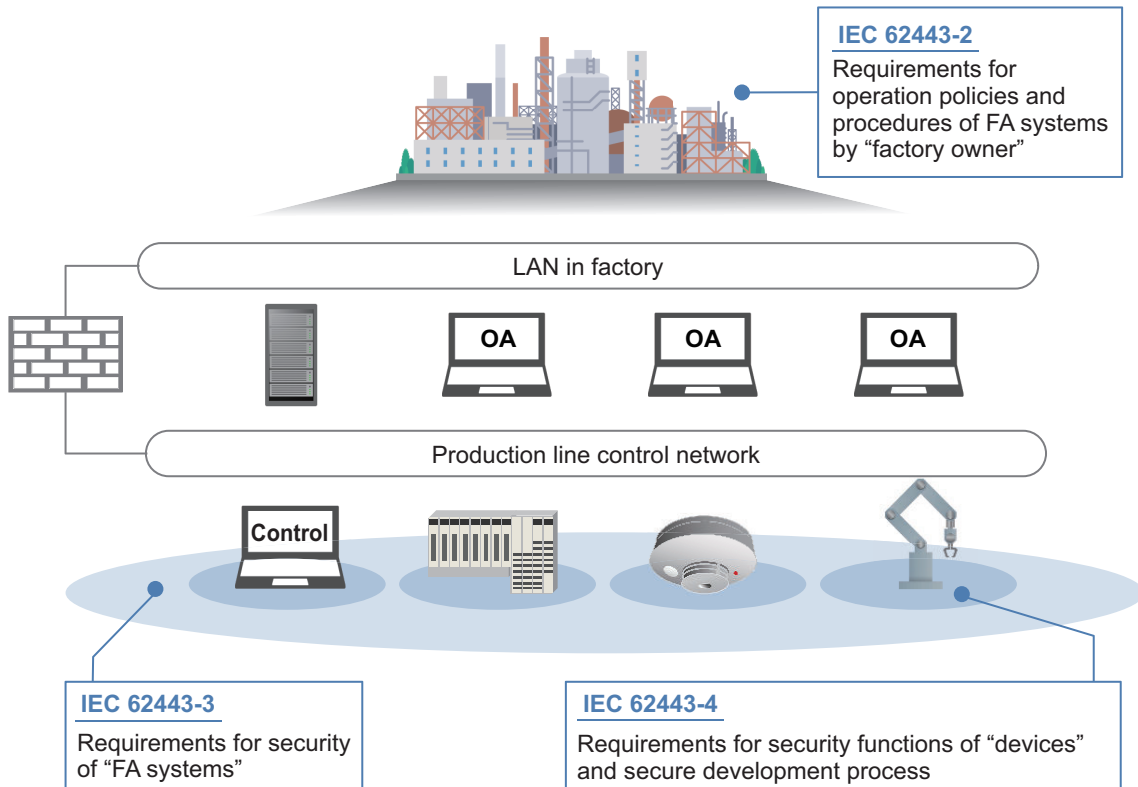
*2. SEMI E169 Guide for Equipment Information System Security (EISS), E187 Specification for Cybersecurity of Fab Equipment, E188 Specification for Malware Free Equipment Integration, etc.

*3. UN-R155: Cyber security and cyber security management system (CSMS), ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering, etc.



In particular, the manufacturing industry is utilizing and acquiring certification for the IEC 62443 series, which was formulated as international standards for cybersecurity of control systems, and many companies and industry organizations are referring to the standards. IEC 62443 defines a wide range of requirements for security of control systems, from requirements for security management that companies should address to requirements for security functions that systems should have.

IEC 62443-2 defines factory operation policies and procedures for factory owners. In addition, IEC 62443-3 defines security requirements that control system integrators should apply when they build production facilities. Furthermore, IEC 62443-4 defines requirements for security functions and secure development process for control components suppliers.



With this background, OMRON Corporation recognizes the importance of protecting people, equipment, and products in your factories from cyberattacks and contributing to stable operation in production and asset protection in your factories, as well as safe and secure utilization of data at your manufacturing sites.

The purpose of this document is to provide you with an understanding of security initiatives of OMRON on its FA products and propose the security measures that the users of the FA products should take on their own.

Intended Audience

This document is intended to be used when you implement security measures in the following organizations.

Organization	Definition
Factory owner	The owner of the entire factory including FA systems
System integrator	An organization in charge of introducing FA systems
Equipment vendor	A manufacturer that develops, produces, and maintains control equipment used in FA systems

Disclaimer

The recommendations we make to our customers in this document are based on the results of our analysis and study. Appropriate security measures vary with customer environment, so these recommendations do not guarantee prevention of all security breaches in customer environments. Referring to this document, please consider and implement analysis and appropriate countermeasures in line with the customer's environment on your own.

CONTENTS

Introduction	1
Background and Objectives	1
Intended Audience	2
Disclaimer	2
Revision History.....	5

Section 1 Product Security Initiatives at OMRON

1-1 Basic Policies on Product Security.....	1-2
1-2 Building an Organizational Structure for Product Security.....	1-3
1-2-1 Organization Strengthened for Promoting Company-wide and Product Security Activities	1-3
1-2-2 Strengthening Governance and Organization.....	1-3
1-3 Providing Products and Services That Take Security into Consideration	1-5
1-3-1 Implementation of FA Product Secure Lifecycle	1-5
1-3-2 Recommendation for Defense in Depth	1-6
1-3-3 Securing the Supply Chain.....	1-6
1-3-4 Compliance with Laws and Standards	1-6
1-4 Responses to Vulnerabilities and Incidents.....	1-8
1-4-1 Establishment of Contact Point (PSIRT) for Vulnerabilities and Incidents	1-8
1-4-2 Responses to Vulnerabilities and Incidents.....	1-8
1-5 Providing Security Information on Products and Services	1-9
1-5-1 Provision of Vulnerability Information and Security Advisories	1-9
1-5-2 Disclosure of Cyber Security and Product Security Policies	1-9
1-5-3 Cooperation with Security Agencies (Coordination Organizations)	1-9

Section 2 Necessity and Purpose of Security Response

2-1 Necessity of Security Response	2-2
2-2 Purposes of Security Response.....	2-3
2-2-1 Elements to Protect.....	2-3
2-2-2 Procedure of Risk Assessment	2-4

Section 3 Implementation of Risk Assessment

3-1 Clarification of Risk Targets	3-2
3-1-1 Determining Analysis Targets.....	3-2
3-1-2 Identifying Use Cases	3-3
3-1-3 Determining the Importance Level of a Security Zone	3-3
3-2 Risk Assessment	3-5
3-2-1 Identifying Assets	3-5
3-2-2 Identifying Threats.....	3-6
3-2-3 Assessing Risks	3-7
3-3 Concept of Risk Countermeasures	3-9
3-3-1 Determining Risk Countermeasures	3-9
3-3-2 Measures to Be Taken throughout the Lifecycle	3-9
3-3-3 Secure by Design.....	3-10
3-3-4 Defense in Depth	3-10

Appendices

- A-1 Related Materials A-2
- A-2 Contact Information for This Guide and Factory Automation Products of OMRON A-3

Revision History

A manual revision code appears as a suffix to the catalog number on the front and back covers of the manual.

