The Cyber/Physical Security Guidelines for Factory Systems

Ver 1.1

[Appendix: Key Considerations for Promoting Smartification]

April 11, 2025

Study Group for Industrial Cybersecurity
Working Group 1 (Systems, Technologies, and Standardization)
Factory sub-working group

Change History

Issue date	Version	Overview
April 4, 2024	Ver1.0	Ver1.0 issued
April 11, 2025	Ver1.1	Change the title to "Appendix" and modify the overall document color scheme to green.

Table of Contents

1 Introduction 1

1.1 Purpose of this document 1
1.2 How to read this document 2
[Reference] Efforts to ensure supply chain security in the semiconductor industry 4

2 Smart Factory in the main Guidelines 5

2.1 What is Smart Factory? 5
2.1.1 Factory smartification 5
2.1.2 Security risks expected in smart factories.. 6
2.1.3 Key points of security framework at smart factories.. 7

3 Key points of smartification at the planning and introduction stage of security measures 8

3.1 Step 1 Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc. 8
3.1.1 Step 1-1: Arrangement of requirements necessary for studying and planning security measures 8
3.1.2 Step 1-2: Arrangement of operations 14
3.1.3 Step 1-3: Setting the importance of business.. 16
3.1.4 Step 1-4: Arrangement of the protection target.. 17
3.1.5 Step 1-5: Setting the importance of the protection target.. 18
3.1.6 Step 1-6: Organize zones and connect zones with operations and protected objects 19
3.1.7 Step 1-7: Zones and the impact of security threats organized.. 21
[Reference] Data Management Framework for Collaborative Data Utilization.. 24

3.2 Step 2: Planning security measures 25
3.2.1 Step 2-1: Formulation of security measures policy 25
3.2.2 Step 2-2: Correspondence of security measures against assumed threats 26

3.3 Step 3: Implementation of security measures and constant review of plans, measures, and operation systems 30
[Reference] Trends in schemes for IoT security conformity assessment 37

4 Summary 39
Annex A Examples of zoning 41
Annex B Reference guidelines for each step 49
Council of this Guideline.. 50

1 Introduction

1.1 Purpose of this document

In recent years, the Ministry of Economy, Trade, and Industry has aimed to promote digital transformation (DX) in the manufacturing industry, focusing on smartification of factories as one of the efforts. Smart factories are the source of enhancing the business competitiveness of manufacturing industry. By improving the efficiency and advancement of manufacturing processes, factories can manufacture and deliver products in a timely manner, meeting diverse new needs. By visualizing data, the efficiency and resilience of the entire supply chain can be enhanced, while ensuring traceability to achieve quality assurance.

On the other hand, factory smartification requires modifications to the control system architecture, while also increasing (cybersecurity) threats caused by supply chains. Therefore, it is necessary to examine the optimal approach to security in the world where factories are closely connected to cyberspace.

In industries such as semiconductors, which are already advancing factory smartification, security measures for business partners are required in their supply chains. In addition, the Economic Security Promotion Act of Japan calls for ensuring the security of facilities installed in the essential infrastructure. Ensuring the security of IoT and digital products is also necessary when operating overseas.

The "Cyber/Physical Security Guidelines for Factory Systems" were designed with the goal of improving the security of the entire industry, particularly factory systems. The Guidelines encourage each industry and business field to develop and implement their own security frameworks for their factories. The document outlines the process of evaluating security measures for factory control systems and what factors to consider.

Amid the background described above, this document serves as a separate volume to the "Guidelines for Cyber/Physical Security Framework for Factory Systems” and presents the key points related to smartification. It aims to encourage advanced companies to promote smartification and create value for their factories without hesitation.

1.2 How to read this document

This document is primarily aimed at readers who work in the following departments of companies that are either promoting or exploring smart factory solutions. Along with the intended readers of the Guidelines, this document is also intended for personnel responsible for digital transformation (DX).

- IT-related departments (information system, information security, etc.)
- Production-related departments (production engineering, production control, engineering, etc.)[1]
- Strategic management department (business planning, etc.)
- Audit department
- Risk management department
- Digital transformation (DX) department
- Equipment system providers and vendors, equipment manufacturers (including suppliers in the supply chain)

In addition to presenting an overview of smart factories, this document also provides specific notes and examples for advancing smartification of countermeasures for each step outlined in Chapter 3 of the Guidelines. Similar to the Guidelines, industry organizations and individual companies can refer to this document for ideas when planning and implementing their countermeasures.

What is important is that industry organizations and individual companies understand the industry/business environment surrounding their factories, make a comparative consideration of such environment and values emphasized in the industry/business type, and maintain and develop the values. They need to think about what kind of factory security is necessary to make it possible, while referring to the ideas, steps, and countermeasures shown in the Guidelines. Ultimately, they need to create their own guidelines according to the circumstances of their industry and business type, and take action such as advancing security measures for their factories.

The departments that are desired to examine and implement security countermeasures at each step are shown below. Each department is expected to promote the countermeasures focusing on the relevant steps after understanding the whole content of this Appendix.

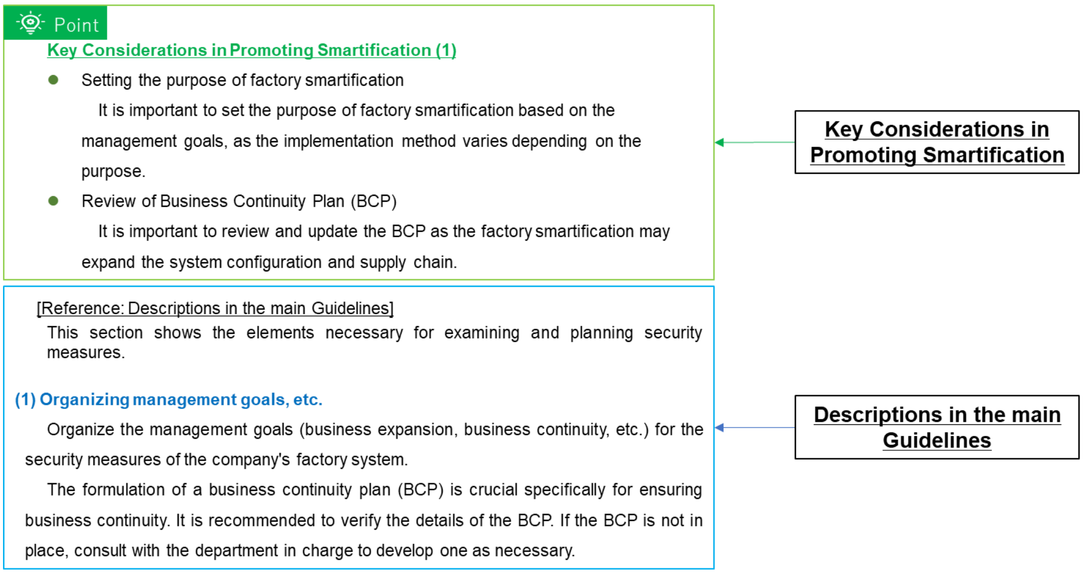
In addition, considerations for promoting smartification are described in the blue frame at the beginning of each step, and the descriptions in the main Guideline is outlined in the green frame. The outline of the Guidelines is presented as a reference to help readers understand the content by reading only this appendix. However, it is recommended that readers read both the Guidelines and this appendix to gain a deeper understanding of the content.

[1] The individuals who play a central role in this department may include those responsible for setting procurement requirements for equipment, systems, and security, configuring the equipment and systems, managers and operators, or those maintaining the equipment and systems, for example.

Table 1-1 Departments that are desired to examine and implement countermeasures at each step

Step	Departments that are desired to examine and implement countermeasures
Step 1:	IT-related departments Production-related departments Strategic management department Audit department Risk management department Digital transformation (DX) department
Step 2:	IT-related departments Digital transformation (DX) department Equipment system providers and vendors, equipment manufacturers
Step 3:	IT-related departments Production-related departments Equipment system providers and vendors, equipment manufacturers

As stated in the main Guidelines, it is crucial to continuously implement security measures while keeping the costs reasonable for promoting security solutions for factory systems. It is necessary to follow the cycle from Step 1 to Step 3 while continuously reviewing each step in accordance with changes in the business environment and technological trends, among other factors. It is also necessary to understand the unique situations and set specific definitions applicable to each company and industry, as they operate in different environments.



Point

Key Considerations in Promoting Smartification (1)

- Setting the purpose of factory smartification

  It is important to set the purpose of factory smartification based on the management goals, as the implementation method varies depending on the purpose.

- Review of Business Continuity Plan (BCP)

  It is important to review and update the BCP as the factory smartification may expand the system configuration and supply chain.

[Reference: Descriptions in the main Guidelines]

This section shows the elements necessary for examining and planning security measures.