Cat. No. P162-E1-01

↑
Revision code

Revision code	Date	Revised content
01	August 2023	Original production

1

Product Security Initiatives at OMRON

To develop and provide safe and secure products, OMRON strives to build an organizational structure to promote product security and is committed to secure implementation of products throughout the product lifecycle.

1-1	Basic Policies on Product Security	1-2
1-2	Building an Organizational Structure for Product Security	1-3
1-2-1	Organization Strengthened for Promoting Company-wide and Product Security Activities	1-3
1-2-2	Strengthening Governance and Organization	1-3
1-3	Providing Products and Services That Take Security into Consideration	1-5
1-3-1	Implementation of FA Product Secure Lifecycle.....	1-5
1-3-2	Recommendation for Defense in Depth	1-6
1-3-3	Securing the Supply Chain.....	1-6
1-3-4	Compliance with Laws and Standards	1-6
1-4	Responses to Vulnerabilities and Incidents	1-8
1-4-1	Establishment of Contact Point (PSIRT) for Vulnerabilities and Incidents	1-8
1-4-2	Responses to Vulnerabilities and Incidents.....	1-8
1-5	Providing Security Information on Products and Services	1-9
1-5-1	Provision of Vulnerability Information and Security Advisories.....	1-9
1-5-2	Disclosure of Cyber Security and Product Security Policies	1-9
1-5-3	Cooperation with Security Agencies (Coordination Organizations).....	1-9

1-1 Basic Policies on Product Security

OMRON is working on the following product security activities in order to provide products and services that implement security measures against cyberattacks.

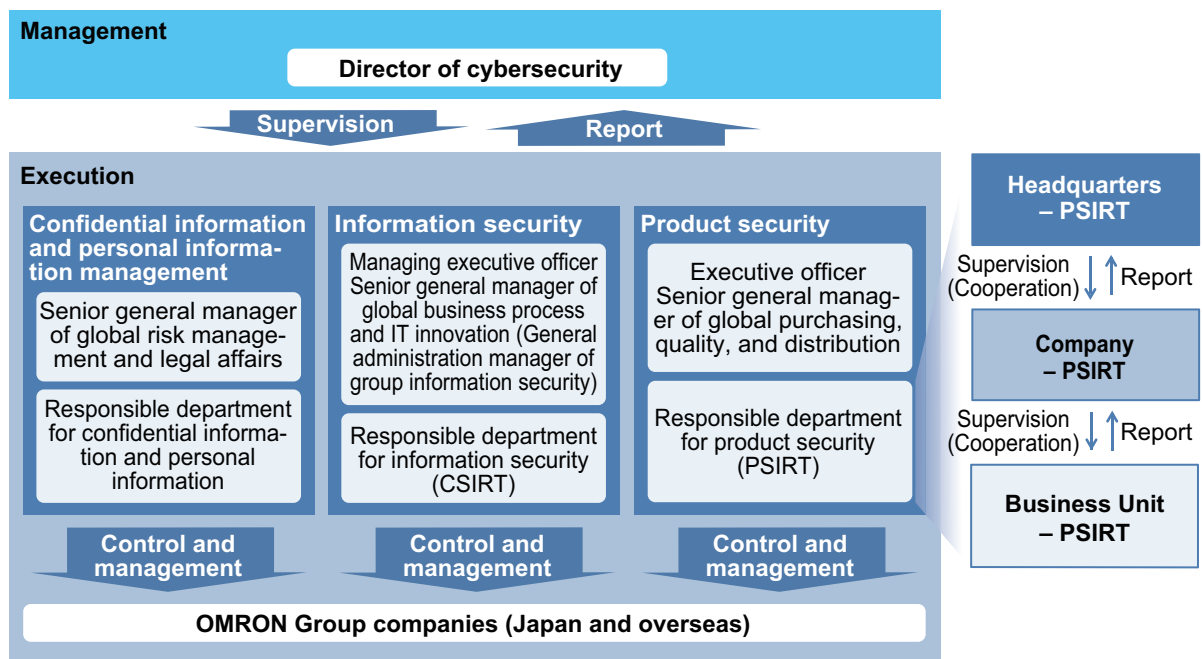
<i>1-2 Building an Organizational Structure for Product Security</i> on page 1-3	OMRON has established a cooperative system involving the head office and business divisions to promote product security activities, and is working to strengthen the organization through vulnerability management of products and services, strengthening internal governance, and educating employees.
<i>1-3 Providing Products and Services That Take Security into Consideration</i> on page 1-5	OMRON is working on security activities to take security measures against cyberattacks throughout the product lifecycle, including planning, development, operation/maintenance, and disposal.
<i>1-4 Responses to Vulnerabilities and Incidents</i> on page 1-8	OMRON widely collects information on vulnerabilities of its products and services, and take timely countermeasures against discovered vulnerabilities. If an incident occurs, OMRON promptly establishes a response system, conducts necessary reporting internally and externally, discloses information, investigates the cause, and prevents recurrence.
<i>1-5 Providing Security Information on Products and Services</i> on page 1-9	OMRON establishes evaluation criteria and response procedures for vulnerability information provided by external organizations and customers, or obtained from self-diagnosis results, cooperates with related organizations, and provides vulnerability information to customers in a timely manner.

Each of these initiatives is introduced in the following sections.

1-2 Building an Organizational Structure for Product Security

1-2-1 Organization Strengthened for Promoting Company-wide and Product Security Activities

OMRON has positioned strengthening cybersecurity as a company-wide priority initiative, and has built a driving organization for each area of *confidential information and personal information management*, *information security*, and *product security*, and is promoting actions to solve cybersecurity issues and initiatives for future enhancements.



In order to promote and manage initiatives related to *product security*, OMRON has an organization called PSIRT*¹, which manages product security across its businesses and divisions. PSIRTs are located at levels from the headquarters to business units, and collaborate closely with each other to ensure product security for the entire OMRON Group.

*1. PSIRT (Product Security Incident Response Team)

1-2-2 Strengthening Governance and Organization

OMRON is strengthening its internal governance and organization through employee training in order to enhance the security of FA products and services provided to its customers.

Initiatives for Governance

- OMRON has formulated the *OMRON Group Guidelines for Product Security*, which stipulates security-related guidelines that employees should follow, and keeps employees informed of it.
- Based on these guidelines, OMRON is working on continuous improvement of security-related initiatives.

Initiatives for Strengthening Organization

- OMRON has formulated a skill map for the security operations it performs in the development and provision of FA products and strives to manage the competence of its employees based on it, including training, encouraging employees to obtain external security certifications, and establishing an internal certification system.
- OMRON promotes periodic security education on the latest security trends to the managers of departments related to security operations.

1-3 Providing Products and Services That Take Security into Consideration

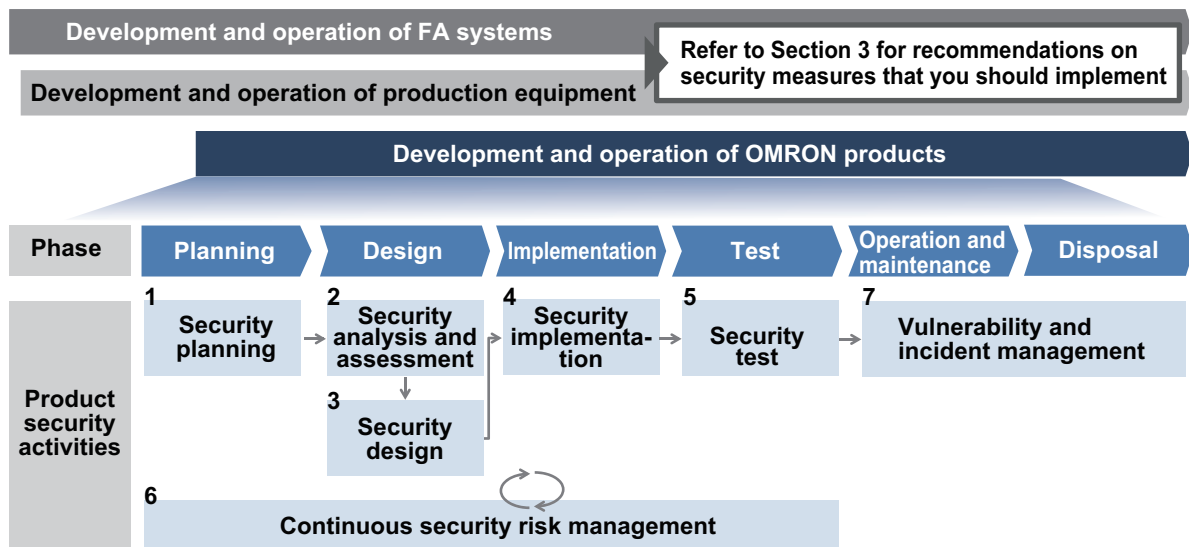
1-3-1 Implementation of FA Product Secure Lifecycle

OMRON develops FA products with security risks in mind from the product planning and design phases, based on the concept of Secure by Design^{*1} to ensure that its customers can securely and safely use the products. To achieve this, OMRON believes that, in addition to product security activities in each phase of development, it is important to check and manage the response status to security risks, regardless of the phase.

Furthermore, even after its FA products are in the hands of customers, OMRON continues to carry out activities to respond to security risks throughout the product lifecycle until its FA products are safely operated, maintained, and discarded by the customer.

*1. Secure by Design is the idea of developing a secure system by considering security of the system from an early stage in the development process. It helps to prevent vulnerabilities and incidents.

The following is an overview of FA product lifecycle activities of OMRON with consideration for security.



1. Security planning:
Define the functions and information assets in the FA product to be developed and the assumptions for security risk response, such as the operating environment, and plan the subsequent FA product security activities.
2. Security analysis and assessment:
Analyze and assess the security risks of the FA product to be developed based on the premises defined in security planning, and determine response policies and priorities.
3. Security design:
Based on the response policies and priorities determined in security analysis and assessment, define security requirements for the FA products to develop and implement a technical design to achieve them.
4. Security implementation:

Apply secure coding to prevent the introduction of vulnerabilities that are difficult to prevent by security design alone, thereby making the responses to security risks stronger.

5. Security test:

Confirm that the responses to security risks in the FA product are complete and reasonable.

6. Continuous security risk management

Provide key points for checking security risks during development of the FA product to ensure that security risks are properly identified, analyzed, and responded to.

7. Vulnerability and incident management:

Detect vulnerabilities and incidents through active information gathering or internal and external reports and manage the situations continuously until completion of the responses.

1-3-2 Recommendation for Defense in Depth

To ensure the security of FA systems at the customers' site, OMRON recommends a security response approach based on the concept of Defense in Depth, which hierarchically combines multiple measures, such as establishing operational policies and procedures, preventing physical penetration into factories, and implementing technical measures for networks and equipment, in order to strengthen security.

Refer to 3-3-4 *Defense in Depth* on page 3-10 for information on the concept of Defense in Depth.

1-3-3 Securing the Supply Chain

OMRON considers vulnerabilities in its supply chain to be a significant security risk and defines outsourcing contractors and suppliers for operations involved in the development and provision of its FA products also as targets of security management.

OMRON implements the following as initiatives for supply chain security management.

Secure Outsourcing and Procurement Processes

In outsourcing and procurement, OMRON assesses and manages contractors and suppliers using appropriate processes, including selection, contracting, and auditing with security in mind.

Security Inspection of Externally Procured Items

To ensure the security quality of externally procured items, OMRON works with contractors and suppliers to manage the security quality of items purchased from the supply chain by asking them to provide configuration management information needed for delivery inspection and post-delivery vulnerability management.

1-3-4 Compliance with Laws and Standards

OMRON is committed to developing and providing safe and secure FA products by complying with domestic and international laws and regulations governing product security and establishing internal security processes to comply with international standards related to control system security.

As an objective evidence that OMRON actually implemented a development lifecycle with security risks in mind, some FA products of OMRON have obtained certification of the international standard IEC 62443-4-1*¹ and the Chinese national standard GB40050*².

OMRON also continues to track the latest domestic and overseas security laws and standards, and makes every effort to make preparations in a timely manner.

*1. IEC 62443-4-1:2018 (Edition 1.0):

Secure product development lifecycle requirements

*2. GB 40050-2021: General security requirements for critical network components

1-4 Responses to Vulnerabilities and Incidents

1-4-1 Establishment of Contact Point (PSIRT) for Vulnerabilities and Incidents

To enable its customers and security researchers who discovered any vulnerability in OMRON products to promptly report it to OMRON, OMRON has established the Product Security Incident Response Team. This allows OMRON to take countermeasures promptly in collaboration with the relevant business units and government organizations.

URL (Japanese): <https://www.omron.co.jp/contact/ContactForm.do?FID=00280>

URL (English): <https://www.omron.com/contact/ContactForm.do?FID=00282>

1-4-2 Responses to Vulnerabilities and Incidents

OMRON widely collects information on vulnerabilities of its products and services, and takes timely countermeasures against discovered vulnerabilities.

If an incident due to a cyberattack occurs in the products or services, OMRON promptly establishes a response system, conducts necessary reporting internally and externally, discloses information, investigates the cause, and prevents recurrence.

1-5 Providing Security Information on Products and Services

1-5-1 Provision of Vulnerability Information and Security Advisories

OMRON discloses vulnerability information related to OMRON products and, for critical vulnerabilities in particular, security advisories that summarize the contents of vulnerabilities, target products, potential impacts, and countermeasure on its website.