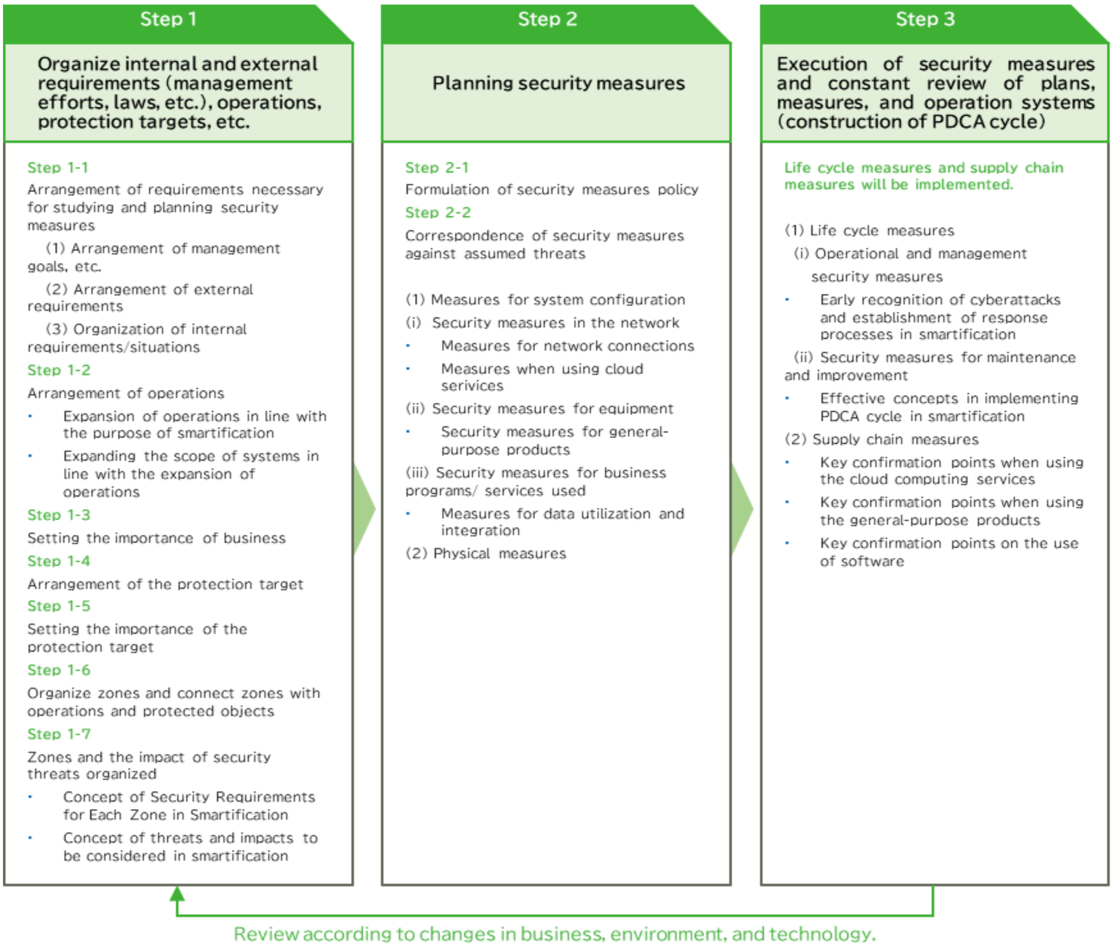
(1) Organizing management goals, etc.

Organize the management goals (business expansion, business continuity, etc.) for the security measures of the company's factory system.

The formulation of a business continuity plan (BCP) is crucial specifically for ensuring business continuity. It is recommended to verify the details of the BCP. If the BCP is not in place, consult with the department in charge to develop one as necessary.

Key Considerations in Promoting Smartification
Descriptions in the main Guidelines

Figure 1-1 Descriptions in blue frame and green frame at each step



Step 1

Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc.

Step 1-1

Arrangement of requirements necessary for studying and planning security measures

(1) Arrangement of management goals, etc.

(2) Arrangement of external requirements

(3) Organization of internal requirements/situations

Step 1-2

Arrangement of operations

- Expansion of operations in line with the purpose of smartification
- Expanding the scope of systems in line with the expansion of operations

Step 1-3

Setting the importance of business

Step 1-4

Arrangement of the protection target

Step 1-5

Setting the importance of the protection target

Step 1-6

Organize zones and connect zones with operations and protected objects

Step 1-7

Zones and the impact of security threats organized

- Concept of Security Requirements for Each Zone in Smartification
- Concept of threats and impacts to be considered in smartification

Step 2

Planning security measures

Step 2-1

Formulation of security measures policy

Step 2-2

Correspondence of security measures against assumed threats

(1) Measures for system configuration

(i) Security measures in the network

- Measures for network connections
- Measures when using cloud serivices

(ii) Security measures for equipment

- Security measures for general-purpose products

(iii) Security measures for business programs/ services used

- Measures for data utilization and integration

(2) Physical measures

Step 3

Execution of security measures and constant review of plans, measures, and operation systems (construction of PDCA cycle)

Life cycle measures and supply chain measures will be implemented.

(1) Life cycle measures

(i) Operational and management security measures

- Early recognition of cyberattacks and establishment of response processes in smartification

(ii) Security measures for maintenance and improvement

- Effective concepts in implementing PDCA cycle in smartification

(2) Supply chain measures

- Key confirmation points when using the cloud computing services
- Key confirmation points when using the general-purpose products
- Key confirmation points on the use of software

Review according to changes in business, environment, and technology.

Figure 1-2　Steps in how to proceed with planning and introduction of security measures

[Reference] Efforts to ensure supply chain security in the semiconductor industry

In recent years, there have been numerous reports of cyberattacks against semiconductor companies, including cases where suppliers of Taiwanese semiconductor manufacturers were infected with ransomware. Amid this background, the security standard "SEMI E187" was published for equipment suppliers, system integrators, and other suppliers providing equipment and services for semiconductor factories. SEMI E187 defines basic cybersecurity requirements for protecting security during operation and maintenance. The aim is to provide safe semiconductor manufacturing equipment and improve the security level of the entire supply chain of the semiconductor industry. The Taiwanese semiconductor manufacturer TSMC has set SEMI E187 as one of their procurement requirements since 2023.

2 Smart Factory in the main Guidelines

2.1 What is Smart Factory?

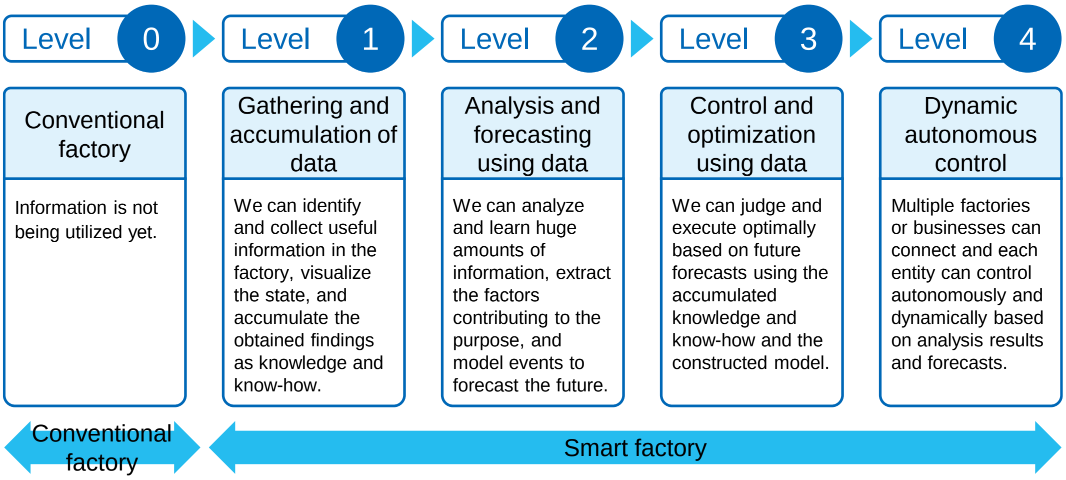
2.1.1 Factory smartification

Factory smartification aims at strengthening the business competitiveness with the use of digital technology. In order to improve quality and reduce costs, factory smartification enables visualization of various situations in factories, work instruction and support based on various data, data integration and cooperative manufacturing, etc. In many cases, smartification of existing factories is promoted step-by-step.

The following efforts are assumed to be made during the process of factory smartification. In some cases, data integration and utilization will grow[2], strengthening the connection between physical and cyberspace. As a consequence, security risks will also increase. Thus, it is crucial to implement appropriate security measures based on the risks. When tackling with smartification of existing factories, it is also necessary to review the security measures.

- Ensuring the sophistication and flexibility of factory lines and facilities
- Integration of the factory control system and the information system
- Remote access
- Integration with third-party systems Security risks expected in smart factories

[2] The Ministry of Economy, Trade, and Industry conducted the *Survey on Ensuring Cyber Security in Smart Factories*, which outlines the different stages of a smart factory. Typically, as the level of factory smartification advances, the connection with cyberspace also increases, thereby raising the risk of security breaches. Therefore, it is crucial to implement appropriate security measures according to the level of smartification.



Level 0 — Conventional factory: Information is not being utilized yet.

Level 1 — Gathering and accumulation of data: We can identify and collect useful information in the factory, visualize the state, and accumulate the obtained findings as knowledge and know-how.

Level 2 — Analysis and forecasting using data: We can analyze and learn huge amounts of information, extract the factors contributing to the purpose, and model events to forecast the future.

Level 3 — Control and optimization using data: We can judge and execute optimally based on future forecasts using the accumulated knowledge and know-how and the constructed model.

Level 4 — Dynamic autonomous control: Multiple factories or businesses can connect and each entity can control autonomously and dynamically based on analysis results and forecasts.

2.1.2 Security risks expected in smart factories

Various efforts are made during the process of factory smartification, depending on the purpose of smartification and the desired outcomes through digital technology utilization. One example is collecting data from IoT devices, analyzing it via cloud computing, etc. and providing feedback based on the results. In smart factories, security risks are expected to increase specifically in the following areas. The table below shows some examples of specific security risks.

- Increased connectivity with external networks

  In the process of smartification, factories are highly likely to integrate their control systems with IT systems and external cloud services, leading to increased connectivity with external networks. This increases the number of entry routes for attackers, which also increases the risk of factory system attacks. In some cases, due to the cyberattacks against control system, systems connected to the control system can also be affected.

- Expansion of supply chains

  In the process of smartification, the introduction of external devices and services may be considered, leading to an increase in the amount of content that cannot be managed in-house only. This poses a risk of the company's factory system being suspended, depending on external circumstances.

Table 2-1 Examples of security risks in factory smartification

	Matter to be considered	Security risk
Ensuring the sophistication and flexibility of factory lines and facilities	Built-in computer in the equipment	• Same risk as a computer
	Use of ICT functions such as Wireless LAN, 5G	• Increased risk of external network connectivity
Integration of factory control system with IT system	Connection of FA system and OA system networks	Increased mutual risks due to gaps in security measures between control and information systems
	Data in FA system also exist in OA system.	• Increased risk of data falsification or leakage due to the usage of different systems for user management.
Remote access	Connection via external network	Cyberattacks via external networks
	Use of external equipment	Risk due to insufficient management of devices and user management
Integration with third-party systems	Different security policy introduced by the external system	• Possible cyberattacks due to gaps in acceptable risks
	Expanded effects of cyberattacks	Difficulty in smooth coordination of response in the event of incident, unclear scope of responsibility

2.1.3 Key points of security framework at smart factories

This Appendix presents specific notes and examples on promoting smartification at each step outlined in Chapter 3 of the main Guidelines, while considering the security risks described in **エラー! 参照元が見つかりません。**. The following points should be considered in particular.

- Concept of Zoning

  In the process of smartification, it is important to have zoning from an operational perspective. This is because operations[3] are added and upgraded based on their purpose. While the importance of zones was described in the main Guidelines, this Appendix explains the concept and the key points to be considered in zoning from an operational perspective.

  * Zone refers to an area set by each company, based on the content and importance of operation and the equipment environment. Zones can be composed of both physical and cyberspaces. This is because Operations can be connected physically but also can be connected by data. Assets in the same zone need to be protected by security frameworks of equal levels.
- Dividing responsibilities and roles in line with the expansion of the supply chain

  To promote smartification, it is especially crucial to clarify the division of responsibilities, assign roles for security frameworks, revies the incident response. The smartification process is highly likely to involve the introduction of external equipment and services, as well as the sharing of data between your factories or your company and other businesses. As a result, there may be an increase in events that your company cannot handle alone, or the scope of in-house management can be unclear. The main Guidelines present the key points in promoting supply chain measures. This Appendix, however, will provide specific examples of setting security requirements for business partners and suppliers.

[3] For the purpose of the Guidelines, "operations" refer to a series of tasks required for production to achieve a goal.

3 Key points of smartification at the planning and introduction stage of security measures

3.1 Step 1 Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc.

The main Guidelines mainly describes the policy for streamlining internal and external requirements, operations, protected targets, etc., and the concept of zones. In addition to the above, this Appendix also describes the points to consider when reorganizing internal and external requirements, operations, and protection targets, as well as the detailed approach to zoning.

3.1.1 Step 1-1: Arrangement of requirements necessary for studying and planning security measures

Point

Key Considerations for Promoting Smartification (1)

- Setting the purpose of factory smartification

  It is important to set the purpose of factory smartification based on the management goals, as the methods and necessary security measures vary depending on the purpose.
- Review of Business Continuity Plan (BCP)

  It is important to review and update the BCP as the factory smartification may add and expand the system configuration and supply chain.

[Reference: Descriptions in the main Guidelines]

This section shows the elements necessary for studying and planning security measures.

（1） Arrangement of management goals, etc.

Organize the management goals (business expansion, business continuity, etc.) related to the security measures of the company’s factory system.

In particular, whether or not a business continuity plan (BCP) has been formulated is important from the perspective of business continuity, so confirm that content. If a BCP has not been developed, implement studies of formulation of a plan together with the department in charge if necessary

- Setting the purpose of factory smartification

  The methods for achieving smartification vary depending on the purpose, and actual practices may also vary, including restructuring production lines, configuring new factory systems, and reviewing supply chains. It is crucial to clarify the purpose of smartification, as the required security measures vary depending on the methods used to achieve smartification.

  The main purpose of smartification includes improving quality, reducing costs, increasing productivity, shortening time to market and mass production, addressing personnel shortages and human resource development, providing new added-value and improving existing value.

Table 3-1 Targets of smartification[4]

Targets of smartification	Specific Examples
Improving quality	Reducing defect rates
	Stabilizing quality and reducing variability
	Improving design quality
Reducing costs	Reducing production resources
	Reducing inventory
	Reducing manpower in facility management and monitoring
Increasing productivity	Improving the operating ratio of equipment and manpower
	Reduction of suspended operation due to equipment failure
Shorter time to market and mass production	Automation of product development and design
	Speeding up responses to specification changes
	Shorter time for designing and constructing production lines
Addressing personnel shortages and human resource development	Utilizing diverse human resources
	Succession of skills
Providing new added value and enhancing the existing value	Improving flexibility to meet diverse needs
	Expanding available processing technologies
	Providing new products and services
	Improving product performance and functions
Others	Strengthening risk management

- Review of Business Continuity Plan (BCP)

When promoting smartification, the BCP should be checked and reviewed from the following viewpoints. It is required to reflect necessary matters in the BCP, such as decision-making criteria, considering the impacts on business partners and supply chains.

- Confirm whether the impacts on business partners and supply chains are considered in the BCP.

✓ The impact for the operation and production of a company's factory system if its business partner is targeted by a cyberattack causing the leakage of production-related information, unavailability of information, network or system suspension, or quality issues.

✓ The impact for the factory system if network or system failures are suspected to be caused by a cyberattack on a business partner, but it is impossible to determine whether it is caused by a mere bug, device failure, or cyberattack

✓ The impact for business partners if the company is suspected of being targeted by a cyber-attack, causing the leakage of production-related information, unavailability of information, network or system suspension or failures, or quality issues.

It is important to note that even if your company's network or system is not directly connected to a business partner, both parties will still be impacted by each other through exchanging information, data, operations, or services.

[4] Compiled based on the *Smart Factory Roadmap -Toward the realization of manufacturing in line with the Fourth Industry Revolution*, The Chubu Bureau of the Ministry of Economy, Trade and Industry, 2017
https://www.chubu.meti.go.jp/b21jisedai/report/smart_factory_roadmap/roadmap.pdf

▪ Confirmation of the assumed impacts on existing factory systems by adding new system/services, etc.

✓ Confirmation of the assumed impacts on existing factory systems by adding new system/services, etc.

✓ The impact on the operation and production of the company's factories if some or all of the functions of the newly added system service are suspended in the event of a cyberattack

✓ The impact on the operation and production of the company's factories in the event of a system failure in the newly added system service

▪ Confirmation of the decision-making process for suspending or continuing factory system operations

✓ Establishment of the criteria for deciding whether to suspend or continue factory system operations in response to the situations as described above.

✓ Clarification of the decision-making structure (who is responsible at the factory and head office) and decision-making representatives

Point

Key Considerations for Promoting Smartification (2)

- Identifying the trends in Japanese and overseas standards and legal systems

  To check if there are any requirements in the perspective of smartification, it is essential to review relevant international standards and legal system.
- Identifying industry guidelines and standards

  To check if there are any requirements in the perspective of smartification, it is essential to review relevant industry standards and guidelines.

[Reference: Descriptions in the main Guidelines]

（2） Arrangement of external requirements

External requirements related to the security measures of the company's factory system (security law / regulation / standard / guideline compliance, requirements from the national / local government, requirements from the industry, requirements from the market / customers, requirements from business partners, requests from investors, etc.) are organized.

When arranging the external requirements, the security threats are perceived based on the standards and guidelines, etc.

- Identifying the trends in Japanese and overseas standards and legal systems

  Keep track of trends in the standards and legal systems that apply to your factory system and business, in addition to smartification. These include IEC 62443 and other standards concerning factory system security, the EU Cyber Resilience Act imposing security requirements on products, and the system for ensuring the security of equipment installed in core infrastructure under the Economic Security Promotion Act of Japan to ensure the stable provision of specified social infrastructure services. Make sure to review these standards and legal requirements regularly. Specifically, check whether there are any specific requirements to be followed from the perspective of smartification.

- Identifying industry guidelines and standards

  In certain industry fields, which are related to in-house business, updated versions of industry guidelines and standards relating to factory systems may be introduced. Therefore, it is useful to stay up-to-date with the latest information from industry associations and other relevant organizations, and review if there are any significant points to consider from the perspective of smartification. Security measures may be clearly required by laws and regulations, etc., but even voluntary standards and guidelines may be widely accepted as standard measures in the market. Therefore, it is important to understand the latest trends of other companies and customer needs in your industry field.

Point

Key Considerations for Promoting Smartification (3)

- Identify internal and external stakeholders

  It is important to review both internal and external stakeholders since smartification may increase the reliance on external devices and services.

- Assess and update the current status of relevant departments and governance system

  When implementing smartification, it is important to review and update the relevant departments and the governance system, due to the increased use of new services and external network connections.

- Understanding and organizing the impact of incidents

  When implementing smartification, it is important to review and assess the impact of the incident, given the increased number of stakeholders and internal stakeholders involved.

[Reference: Descriptions in the main Guidelines]

（3） Organization of internal requirements / situations

Organize the current status of internal requirements (system, operation / management, maintenance / improvement, etc.) and systems related to the company's factory security. If the system for promoting factory security is unclear, the way of thinking will be organized at this stage, systems, rules and procedures, etc. for promoting security measures will be developed, implementation plans will be planned, and dissemination, education, etc. will be implemented.

- Identify internal and external stakeholders

  With the increasing use of external devices and services with smartification, the number of stakeholders is highly likely to increase. Thus, it is important to identify all the stakeholders. The following examples show stakeholders that are highly likely to be included specifically through smartification. In some cases, tasks may be reassigned to subcontractors, and it is essential to identify all subcontractors.