Information on vulnerabilities in OMRON products

URL (Japanese): https://www.omron.com/jp/ja/inquiry/vulnerability_information/

URL (English): https://www.omron.com/global/en/inquiry/vulnerability_information/

Information on vulnerabilities in OMRON FA products

URL (Japanese): <https://www.fa.omron.co.jp/product/vulnerability/index.html>

URL (English): <https://www.ia.omron.com/product/vulnerability/index.html>

1-5-2 Disclosure of Cyber Security and Product Security Policies

OMRON regards our cyber security initiatives as one of our company-wide risk management activities, and discloses the details of these activities and our promotion system below.

URL (Japanese): <https://sustainability.omron.com/jp/compliance/>

URL (English): <https://sustainability.omron.com/en/compliance/>

To ensure that you can use OMRON products securely, OMRON discloses its basic policies and activities for product security as the product security policy.

URL (Japanese): https://www.omron.com/jp/ja/inquiry/product_security/

URL (English): https://www.omron.com/global/en/inquiry/product_security/

1-5-3 Cooperation with Security Agencies (Coordination Organizations)

To ensure prompt information sharing and collaboration in vulnerability response when any vulnerability is discovered in OMRON's products, OMRON collaborates with domestic and international coordination organizations, including the following.

- CISA(Cybersecurity and Infrastructure Security Agency)*¹
URL:<https://www.cisa.gov/>

*1. U.S. Cybersecurity and Infrastructure Security Agency. An administrative agency with functions such as promotion of cybersecurity measures in relevant governmental organizations and critical infrastructure in the United States and promotion of partnerships among industry, academia, and government.

2

Necessity and Purpose of Security Response

This section describes the necessity of security risk responses in FA systems and their purposes.

2-1	Necessity of Security Response.....	2-2
2-2	Purposes of Security Response	2-3
2-2-1	Elements to Protect	2-3
2-2-2	Procedure of Risk Assessment	2-4

2-1 Necessity of Security Response

To ensure the security and safety of your FA system, in addition to the measures taken by OMRON for its FA products, you should also take security measures according to your roles.

To this end, it is important for you to correctly understand and assess the security risks involved in operations, services, and systems that you provide, and implement appropriate security measures throughout the lifecycle of the FA system.

2-2 Purposes of Security Response

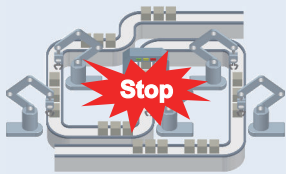


It is important to indicate the purpose of security measures, goals, and the necessity of business security measures with clear grounds, and to proceed with agreement with management. Without these consensus, priority is given to other business requirements and it becomes difficult to get alignment and cooperation across divisions. Possible security objectives include the following.

1. Continue business and production
2. Keep the factory safe and ensure product quality
3. Ensure normal operation of FA systems
4. Protect information, know-how, and data related to products and production
5. Ensure the security quality of products and fulfill responsibilities as a manufacturer
6. Meet social demands from standards and external requirements
7. Maintain company's brand image and prevent loss of customer trust

From these security objectives, identify threats that have a particularly high business impact, calculate the cost of countermeasures, and reach agreement on your goals.

2-2-1 Elements to Protect

It is easier to set goals if you clarify what will have a significant impact on your business in relation to the purpose of your security response. The objective of security measures is to ensure the three elements of security, which are *availability*, *integrity*, and *confidentiality* of operations, services, and products that your company provides.

	Ensuring Availability	Ensuring Integrity	Ensuring Confidentiality
Objective	Prevention of production equipment operation stop 	Prevention of production equipment failure due to unauthorized overwriting of settings and data 	Prevention of disclosure of important information such as production know-how and control programs 
Impact in case of compromise	<ul style="list-style-type: none"> • Business suspension • Delivery delays • Increased costs 	<ul style="list-style-type: none"> • Quality degradation • Reduced safety • Adverse impact on health • Adverse impact on environment 	<ul style="list-style-type: none"> • Damage to social trust • Loss of business advantage • Breach of laws and regulations

The severity of the impact given by *availability*, *integrity*, and *confidentiality* differs depending on the industry, services and products that you provide, and the assets to protect. For example, the security element that is important varies with the industry. In addition, even in the same industry, it varies depending on the business role and the process. It is important to carefully consider which element your company should focus on and promote security measures.

Industry	Element to emphasize and reason	
Automotive	Emphasis on availability	• Even short suspension of operation has significant impact on business and society.
Infrastructure	Emphasis on availability	• Even short suspension of operation has significant impact on society and the environment.
Food and medical	Emphasis on integrity	• Incorrect production has significant impact on users' health and safety.
Equipment vendor (impact given differs depending on the equipment)	Emphasis on availability	• Even short suspension of operation has significant impact on society and the environment.
	Emphasis on integrity	• Incorrect production has significant impact on users' health and safety.
	Emphasis on confidentiality	• Leakage of equipment know-how has significant impact on business.

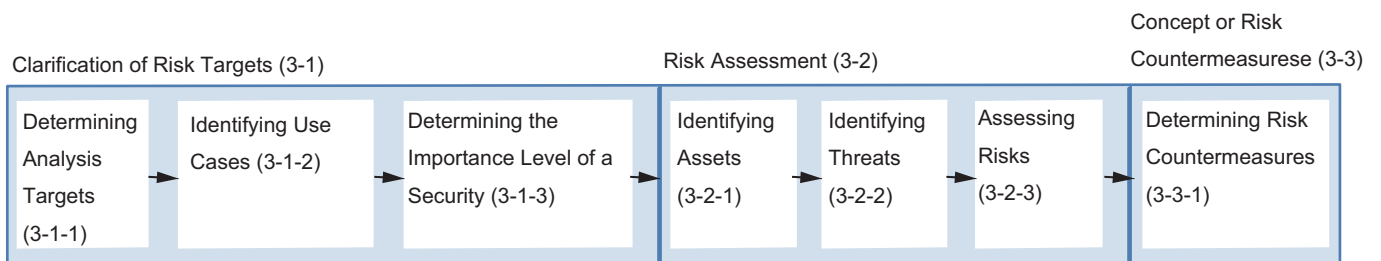
2-2-2 Procedure of Risk Assessment

In order to obtain consensus on security measures, it is important to conduct a risk assessment to clarify security-related risks. In the risk assessment, it is necessary for the customer to consider measures based on the company's environment, laws and regulations to comply with, and the latest trends in threats. By responding to threats preferentially from those with greater risks to your business, you can maximize the cost-effectiveness of your security measures.

Risk assessment is the first step that you should take for a proper security response. It is an activity to identify threats to the system to protect, or the business (including operations and services) in which the system is being used or operated, and assess the risks based on the magnitude of impact and likelihood of occurrence of damage caused by the threats.

The implementation of such risk assessment is required, for both factory owners and equipment vendors, in many security regulations and international standards, such as IEC 62443. On the other hand, since the methods of risk assessment vary widely, it is necessary to select or combine appropriate methods according to the actual circumstances of the organization (e.g., systems to handle, products, and organizational capabilities).