  ･ Suppliers of external equipment (IoT devices, routers, etc.) introduced (to the factory system)
  ･ Providers of cloud services used by the factory system
  ･ Outsourced vendors handling the configuration, operation, and maintenance of the factory system

- Assess and update the current status of relevant departments and governance system

  Smartification increases the introduction of new services and external network connections. It is important to review relevant departments and governance systems and update them as necessary. The following examples show relevant departments that are highly likely to be included specifically through smartification.

  ･ Production engineering department at the head office
  ･ IT systems and security departments at the head office
  ･ Digital transformation (DX) department

  After identifying relevant departments, assess the division of roles and cooperation among them. Specifically, the following points need to be confirmed.

- In order to improve the security of the factory, it is important to verify if the relevant departments can provide the necessary information for the factory, or if the factory can provide the information required by the relevant departments. Additionally, it is crucial to confirm the organizational structure for information collection, including its procedures, timing, and other relevant details.
- Confirm if relevant departments can collaborate and if the company has a governance system that allows business owners to commit.

● Understanding and organizing the impact of incidents

When implementing smartification, it is important to review and assess the impact of the incident, given the increased number of stakeholders and internal stakeholders involved. Incidents related to the factory system can have an impact on the company's business, other companies and the surrounding environment, as well as the factory itself.

In order to ensure the BCP as explained in (1), it is important to clearly identify the stakeholders and reexamine the organizational structure, rules, and procedures for incident response from the following perspectives.

- Confirmation of the assumed impact on other companies in the event of an incident, associated with expanding operations and the scope of the systems
- Confirmation of the assumed impact on the company in the event of an incident arising in another company.
- Confirmation of the assumed impact on the company and its factory systems when a vulnerability is found in a procured product or in the event of an incident

3.1.2 Step 1-2: Arrangement of operations

Point

Key Considerations for Promoting Smartification (1)

- Expansion of operations in line with the purpose of smartification

  In order to examine the security measures corresponding to smartification, it is important to confirm the operations expanding along with it.

- Expanding the scope of systems in line with the expansion of operations

  With new operations expanding along with smartification, it is important to confirm the expanded scope of systems according to the volume of operations.

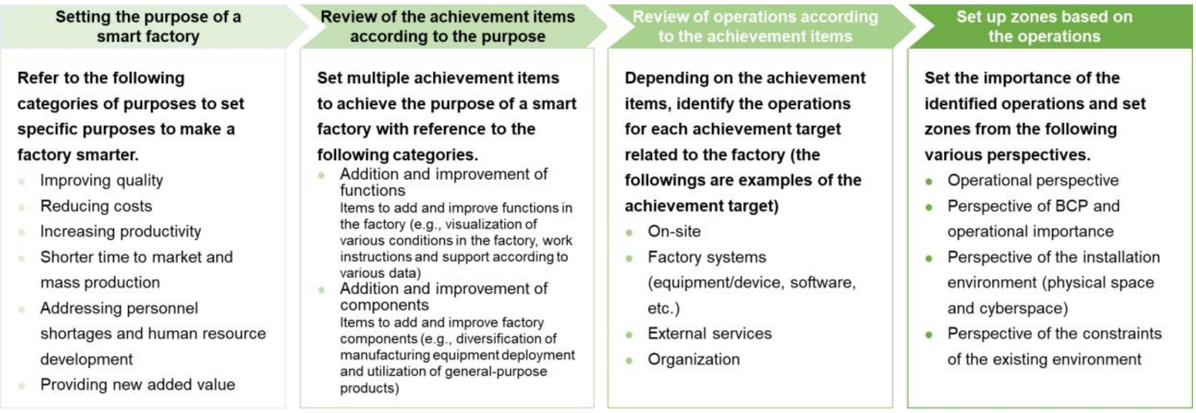
[Reference: Descriptions in the main Guidelines]

Find out how the factory system is used in daily work.

- Expansion of operations in line with the purpose of smartification

  Newly added operations needed for achieving the purpose of smartification as described in 3.1.1 should be identified according to the following procedure. It is important to identify both the operations performed in-house and the operations outsourced to other companies, as well as the scope that cannot be managed by your company alone. Set the zones at Step 1-6 and 1-7 based on the identified operations.

  1. Identify the tasks to be achieved to meet the purpose of smartification. Tasks to be achieved can be broadly divided into the improvements and additions to factory system functions, and the improvements and additions to factory system components.
  2. Elaborate the tasks to be achieved for each purpose (e.g. production site, factory system, external services, organization) of the required task.



Setting the purpose of a smart factory

Refer to the following categories of purposes to set specific purposes to make a factory smarter.

- Improving quality
- Reducing costs
- Increasing productivity
- Shorter time to market and mass production
- Addressing personnel shortages and human resource development
- Providing new added value

Review of the achievement items according to the purpose

Set multiple achievement items to achieve the purpose of a smart factory with reference to the following categories.

- Addition and improvement of functions
  Items to add and improve functions in the factory (e.g., visualization of various conditions in the factory, work instructions and support according to various data)
- Addition and improvement of components
  Items to add and improve factory components (e.g., diversification of manufacturing equipment deployment and utilization of general-purpose products)

Review of operations according to the achievement items

Depending on the achievement items, identify the operations for each achievement target related to the factory (the followings are examples of the achievement target)

- On-site
- Factory systems (equipment/device, software, etc.)
- External services
- Organization

Set up zones based on the operations

Set the importance of the identified operations and set zones from the following various perspectives.

- Operational perspective
- Perspective of BCP and operational importance
- Perspective of the installation environment (physical space and cyberspace)
- Perspective of the constraints of the existing environment

Figure 3-1 Steps for Zoning

Table 3-2 Example of Tasks to be Achieved for Meeting the Target of Smartification

Category	Tasks to be achieved	Details
Functional addition and improvement	Visualization of various situations in a factory	● Visualization of equipment status, work status, production performance, quality performance, and raw material/ component status
	Trace of factory components	● Identification of the scope that may be affected by quality ● Parts, equipment, human resources, and information trace
	Various data use for work instruction and support	● Production instructions to equipment and operators based on production plans ● Data provision necessary for work in accordance with production status ● Real-time production instructions based on equipment operation performance
	Understanding production issues and taking measures	● Discovering production bottlenecks ● Yield
	Production/operation forecast and optimization	● Optimization of production plans based on operation status ● Optimization of operation status by production status
	Data integration and coordination	● Productivity improvement ● Low asset production ● Life cycle quality management
	Business continuity	● Cooperation among BCP-related organizations ● Optimization of maintenance
Component addition and improvement	Diversification of workplaces and production equipment installation layouts	● Workplaces for human resources (in-house/outsourced) ● Locations of control systems (Human machine interfaces (HMI), etc.) (in-house/outsourced) ● Production lines (in-factory, in-company, in-house, outsourced teams)
	Utilization of general-purpose products	● Hardware (built-in general-purpose software, hardware with network function, etc.) ● Software (package, OSS, outsourced development, etc.)

- Expanding the scope of systems in line with the expansion of operations

  The scope of systems is often expanded compared with conventional factory systems when carrying out the necessary operations for achieving the purpose of smartification. Therefore, the status of cooperation and data integration for operations should be checked for the following areas with particularly high security concerns.

  ・ Connection between the factory control system and the IT system
  ・ Interconnection between factories
  ・ Interconnection between companies
  ・ Use of cloud and other external services

3.1.3 Step 1-3: Setting the importance of business

Point

Key Considerations for Promoting Smartification (1)

- Review of the importance level of operations in line with the expansion of operations
  It is critical to review the importance level of operations newly added with smartification.

[Reference: Descriptions in the main Guidelines]

Determine the importance of each kind of work for the work that uses the identified factory system. The importance of business is a factor in determining the importance / priority of security measures.

However, since the environment set for each company or industry is different, it is necessary to define the importance of work suitable for each company or industry.

- Review of the importance level of operations in line with the expansion of operations
  Review the level of importance for the new operations added to the factory system along with smartification, as identified in 3.1.2. When reviewing the operations, attention should be given to the fact that the level of importance for operations may differ depending on the purpose of smartification.

3.1.4 Step 1-4: Arrangement of the protection target

Point

Key Considerations in Promoting Smartification (1)

- Review of the objects to be protected in line with the expansion of systems.
  It is important to review the objects to be protected in line with the expansion of systems along with smartification.

[Reference: Descriptions in the main Guidelines]

For operations for which security measures should be strengthened, identify the components (network, equipment / devices (functions / programs) / data) of the factory system that supports / implements the operations, and organize the schematic diagram of the system configuration diagram.

In factories, components frequently change, such as changes to the production line, etc., so even in the measures implementation and operation stage in step 2 and step 3, it is required to organize and ascertain the individual components and consider the response continuously and efficiently while utilizing the automation tools, etc. if necessary.

- Review of the objects to be protected in line with the expansion of systems.
  Examine the components of the factory system in accordance with the expansion of the system confirmed in 3.1.2, and review the diagram. It is important to consider that systems and services outside the factory (such as those found in other factories and cloud services) may also be included as components of the entire system when promoting smartification. Below are some examples of protected objects that can be added to achieve smartification.

Table 3-3 Examples of protected objects that can be added to achieve smartification

Type	Component
External services	Cloud computing system
	AI analysis system
Equipment / devices	New computer and network equipment (wireless LAN, router, etc.)
	Highly functional production facilities
	IoT sensors and equipment (cameras, etc.)
Software operation program	New software (equipment monitoring, etc.)
	Packaged software
	Sophisticated control model
Data	Data integration with new partners
	IoT sensor data
	Production instructions to production facilities
	Data on the production process

3.1.5 Step 1-5: Setting the importance of the protection target

Point

Key Considerations for Promoting Smartification (1)

- Review of the importance level of each protected object based on Steps 1-3 and 1-4.

  With smartification, it is important to reassess the level of importance for each protected object.

[Reference: Descriptions in the main Guidelines]

From the perspective of business expansion / continuation (BC), which is the value axis that the manufacturing industry / factory emphasizes, from the perspective of safety assurance (S), quality assurance (Q), on-time delivery / delay prevention (D), and cost reduction (C), and from the perspective of the importance of the work, the importance of each of the identified protection targets will be clarified. The importance of the protected object is a factor in determining the priority of security measures.

- Review of the importance level of each protected object based on Steps 1-3 and 1-4.

  Review the importance level of each protection object identified in 3.1.4 from the perspectives of business continuity and production operations.

  When reviewing the importance, it is necessary to clarify the importance of the external system services as well. The importance of these services will be a factor to determine the system's requirements and service contract details, etc.

3.1.6 Step 1-6: Organize zones and connect zones with operations and protected objects

Point

Key Considerations for Promoting Smartification (1)

- Organize the concept of internal and external connections when advancing smartification based on the evolution of technology

  It is important to reconfigure the zoning necessary to implement security measures by considering the newly added operations along with smartification.

[Reference: Descriptions in the main Guidelines]

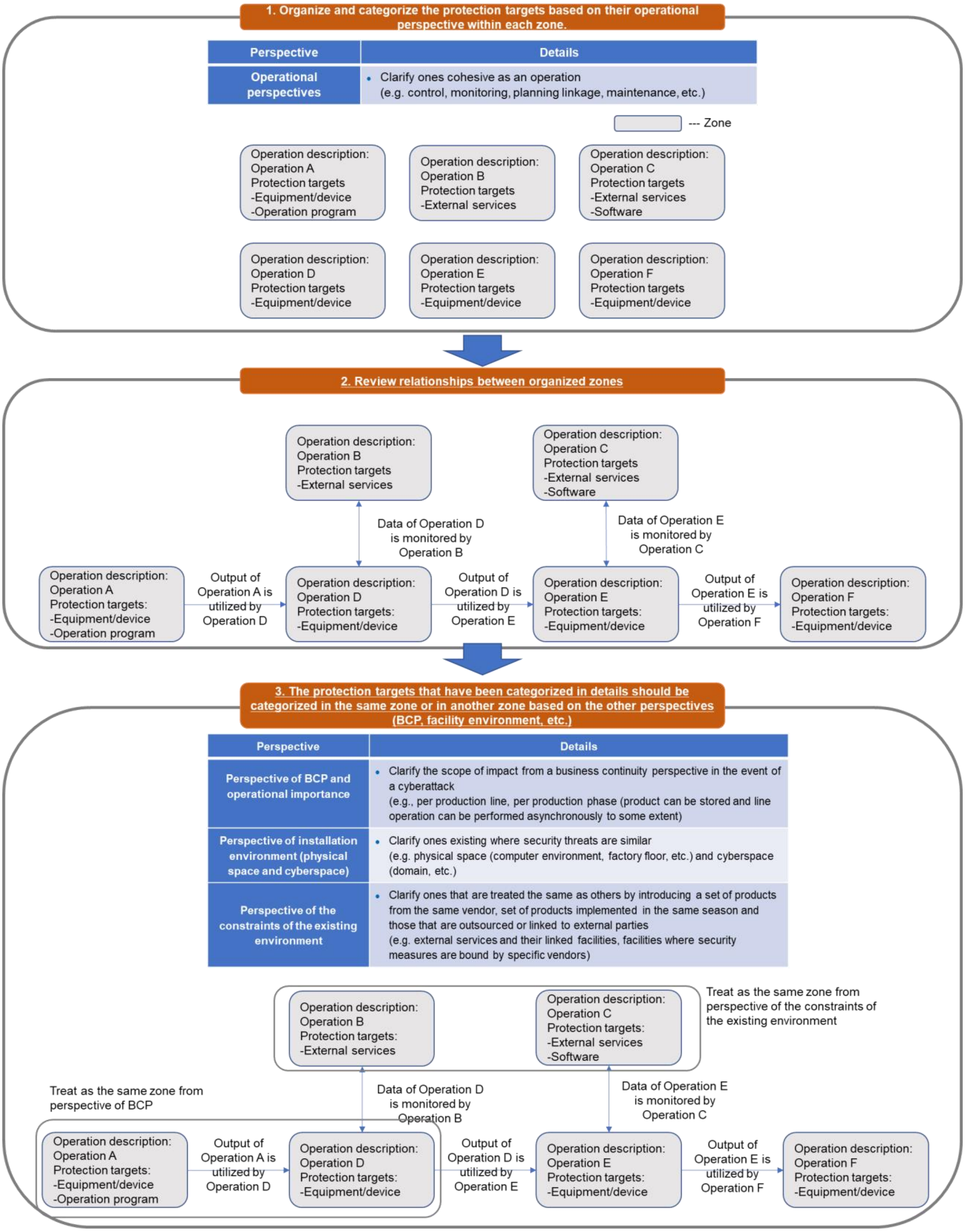
The factory system sets a zone as an area in which security measures at an equal level are required while considering the business content and business importance. Also, for each zone, connect the operations and protection targets that have been organized so far. By setting the zones, it becomes possible to see a bird's eye view of the equipment and systems of the factory as large category concepts, and when protection targets inside a certain zone receive cyberattacks, it will be possible to consider deterring the impact on different zones and minimizing the damage.

- Organizing the concept of internal and external connections when advancing smartification based on the evolution of technology (Wrap up the current status and envision the future form)

In factory smartification, the security risks can vary depending on the system expansion and addition of new equipment or external service connections. In order to ensure appropriate security measures are in place, it is important to review the zoning.

In order to achieve smartification, new operations should be added or updated. Therefore, when setting a zone, it is important to break down and organize the protected objects to be handled within that zone from an operational perspective. To achieve this, the following procedures should be followed during the zoning process.

1. Organize and categorize the protected objects based on their operational perspective within each zone.
2. Confirm how the organized zones are connected (Check how their operations relate to one another.)
3. The facilities and equipment that have been categorized in details should be treated as the same zone or as another zone based on the other perspectives such as BCP, facility environment (physical, cyberspace), etc.



1. Organize and categorize the protection targets based on their operational perspective within each zone.

Perspective	Details
Operational perspectives	• Clarify ones cohesive as an operation (e.g. control, monitoring, planning linkage, maintenance, etc.)

--- Zone

Operation description: Operation A
Protection targets
-Equipment/device
-Operation program

Operation description: Operation B
Protection targets
-External services

Operation description: Operation C
Protection targets
-External services
-Software

Operation description: Operation D
Protection targets
-Equipment/device

Operation description: Operation E
Protection targets
-Equipment/device

Operation description: Operation F
Protection targets
-Equipment/device

2. Review relationships between organized zones

Operation description: Operation B
Protection targets
-External services

Operation description: Operation C
Protection targets
-External services
-Software

Data of Operation D is monitored by Operation B

Data of Operation E is monitored by Operation C

Operation description: Operation A
Protection targets:
-Equipment/device
-Operation program

Output of Operation A is utilized by Operation D

Operation description: Operation D
Protection targets:
-Equipment/device

Output of Operation D is utilized by Operation E

Operation description: Operation E
Protection targets:
-Equipment/device

Output of Operation E is utilized by Operation F

Operation description: Operation F
Protection targets:
-Equipment/device

3. The protection targets that have been categorized in details should be categorized in the same zone or in another zone based on the other perspectives (BCP, facility environment, etc.)

Perspective	Details
Perspective of BCP and operational importance	• Clarify the scope of impact from a business continuity perspective in the event of a cyberattack (e.g., per production line, per production phase (product can be stored and line operation can be performed asynchronously to some extent)
Perspective of installation environment (physical space and cyberspace)	• Clarify ones existing where security threats are similar (e.g. physical space (computer environment, factory floor, etc.) and cyberspace (domain, etc.)
Perspective of the constraints of the existing environment	• Clarify ones that are treated the same as others by introducing a set of products from the same vendor, set of products implemented in the same season and those that are outsourced or linked to external parties (e.g. external services and their linked facilities, facilities where security measures are bound by specific vendors)

Operation description: Operation B
Protection targets:
-External services

Operation description: Operation C
Protection targets:
-External services
-Software

Treat as the same zone from perspective of the constraints of the existing environment

Treat as the same zone from perspective of BCP

Data of Operation D is monitored by Operation B

Data of Operation E is monitored by Operation C

Operation description: Operation A
Protection targets:
-Equipment/device
-Operation program

Output of Operation A is utilized by Operation D

Operation description: Operation D
Protection targets:
-Equipment/device

Output of Operation D is utilized by Operation E

Operation description: Operation E
Protection targets:
-Equipment/device

Output of Operation E is utilized by Operation F

Operation description: Operation F
Protection targets:
-Equipment/device

Figure 3-2 Diagram of the concept in zoning

3.1.7 Step 1-7: Zones and the impact of security threats organized

Point

Key Considerations for Promoting Smartification (1)

- Concept of Security Requirements for Each Zone in Smartification
  It is important to consider the necessary security requirements for each of the newly set zones with smartification.
- Concept of Threats and Impacts by Smartification
  It is important to examine the threats and impacts that require special attention, such as integration with external services and connections with external networks in the process of smartification.