Conduct risk assessments in FA system according to the following procedure.



The specific implementation of each procedure is explained in the next section.

3

Implementation of Risk Assessment

This section explains in detail the implementation of risk assessment in an FA system.

3-1	Clarification of Risk Targets	3-2
3-1-1	Determining Analysis Targets	3-2
3-1-2	Identifying Use Cases	3-3
3-1-3	Determining the Importance Level of a Security Zone	3-3
3-2	Risk Assessment	3-5
3-2-1	Identifying Assets	3-5
3-2-2	Identifying Threats	3-6
3-2-3	Assessing Risks	3-7
3-3	Concept of Risk Countermeasures	3-9
3-3-1	Determining Risk Countermeasures	3-9
3-3-2	Measures to Be Taken throughout the Lifecycle	3-9
3-3-3	Secure by Design	3-10
3-3-4	Defense in Depth.....	3-10

3-1 Clarification of Risk Targets

Clarify risk targets in order to conduct a risk assessment.

3-1-1 Determining Analysis Targets

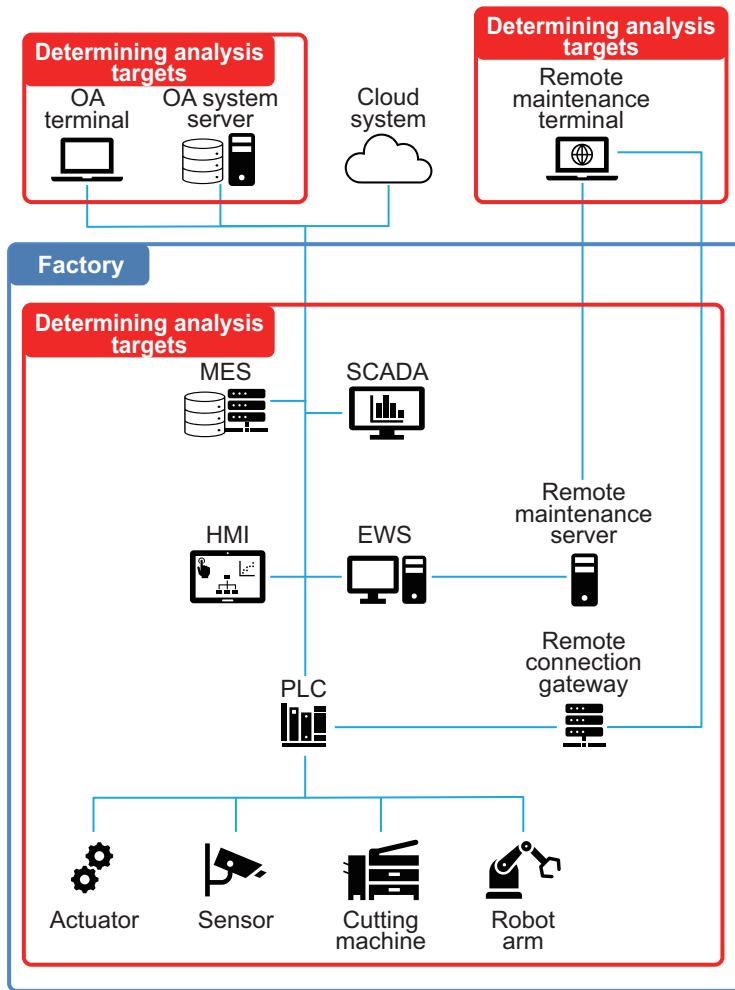
The first step that you should do in risk assessment process is to determine the target systems to assess. Basically, the scope should be all systems related to the business and services of the organization and the business sites in which the organization operates.

Perspectives that you should consider when defining analysis targets are as follows.

- Scope of organization and business site (e.g., factories)
- Scope of the systems (e.g., IT systems and production management systems)

Next, clarify the configuration of the analysis target systems determined. Make a list of networks, equipment, and roles that make up the system. By learning the system configuration, it is possible to derive the conditions (attack methods, paths, etc.) under which threats become apparent and comprehensive countermeasures for them. To clarify the system configuration, the following elements should be considered.

- FA system, placement of devices on the network, and roles of devices
- Network configuration
- Physical area zoning for each system
- Cyber security measures already in place



3-1-2 Identifying Use Cases

To grasp the security risks involved in an FA system and assess their severity level, it is necessary to identify the use cases of the FA system (i.e., activities performed by operating the FA system). By properly deriving use cases, it is possible to clarify operations and services of high importance to your company that are achieved by the FA system, and properly assess the risks in case they are compromised.

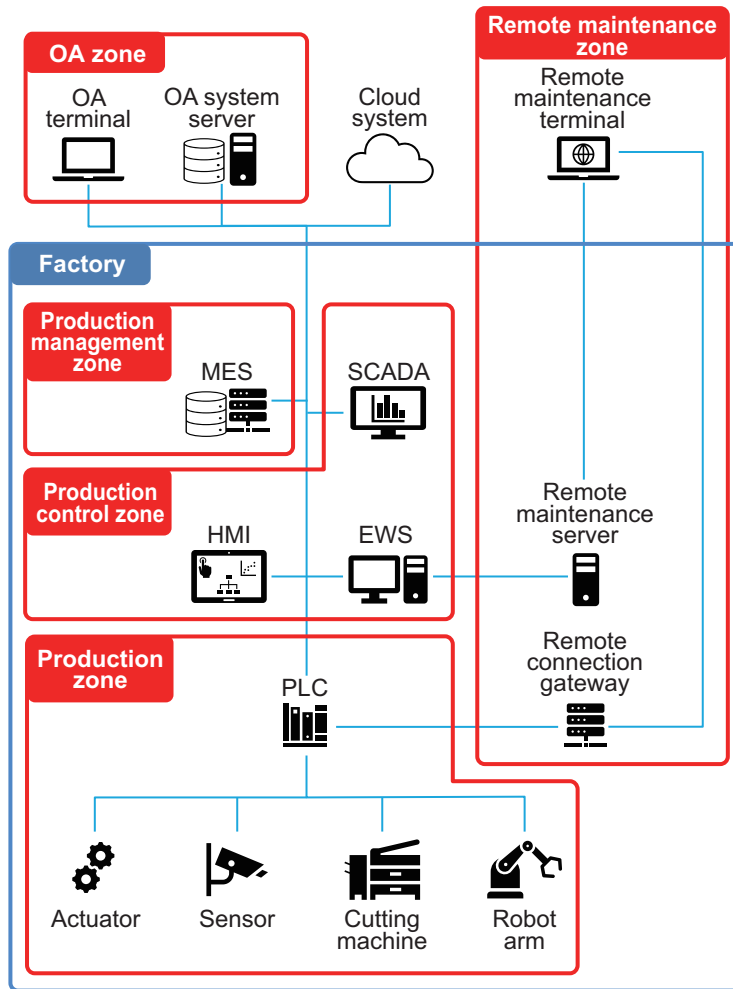
In deriving use cases, consider the following aspects.