[Reference: Descriptions in the main Guidelines]

Examples of threat types which have an impact on the operation of factory systems include:

- Theft of equipment, destruction and unauthorized operation of systems and equipment
- Abnormal control or shutdown of equipment
- Data theft / leakage
- Data falsification / destruction
- Reduced availability
- Used as a steppingstone for external attacks
- System / equipment failure / fault
- Employee or maintenance staff (equipment vendor) negligence
- Facilities and work environment threats
- Natural environment threat Abnormal control or stoppage of equipment

After perceiving the above kinds of latest threats concerning cybersecurity pertaining to the company's factory systems, we will consider these threats and the impact on production and business and sort out what kind of security threats are expected for each zone and what kind of impact they will have.

- Concept of Security Requirements for Each Zone in Smartification5
  Examine the security requirements for zones organized in Step 1-6. When examining the security requirements, it is important to consider security threats both between zones and within each zone. Each zone may have different security threats, but information such as data and control instructions may be exchanged between different zones. For the concept of security within and between zones, please refer to the "Data Management Framework for Collaborative Data Utilization" by the Ministry of Trade, Economy and Industry.

[5] There is a new approach to security called "zero trust" that differs from the method of implementing security measures at the boundary. This approach focuses on implementing security measures for protected assets. Depending on the status of smartification, it might be effective to consider implementing the zero trust concept.

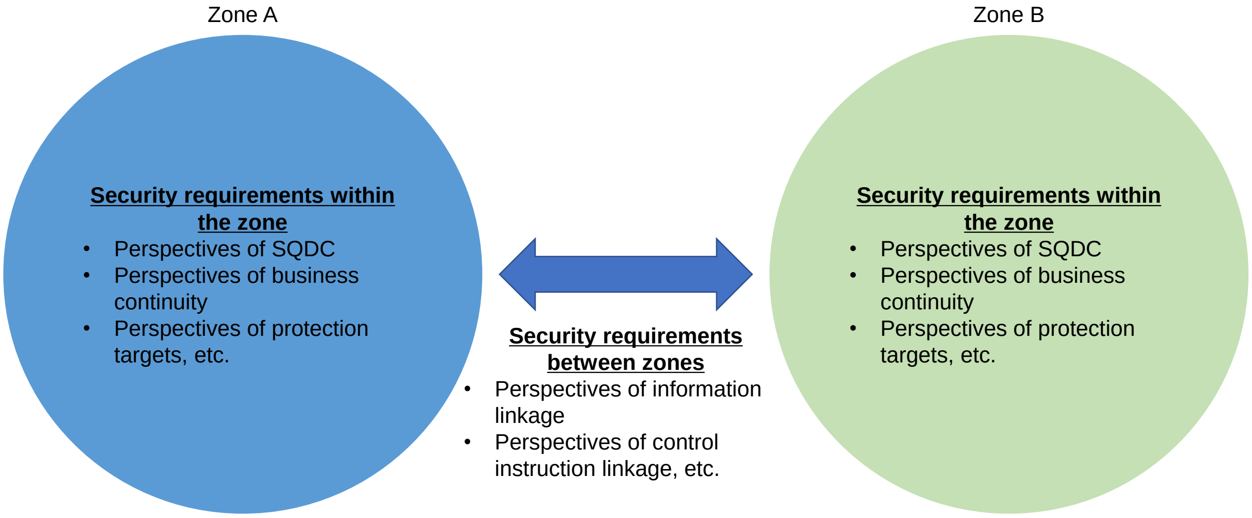

Zone A
Zone B
Security requirements within the zone
Perspectives of SQDC
Perspectives of business continuity
Perspectives of protection targets, etc.
Security requirements between zones
Perspectives of information linkage
Perspectives of control instruction linkage, etc.
Security requirements within the zone
Perspectives of SQDC
Perspectives of business continuity
Perspectives of protection targets, etc.

Figure 3-3 Overview Concept of Security Requirements in Zones

It is also important to consider security threats from both physical safety and cybersecurity perspectives. Some examples of perspectives that can be used for examining security threats are shown below. As the concept for the above viewpoint, please refer to the ”IoT Security Safety Framework” by the Ministry of Economy, Trade and Industry.

Table 3-4 Examples of perspectives to consider when examining security threats between different zones

Category	Viewpoint	Details
Security requirements within the zone	SQDC	• Viewpoint of safety assurance (S) • Viewpoint of quality assurance (Q) • Viewpoint of delivery date compliance and delay prevention (D) • Viewpoint of cost reduction (C)
	Business continuity	• Impact of stoppage (period and costs of stoppage) • Impact of data leakage • Impact of malfunction • Degree of ripple effect • Quality of ease recovery • Identification of the extent of impact
	Protected object	• Ensuring the elements of security from the viewpoints of Availability, Integrity, and Confidentiality (examples of protected objects: equipment and devices, software, operational programs, and data)
Security requirements between zones	Information transfer	• Ensuring the confidentiality on the sending and receiving sides of information (confirmation of data that may be sent and received) • Ensuring the availability on the sending and receiving sides of information (backup of sent and received data) • Ensuring the integrity on the sending and receiving sides of information (comparison of sent and received data)
	Integration of control instructions	• Existence of control instructions from outside the factory's control network

- Concept of threats and impacts to be considered in smartification

  The following threats need special attention in smartification. Organize threats from the viewpoint of Table 3-5. The following shows some examples of viewpoints used for examining security threats.

Table 3-5 Examples of viewpoints for examining security threats

	Matter to be considered	Viewpoints for examining security threats
Ensuring the sophistication and flexibility of factory lines and facilities	Built-in computer in the equipment	Protected object ● The computer is performing incorrect calculations, causing the data value to change.
	Use of ICT functions such as Wireless LAN	Business continuity ● Increasing external network connectivity raises the risk of unauthorized access and production line stoppages.
Integration of factory control system with IT system	Connection of FA system and OA system networks	Information transfer ● Lack of input validation between the control and information systems results in sending inaccurate data and incorrect control instructions.
	Data in FA system also exist in OA system.	Information transfer ● • Data falsification/leakage due to the use of different systems for user management.
Remote access	Connection via external network	Business continuity ● A cyberattack from an external network causes external devices to become unavailable.
	Use of external equipment	Business continuity ● Insufficient management of user devices or user management, resulting in data leakage to external networks
Integration with third-party systems	Different security policy introduced by the external system	Business continuity ● Cyberattacks on external systems with varying risk tolerances cause factory system operations to stop.
	Expanded effects of cyberattacks	SQDC ● Difficulty in smooth cooperation in the event of an incident, unable to comply with delivery schedule due to unclear scopes of responsibility
	Guaranteeing the operation of external systems and responding to system stoppage	Business continuity ● Different levels of maintenance can lead to gaps in incident response speed, resulting in inadequate business continuity.
	Handling of information on external systems	Protected object ● A cyberattack on an external system result in the leakage of factory control system data stored on the external system beyond the factory's network.

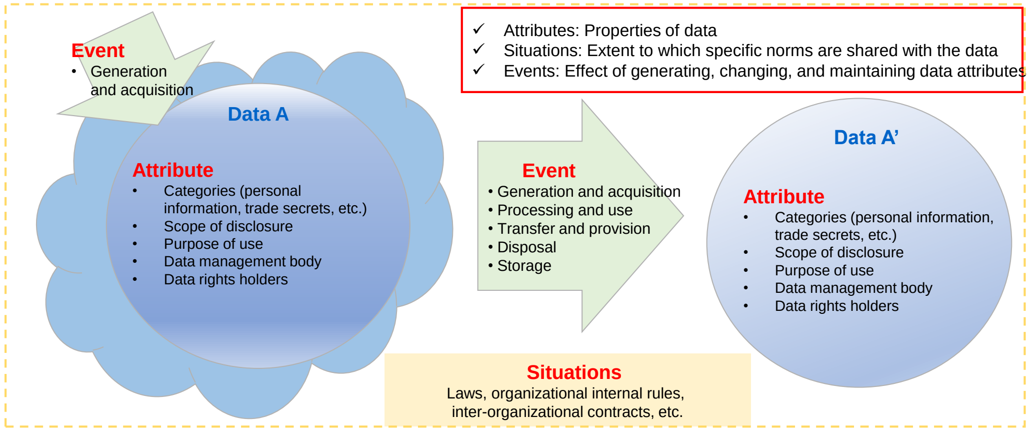
[Reference] Data Management Framework for Collaborative Data Utilization

METI's Data Management Framework for Collaborative Data Utilization is a reference framework for implementing necessary security measures through appropriate data management. It focuses on managing data throughout its lifecycle, visualizing the status of data and identifying risks. The Framework defines data management as the “process of managing changes to data attributes that occur due to events under certain situations while taking into account the data's life cycle” and organizes a model consisting of the following three interrelated elements.

- Events (data generation and acquisition, processing and usage, transfer and provision, storage, and disposal)
- Situations (laws and regulations of each country/region, internal rules of the organization, contracts between organizations, etc.)
- Attributes (category, scope of disclosure, purpose of use, data controller, data rights holder, etc.)

The framework aims to help visualize the status of data, thereby enabling appropriate data management across all stakeholders.

The main Guidelines refer to the Framework, by replacing the Framework’s data with zones and its events with data transfer and processing between zones.



✓ Attributes: Properties of data
✓ Situations: Extent to which specific norms are shared with the data
✓ Events: Effect of generating, changing, and maintaining data attributes

3.2 Step 2: Planning security measures

The main part of the Guidelines maps threats and countermeasures and summarize practical measures in terms of system configuration and physical aspects. Based on the above, the separate volume describes the key confirmation points in terms of system configuration and physical aspects in smartification. Measures for operation and management are described in Step 3.

3.2.1 Step 2-1: Formulation of security measures policy

Point

Key Considerations for Promoting Smartification (1)

- Formulation of a security policy based on smartification

  It is important to formulate a security policy based on the security requirements for each zone.