Perspectives for derivation	Key points of derivation
Contents of operations and services	<ul style="list-style-type: none"> Objectives achieved by business and services (status and output) Specific work content
Persons performing operations and services	<ul style="list-style-type: none"> The person in the organization/subcontractor who performs the work Role of the above person
Systems and data related to operations and services	<ul style="list-style-type: none"> Devices and systems utilized to execute the operations Data handled by the above devices and systems

3-1-3 Determining the Importance Level of a Security Zone

Classify areas in the FA system into groups of those requiring an equivalent level of security measures based on the contents and importance level of operations. This is called the definition of security

zones. By defining security zones, it is possible to identify the areas where security measures should be preferentially implemented, which allows for efficient implementation of the security measures.



Determine the security level for each security zone. The “security level” refers to the target of security measures required to protect the operations performed and assets handled in the defined security zone. The security levels and assumed attacker profiles defined in IEC 62443 are shown in the table below.

Security level (SL)	Profile of assumed attacker	Definition
SL0	None	No specific requirements or security protection required
SL1	Employees	Protection from unintentional or accidental breaches
SL2	Script kiddies (Attackers who use commonly available attack tools)	Protection against intentional attacks by simple means, with low resources, generic skills, and low motivation
SL3	Professional hackers Insiders and former employees	Protection against intentional attacks by sophisticated means, with moderate resources, skills specific to control systems, and moderate motivation
SL4	State-sponsored cyber-terrorists	Protection against intentional attacks by sophisticated means, with extended resources, skills specific to control systems, and high motivation

3-2 Risk Assessment

Identify threats to assets you want to protect and assess the risk of threats.

3-2-1 Identifying Assets

To properly select the security risks to consider and the measures to implement in a risk assessment, define the *assets to protect* for your company.

Assets to protect refers to devices and data of which a loss of the three elements of security (i.e., availability, integrity, and confidentiality) caused by cyberattacks could lead to damage to the business of your company or your customers. Therefore, you should determine yourself what are valuable assets.

Listing Assets

Identify the physical assets, information assets, and functional assets that exist in the defined system configuration and list them as assets held by the system. When deriving assets, you can analyze them from several perspectives (asset classification). In addition, to streamline the analysis, you can use this classification to reduce the number of assets to analyze by integrating assets with equal technical characteristics and importance level, if necessary.

Examples of asset types are as follows.

- Physical assets: Controllers, servers, PCs, etc.
- Information assets: User programs, recipe data, log information, etc.
- Functional assets: Control functions, safety functions, etc.

Assessing the Importance Level of Assets

Assess the importance level of asset on the economy from several perspectives, such as economic loss, impact on safety, and suspension of system operation. For example, if an attack causes only a small amount of monetary damages, it can be assessed as small impact, whereas if the attack causes a long-term suspension of factory operations, it can be assessed as large impact.

For the assessment criteria, it is important to take into account several perspectives, for example, impact on the continuation of production activities, economic losses, and impact on the Health, Safety, and Environment of the factory. You should decide which perspective to adopt based on your company's situation.

The table below shows an example of assessing the importance level from several security perspectives.

Assessment value	Assessment criteria
3	<ul style="list-style-type: none"> • If the asset is attacked, there is a risk of system shutdown for one week or more. • If information is leaked from the asset, there is a risk of loss of 500 million yen or more. • If the asset is attacked, there is a risk of death of employees.

Assessment value	Assessment criteria
2	<ul style="list-style-type: none"> • If the asset is attacked, there is a risk of system shutdown for 24 hours or more but less than one week. • If information is leaked from the asset, there is a risk of loss of 5 million yen or more but less than 500 million yen. • If the asset is attacked, there is a risk of serious injury to employees.
1	<ul style="list-style-type: none"> • Even if an asset is attacked, there is no risk of system shutdown for 24 hours or more. • If information is leaked from the asset, there is no risk of loss of 5 million yen or more. • If the asset is attacked, there is no risk of serious injury to employees.

3-2-2 Identifying Threats

It is necessary to identify threat that may compromise the asset and threat combined with the cyberattack methods that can realize it. Identify the threats comprehensively, because it is an important activity to appropriately set security countermeasure targets.

Listing Threats

Identify threats to the assets to be protected, and the impact on production and business when those threats occur. Examples are shown in the table below.

Asset	Threat	Impact on production and business
Controller	Theft of the Controller	<ul style="list-style-type: none"> • Product delivery delays due to production stoppages • Damage caused by equipment destruction
User program	Tampering with user programs by connecting a computer brought in from the outside	<ul style="list-style-type: none"> • Poor quality and resulting brand damage • Personal injury due to equipment malfunction
Production recipe data	Leakage of production recipe data	<ul style="list-style-type: none"> • Decrease in competitiveness
User settings	Tampering with access control settings	<ul style="list-style-type: none"> • Leakage of know-how due to illegal access
Control function	Control function stopped due to operation error	<ul style="list-style-type: none"> • Product delivery delays due to production stoppages
...

Various methods for analyzing threats and attack methods are defined by industries, standards, etc., and their characteristics are diverse. To ensure the quality of analysis, properly utilize recognized analysis methods and frameworks and understand the industry standard related to your organization and the scope of analysis.

Examples of analysis methods are shown in the table below.

Analysis method	Overview
STRIDE	A method of deriving threats from the following six guide words based on the attacker's purpose <ul style="list-style-type: none"> • Spoofing • Tampering • Repudiation • Information Disclosure • Denial of Service • Elevation of Privilege
Attack Tree Analysis	A method of decomposing and clarifying the configuration element of an attack method in a tree diagram

Assessing the Likelihood of Threat Occurrence

The likelihood of occurrence of a threat can be assessed based on indicators such as the difficulty in obtaining the knowledge and technology to achieve the attack, the time at which the attack can be carried out, and the time required to complete the attack. For example, if attack methods against vulnerabilities possessed by devices are widely known and attacks can be executed at any time, attacks are easy and there is a high possibility that a threat will occur.

The following are examples of threat likelihood metrics.

Likelihood of occurrence	Knowledge and technology (tools, etc.) required for attack	Required time and opportunity for attack
3	<ul style="list-style-type: none"> • No expertise is required. • Required technology is easy to obtain. 	<ul style="list-style-type: none"> • Required time is short. • Attacks can be carried out at any time.
2	<ul style="list-style-type: none"> • Some level of expertise is required. • Required technology is difficult to obtain to some extent. 	<ul style="list-style-type: none"> • Required time is of medium length. • Opportunities to attack are limited.
1	<ul style="list-style-type: none"> • Expertise is required. • Required technology is difficult to obtain. 	<ul style="list-style-type: none"> • Required time is long. • There are few opportunities to attack.

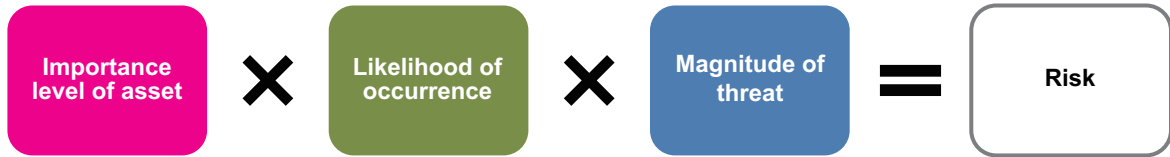
Assessing Magnitude of Threat

Assess the extent to which your system is affected if security (availability, integrity, and confidentiality) is compromised. An example of threat impact criteria is shown below.

Magnitude of threat	Assessment criteria
3	The threat impact affects the entire system.
2	The threat impact is limited in the system.
1	There is no impact from the threat.

3-2-3 Assessing Risks

Assess security risks to determine whether or not to implement security measures against the identified threat and their priority in response. Security risks can be assessed by multiplying the *importance level of asset*, *likelihood of occurrence* of a threat, and *magnitude of threat* when it occurs.



Calculate the comprehensive security risk assessment value with three elements, i.e., the importance level of asset, likelihood of threat occurrence, and magnitude of the threat. For example, if a vulnerability that could lead to a production suspension remains in a control device (PLC) (i.e., the threat is large) and the attack method for the vulnerability is widely known (i.e., likelihood of occurrence is high), the security risk can be assessed as high.

The table below shows the examples of evaluation criteria for determining risk assessment values.

Importance level of asset	Likelihood of occurrence	Magnitude of threat	Risk assessment value	Judgment conditions
3	3	3	A	Importance level of asset: 3 Threat × Likelihood of occurrence: 6 to 9
3	2	3		
3	3	2		
3	2	2	B	Importance level of asset: 3 Threat × Likelihood of occurrence: 3 to 5
3	1	3		
3	3	1		
2	3	3		
2	2	3		
2	3	2	C	Importance level of asset: 2 Threat × Likelihood of occurrence: 6 to 9
3	1	2		
3	2	1		
3	1	1		
2	2	2		
2	1	3		
2	3	1		
1	3	3	D	Importance level of asset: 1 Threat × Likelihood of occurrence: 7 to 9
2	1	2		
2	2	1		
2	1	1		
1	2	3		
1	3	2		
1	2	2	E	Importance level of asset: 1 Threat × Likelihood of occurrence: 4 to 6
1	1	3		
1	3	1		
1	1	2		
1	2	1		
1	1	1		Importance level of asset: 1 Threat × Likelihood of occurrence: 1 to 3

3-3 Concept of Risk Countermeasures

Consider specific security measures against threats. Note also that optimizing security measures on an individual basis could make them insufficient. Therefore, it is important to consider comprehensive measures, taking into account the four perspectives introduced in this sections: *risk countermeasures*, *measures to be taken throughout the lifecycle*, *secure by design*, and *defense in depth*.

3-3-1 Determining Risk Countermeasures

Determine if countermeasures against risks are needed.

Depending on the security level of the security zone, different measures are required. Zones with high security levels require countermeasures against threats with low risk assessment values. On the other hand, it can be determined that countermeasures should be taken only for those with high risk assessment values in zones with low security levels.

The table below provides an example of defining the security level and the scope of measures.

Security level (SL)	Scope of measures
SL0	Take countermeasures against risks of A.
SL1	Take countermeasures against risks A and B.
SL2	Take countermeasures against risks A, B, and C.
SL3	Take countermeasures against risks A, B, C, and D.
SL4	Take countermeasures against risks A, B, C, D, and E.

Divide the countermeasures against security risks into the following categories.

- Avoid: Measure to eliminate the root cause of a threat, such as the removal of a function that has a risk
- Mitigate: Measure to reduce the likelihood and impact of a risk, such as adding a security function
- Transfer: Measure to transfer the risk to another organization, such as outsourcing system operations
- Accept: Measure to accept the risk without taking specific measures

3-3-2 Measures to Be Taken throughout the Lifecycle

To strengthen the security of FA systems, it is necessary to address security throughout the lifecycle of the FA systems. The table below provides an overview of the lifecycle of an FA system and security measures that should be implemented in each phase.

Lifecycle of FA system	Main activities and role assignment
Design and startup	<ul style="list-style-type: none"> • Factory owner: Develop risk countermeasures on production lines and security rules • System integrator and equipment vendor: Implement risk countermeasures (security functions) in equipment, and provide a guide for using the equipment securely
Operation	<ul style="list-style-type: none"> • Factory owner: Monitor the status of the production line and compliance with security rules established in the design process • System integrator: Monitor vulnerability information of equipment and adopt security rules • Equipment vendor: Disclose vulnerability information of equipment

Lifecycle of FA system	Main activities and role assignment
Maintenance	<ul style="list-style-type: none"> • Factory owner: Verify the account information, check audit logs, and update equipment • System integrator: Update equipment • Equipment vendor: Provide account management recommendations and software (security patch) update procedure
Disposal	<ul style="list-style-type: none"> • Factory owner and system integrator: Erase confidential information from equipment • Equipment vendor: Provide instructions for safe disposal of equipment

3-3-3 Secure by Design

Secure by Design refers to the concept of achieving reduced delays due to rework during development, reduced introduction and operation costs of security measures, and improved maintainability of security systems by taking a security-conscious approach from an earlier stage of the FA system lifecycle.

To realize the concept of Secure by Design, define security requirements based on the results of risk assessment and construct an FA system by using established secure design principles.