[Reference: Descriptions in the main Guidelines]

Develop a policy for implementing security measures for factory systems. Set the importance and priority of the zones organized in step 1 and the related operations, protection targets, and assumed threats according to the environment in which the industry or individual company is located.

It is important that the importance and priority be assigned appropriately for each individual company / industry.

- Formulate a security policy based on smartification

  Based on the security requirements for each zone set in Steps 1-6 and 1-7, review the importance and priority of each zone and associated operations, protected objects, and assumed threats. It is crucial to allocate the appropriate level of importance and priority to each company and industry. Please refer to the descriptions in the main part of the Guidelines for assistance. It is specifically important to review and confirm any changes (e.g. expansion of the factory system, expansion of the supply chain, etc.) made to the factory system in the process of smartification. Formulate the security policy for each zone based on the revised level of importance and priority.

  It is important to prioritize responding to the most significant threats first, such as those that could lead to business interruption, rather than responding to all threats. It is also necessary to consider comprehensive measures, including operation and management as described in Step 3.

3.2.2 Step 2-2: Correspondence of security measures against assumed threats

Point

Key Considerations for Promoting Smartification (1)

- Measures on system configuration and physical aspects of smartification
  As more external devices and services are used in the process of smartification, it is important to review security measures according to the characteristics of smartification.

[Reference: Descriptions in the main Guidelines]

Link the corresponding security measures with the zones, protected objects, operations, threats, and impacts that were previously organized.

Regarding the individual security measures, the measures are exemplified in the following (1) Measures for system configuration and (2) Physical measures, so while referring to these as appropriate, and depending on the environment of the individual company or industry, it is important to plan and implement necessary measures while considering the cost-effectiveness of the measures.

- Measures on system configuration and physical aspects of smartification
  it is necessary to review security measures in terms of system configuration and physical factors. This review should be based on a viewpoint of examining the security requirements for each zone, within the same zone, and between different zones, as determined in Step 1-6 and Step 1-7. The following security measures should be taken with special attention when advancing smartification.

(1) Measures for system configuration

(i) Security measures in the networks

- Measures for network connections
  During the process of factory smartification, it is expected to establish diverse network connections, including connections to and through external networks. With diverse network connections, the routes for potential attackers to intrude also increase, leading to a higher risk of security breaches. With the increasing diversity of network connections, larger amounts of data will be distributed, and the impact of data falsification and destruction will also spread.
  Regarding security measures for network connections in smartification, it is important to not only establish secure connections but also to examine the comprehensive security measures taking into account system configuration, while cooperating with other companies, offices, and hubs to ensure the confidentiality, integrity, and availability of data. When examining security measures, it is necessary to consider specifically the following points.
  - Measures to be taken when networks are connected between zones with different security requirements
  - Supply chain requirements when connecting the factory system to the zone managed by an external company
  - Ensure the confidentiality, integrity, and availability of data distributed between different zones

- Measures when using cloud services

When aiming to advance factory smartification, one might want to consider the utilization of cloud services. It is necessary to select which cloud service to use from the following viewpoints. Specific items to be checked are shown in Step 3.

- The company's environment and the terms of use of the cloud services
- Purpose of using the cloud services
- The service provider's policy on responsibilities and responses in the event of an incident
- Reliability in data migration (if data migration is required)
- Policy for resumption of operations after restoration in the event of cloud service failure

For additional information on security measures when using cloud services, please refer to the "Information Security Management Guidelines for the Use of Cloud Computing Services" published by the Ministry of Trade, Economy, and Industry.

(ii) Security measures for equipment

- Security measures for general-purpose products

When advancing factory smartification, the use of general-purpose products without specified security functions also increases. The use of general-purpose products can contribute to usability and cost reduction, but it is necessary to ensure the necessary security level for each use and purpose. The following points should be noted for each hardware and software in examining actual security measures.

- Hardware

When advancing factory smartification, it is assumed that general-purpose products such as hardware with embedded general-purpose software (OS), open interfaces, and network-enabled hardware will be procured.

Implementing specific security measures for general-purpose hardware is difficult for procurers. Therefore, the use of such hardware should be examined based on the following points. In addition to asking the supplier, it is important to consider indirect security measures that can be implemented in introduced hardware. Many of these measures are for operations and management, and they will be discussed in details in Step 3.

- ➢ Implementation of security measures for hardware
- ➢ The supplier's and the maintenance provider's vulnerability response status
- ➢ Policies for equipment maintenance and operation in the event of an incident

- Software

When advancing factory smartification, it is expected that the software used will incorporate open-source software (OSS). OSS can be used for in-house development or parts provided by suppliers.

When developing software that includes OSS within the company, it is essential to prioritize the following measures.

- Management of component information for the OSS used
- Implementation of daily vulnerability management and necessary security measures

In addition, when procuring the OSS from external sources, the following points need to be checked as the measures that can be taken by users are limited depending on the form of provision. Specific measures shall be described in Step 3 for operation and management.

- Can the user check the software components?
- Are the licenses for the software components that were introduced been managed properly?
- Have security measures and vulnerability responses been implemented?

(iii) Security measures for business programs and services used

- Measures for data utilization and integration

In a smart factory system, data utilization and integration are expected to take place. This involves collecting information from various facilities and IoT equipment, then accumulating and processing the data in cloud services and other relevant methods. Finally, the results of analysis are fed back to each factory for further usage. On the other hand, malfunctions and failures in the program and services may cause incorrect data utilization and unintended feedback. Particular attention should be paid to the use of OSS when using software in areas where security measures are required.

When planning data utilization and integration, it is important to confirm the following points specifically, within or between companies and external operators.

- Assurance for data quality (standardization of data quality)
- Measures to prevent data defect and loss
- Scope of data acquisition
- Scope of data utilization

（2） Physical measures

It is important to plan and implement necessary physical measures to protect against natural threats and physical intrusion, even in a smart factory.

Table 3-6 Examples of security measures to address potential threats in smartification

	Type of threat	Content of threat	Type of measure	Content of measure
1	Theft of equipment, destruction or unauthorized operation of systems or equipment	Unauthorized access to the system from an external network	(1) Measures for system configuration	(1) (i) Measures for the network
2		Unauthorized control of equipment capitalizing on software defects	(1) Measures for system configuration	(1) (ii) Measures for equipment
3	Abnormal equipment control and destruction	Unauthorized access to facilities capitalizing on vulnerabilities	(1) Measures for system configuration	(1) (ii) Measures for equipment

4	Data theft/ leakage	Leakage of data stored in external services	(1) Measures for system configuration	(1) (ii) Measures for equipment
			(1) Measures for system configuration	(1) (iii) Security measures for operational programs and services used in the system
5	Data falsification• destruction	Missing data in a program	(1) Measures for system configuration	(1) (ii) Measures for equipment
6		Inappropriate feedback from incorrect data entry	(1) Measures for system configuration	(1) (i) Measures for the network
7	Reduced availability	Data unavailability due to database capacity shortage	(1) Measures for system configuration	(1) (iii) Security measures for operational programs and services used in the system
8	Negligence of an employee or a maintenance personnel (equipment vendor)	Suspended use due to insufficient software licensing	(1) Measures for system configuration	(1) (ii) Measures for equipment
9		External data leakage due to inadequate data handling	(1) Measures for system configuration	(1) (iii) Security measures for operational programs and services used in the system

3.3 Step 3: Implementation of security measures and constant review of plans, measures, and operation systems

The main part of the Guidelines outlines the measures for life cycle and supply chains (outsourcing of operations of the factory system and consignment of system development, etc.) This appendix describes the concept of dividing responsibilities while considering the organization's expansion from the perspective of life cycle countermeasures, while also covering practical supply chain countermeasures along with the introduction of external equipment and services from the viewpoint of supply chain countermeasures.

Point

Key Considerations for Promoting Smartification (1)

- Measures for lifecycle in smartification

  It is important to review the life cycle measures, as the related departments expand and external network connections increase with smartification.
- Supply Chain Measures in Smartification

  It is important to review the supply chain measures, as the use of external devices and services increases with smartification.

[Reference: Descriptions in the main Guidelines]

In step 3, the security measures planned in step 2 will be executed and measures will be taken in the life cycle and in consideration of the supply chain.

Based on the information obtained from these efforts, after step 3, it is important to implement the PDCA cycle from step 1 to step 3 of reviewing the plans, measures, and operational status according to changes in business, environment, technology, etc., and if necessary, promoting the efforts again from step 1.

When implementing step 3, depending on the environment of the individual company or industry, it is important to plan and implement the necessary measures while considering the cost-effectiveness of the measures.

（1） Measures for lifecycle

(i) Security measures for operation and management

- Early recognition of cyberattacks and establishment of response processes in smartification

  It is important to establish early recognition of cyberattacks and countermeasures (OODA process[6]) to cope with the increased security risks associated with increased external network connections and other factors.

[6] The Observe-Orient-Decide-Act cycle is a model that summarizes a series of measures for detecting and responding to cyberattacks.