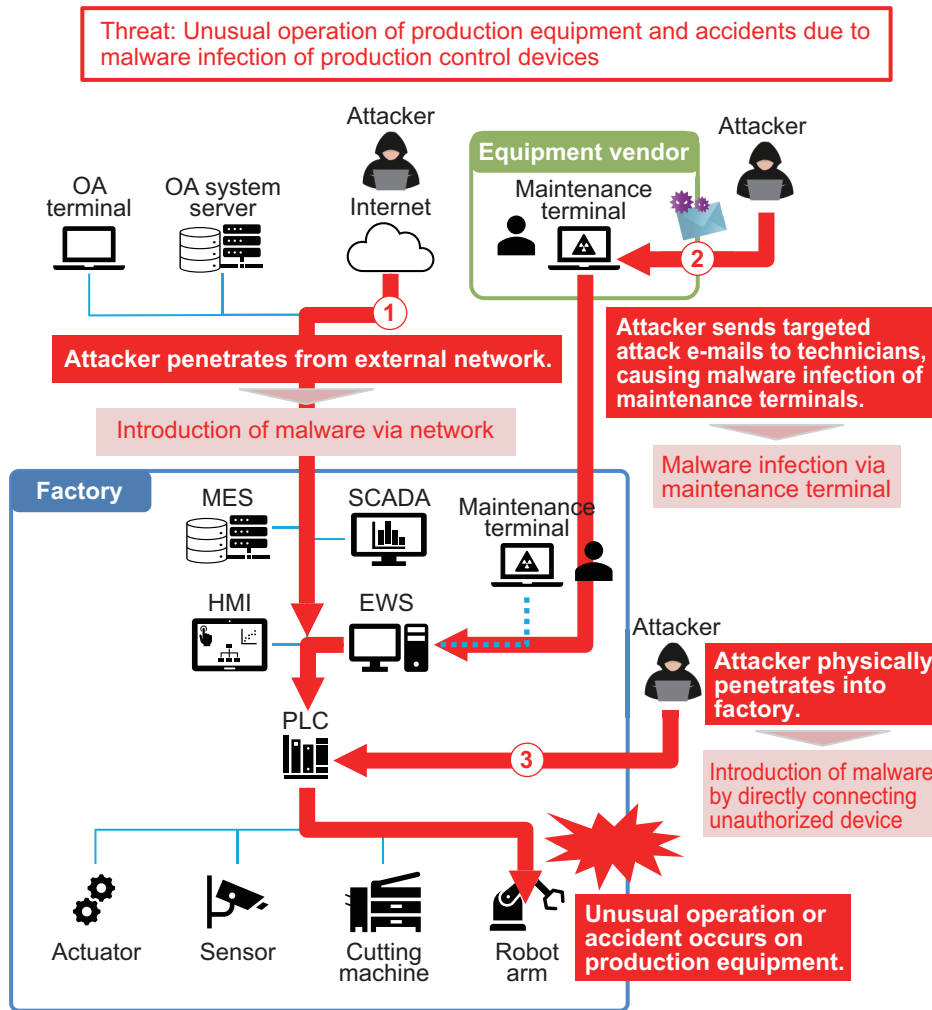
Principle	Description
Secure by Default (Ensuring security by default settings)	Make an FA system or devices composing an FA system available for safe use with the default settings.
Security Based on System Characteristics	Implement security measures without excess or deficiency based on the system characteristics, importance level, etc., instead of implementing uniform security measures for all systems.
Balance between Security and Convenience	Simultaneously achieve both convenience and enhanced security with a system toward the goal of "positive sum" that benefits both sides.
Open Design (Avoiding security through obscurity)	If security measures are affected by the concealed design and implementation information, there may be no effective defense method in the event of information leakage. Therefore, use known and proven safe technologies and methods to strengthen security measures.
Fail-safe	Design a system so as to ensure security even if a specific device that contributes to security fails or stops working.
Functional Separation and Minimum Functionality	Keep the functions of FA systems to a minimum requirement from the perspective of security risk, with each function separated from each other (with limited dependencies).
Separation of Privilege and Least Privilege	Grant privileges in the FA system in minimum units, with each privilege granted to a minimum number of users.
End-to-End Security	Ensure security by verifying the integrity of data to protect through the communications paths.

3-3-4 Defense in Depth

When considering security measures, it is important to combine several different security measures in a hierarchical manner, from establishing organization policies and rules to implementing entry and exit control against physical penetration into the factory and measures taken to protect devices that make up the factory network and systems, in order to achieve robust security.

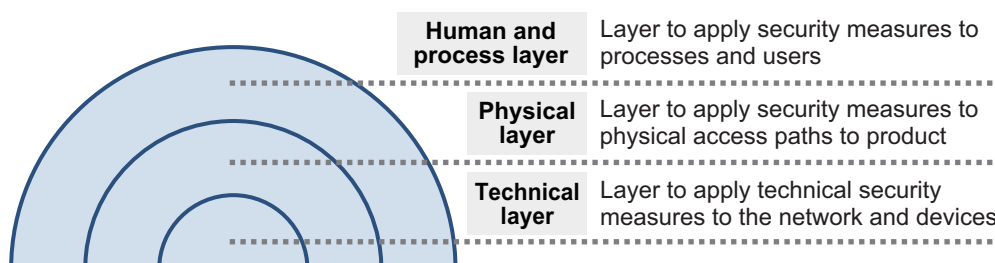
As shown in the figure below, there is a wide range of attack methods even for a single threat (e.g., unusual operation or accident of production devices caused by malware infection of a production control device). Therefore, to ensure security, you need to take not only technical measures for the

systems, but also measures against risks to *people* using the systems and the risk of attackers *physically* penetrating into zones where the devices are located.



Based on this concept, combining several measures to achieve robust security is called Defense in Depth. In this guide, the multi-layered security measures are defined as follows.

- Security measures for organizations and people (measures in the human and process layer)
- Security measures against physical penetration and contact (measures in the physical layer)
- Security measures for networks and devices (measures in the technical layer)



The table below shows examples of security measures against the above-mentioned threat and attack examples considered from these three perspectives, *human*, *physical*, and *technical* layers.

Attack method and damage	Human-related measures	Physical measures	Technical measures
1 Attacker exploits faulty FW setup to penetrate from an external network.	Implementation of security training (FW configuration and operation)	-	Introducing firewalls interfaces with external networks
2 Attacker sends targeted attack e-mails to technicians, causing maintenance terminals to be infected with malware.	Implementation of security training (targeted attack e-mails, maintenance work)	Control of carried-in devices and security inspection	
3 Attacker physically penetrates into factory.	Implementation of security training (entry and exit control)	Entry and exit control for factory and zones where the devices are installed	Permitting connections only to legitimate devices (device verification)
4 Production equipment is infected with malware.	-	-	Verifying input data to devices
			Introducing anti-malware software
5 Unusual operation or accident occurs on production equipment.	-	-	Detecting device errors (temperature, etc.)



Appendices

A-1	Related Materials.....	A-2
A-2	Contact Information for This Guide and Factory Automation Products of OMRON.....	A-3

A

A-1 Related Materials

The table below provides an overview of related documents to this document.

Publisher	Document name, overview, and related sections of this document
IEC/ISA99	IEC 62443-1 General and common matters for all documents Provides explanations of concepts, models, terms, etc. commonly referenced in the IEC 62443 series, as well as seven foundational requirements (FRs) for FA systems.
IEC/ISA99	IEC 62443-2 Security operation policies and procedures for system development and operation organizations Provides security requirements for policies and procedures for management and operation of organizations involved in FA systems.
IEC/ISA99	IEC 62443-3 Security requirements for systems Provides security function requirements, security function design, and technology for FA systems.
IEC/ISA99	IEC 62443-4 Security requirements for components Provides the security development process and security functional requirements for each component that makes up an FA system.

A-2 Contact Information for This Guide and Factory Automation Products of OMRON

If you have any questions about this guide or FA products of OMRON, please contact your nearest OMRON branch or sales office from the following links.

https://www.ia.omron.com/global_network/

Note: Do not use this document to operate the Unit.

OMRON Corporation Industrial Automation Company

Kyoto, JAPAN

Contact : www.ia.omron.com

Regional Headquarters

OMRON EUROPE B.V.

Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ASIA PACIFIC PTE. LTD.

438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON ELECTRONICS LLC

2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON (CHINA) CO., LTD.

Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

©OMRON Corporation 2023 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. P162-E1-01 0823