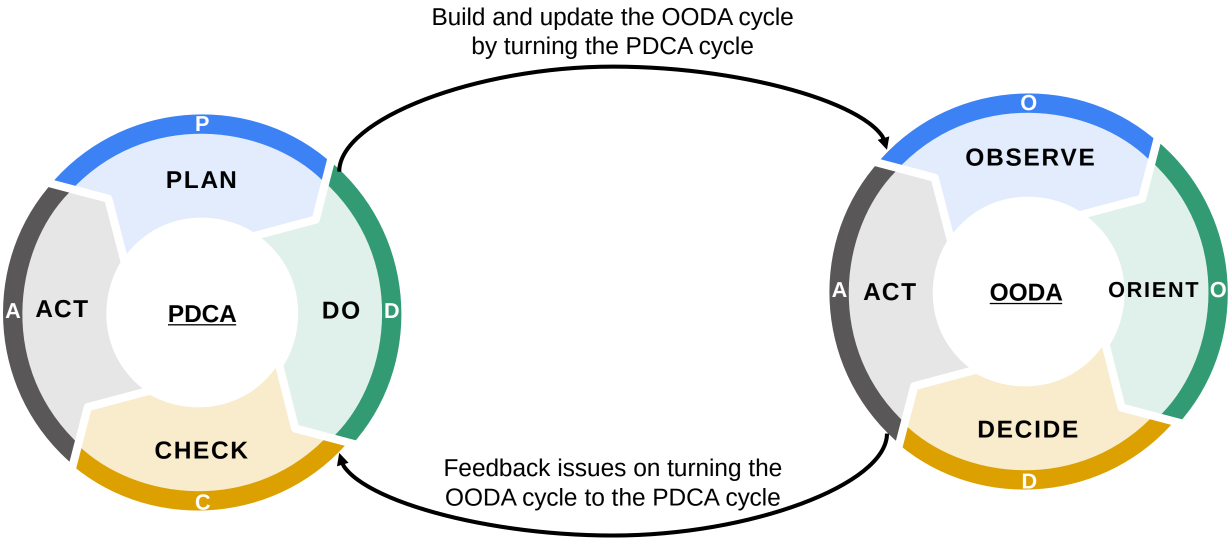

Build and update the OODA cycle
by turning the PDCA cycle
P
PLAN
A
ACT
PDCA
DO
D
CHECK
C
O
OBSERVE
A
ACT
OODA
ORIENT
O
DECIDE
D
Feedback issues on turning the
OODA cycle to the PDCA cycle

Figure 3-4 Relationship between PDCA cycle and OODA cycle

When examining security measures for increased external connections in the process of smartification, the integration of OT and IT security is more required than before. To achieve this, it is crucial to define the departments responsible and decision-makers involved in each process. Additionally, a system of information coordination should be established to enable early detection and countermeasures against cyberattacks. In addition to the occurrence of damage, as security risks continue to rise, it is becoming increasingly important to collect, understand, and respond to information related to new attack methods and vulnerabilities. Therefore, it is essential to clarify the division of roles during the preventive maintenance stage. The examples of role division during the preventive maintenance stage and damage occurrence stage are shown below.

- Preventive maintenance stage

  In the preventive maintenance stage, collect and analyze information about potential cyberthreats before an incident occurs and take necessary measures. The table below shows a scenario where a vendor or the security department has shared vulnerability information.

Table 3-7 Example of role division in early detection and countermeasures for cyberattacks (preventive maintenance stage)

	Main department in charge	Decision maker	Example of implementation
Monitoring (Observe)	Vendor	• Representative of security department	• Collecting vulnerability information of installed devices • Communication on vulnerability information of installed devices
Analysis (Orient)	Security Department	• Representative of security department	• Analyzing the exploitability of vulnerability • Analyzing the degree of impact on the factory system if vulnerability is exploited
Decision (Decision)	Security Department	• Business owner (depending on importance) • Representative of security department • Factory manager, production site manager	• Considering the countermeasures against vulnerabilities • Analyzing the effects on factory operation when measures are taken • Decision to implement measures
Action (Action)	Production site	• Factory manager, production site manager	• Instruct the production site to take measures according to the details. • Implement measures according to the instructions given to the production site

- Damage occurrence stage

  The damage occurrence stage involves dealing with unexpected incidents, whether they are the result of cyberattacks or not. Analyze and determine if the reported production site incident is caused by a cybersecurity issue, and take appropriate measures if necessary.

Table 3-8 Example of role division in early detection and countermeasures for cyberattacks (damage occurrence stage)

	Main department in charge	Decision maker	Example of implementation
Monitoring (Observe)	Production site	• Head of the Production Department	• Occasional reporting of any gaps between the conventional production site and the smart system, along with the reasons for any discrepancies. • Identifying and updating the factory system components
Analysis (Orient)	Appropriate department based on the content of the report	• Head of the department in charge of BCP • Head of the department in charge of security	• Analyzing the degree of impact that a reported incident may have on the factory system • Analyze if the reported incident is a result of a security concern.

Decision （Decision）	Security Department	● Business owner (depending on importance) ● Head of the department in charge of security ● Factory manager, production site manager	● Considering the measures for reported events ● Analyzing the effects on factory operation when measures are taken ● Decision on implementation of measures
Action （Action）	Production site	● Factory manager, production site manager	● Instruct the production site to take measures according to the details. ● Implement measures according to the instructions given to the production site

Even in the above-mentioned role division, there are too few security personnel in the control field and even fewer in the production site. The following measures can be effective in addressing the shortage of human resources.

- Introduction of tools to monitor equipment in the factory
- Introduction of tools to detect cybersecurity incidents
- Outsourcing a part of the early recognition and response process for cyberattacks to external security vendors.

(ii) Security measures for maintenance and improvement

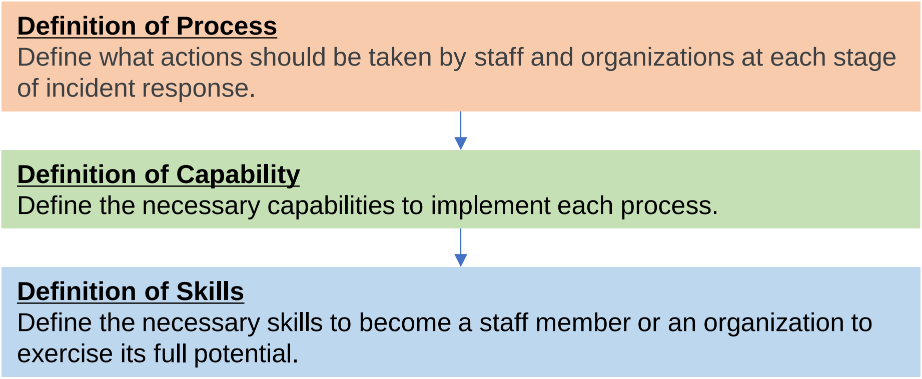
- Effective concepts in implementing PDCA cycle in smartification

When a factory undergoes smartification, security risks are expected to increase, due to greater connectivity to external networks, greater use of external equipment, and more number of involved parties such as equipment vendors. To accommodate changes made by smartification, security measures must be evaluated from physical, system, operation, and management perspectives, followed by running the updated PDCA cycle.

The following measures are effective in implementing the PDCA cycle for smartification, even in the face of frequent changes.

- Compilation of manuals for security measures and incident responses
- Development of human resources that are capable of responding to cybersecurity issues
- Establishment of an organizational structure capable of implementing the PDCA cycle
- Include a production site manager and others relating to production, in the PDCA cycle structure

When implementing the above measure, it is important to consider the definition of necessary skills and maturity model for the organization and human resources. The following are examples of policies for examining required skills and maturity models.



Definition of Process
Define what actions should be taken by staff and organizations at each stage of incident response.

Definition of Capability
Define the necessary capabilities to implement each process.

Definition of Skills
Define the necessary skills to become a staff member or an organization to exercise its full potential.

Figure 3-5 Definition of skills required for organizations and human resources

Table 3-9 Example of maturity model for organizations and human resources

Organization	Maturity level		
	Basic	Practice	Application
Cooperation between internal and external organizations	Example: Information sharing within and outside the company	Example: Confirmation of measures to be taken by internal and external organizations assuming a practical incident	Example) Confirmation of measures to be taken by internal and external organizations in the event of a high-level incident (unknown or combined)
Related departments	e.g.: Information sharing among internal departments	Example: Confirmation of measures to be taken by multiple organizations assuming a practical incident	e.g.: Confirmation of measures to be taken among multiple organizations in the event of a high-level incident (unknown or combined)
Within the relevant department	Example) Confirmation of incident response methods within the relevant department	Example) Confirmation of actions within the relevant department assuming an actual incident	e.g.) Confirmation of measures to be taken within the relevant department in the event of a high-level incident (unknown or combined)

Moreover, as the existing factory will change with smartfication, unexpected events that could not be anticipated in the previous system are highly likely to occur. On the other hand, it is difficult to prepare for unexpected events. Therefore, it is suggested to take measures against unexpected events after implementing existing security measures. Here are some examples of measures that may be taken in response to unexpected events.

- Investigate any related incidents and confirm the appropriate measures to take in the case of your company.
- Estimate other possible incidents based on the incidents that have occurred in-house
- Establish a management framework that allows employees to learn from their own case studies
- Introduce AI-based tools to analyze information about unexpected events and detect unexpected threats

（2） Measures for supply chains

The main part of the Guidelines provides examples of key points to confirm with business partners and suppliers, such as purchased products/parts, outsourced operations, system development consignment, and integrated systems.

Based on the above viewpoint, this separate volume summarizes the key confirmation points from a viewpoint of requiring further examination in the case of smartification.

- Key confirmation points when using the cloud computing services

In the process of smartification, the use of external cloud computing services may be considered. However, it is difficult for many cloud service users to manage security measures by themselves. Therefore, it is necessary to confirm the responsibilities and policies on incident response with service providers in all three stages of cloud service procurement, contract, and operation/maintenance.

The following points should be confirmed at each stage of procurement, contract, and operation/maintenance of cloud services. It is not necessary to cover all these points, but it is important to choose and contract with a cloud service provider that considers security risks and response measures based on expected usage of the services. The "Guidelines for the Safe Use of Cloud Services for Small and Medium-sized Enterprises" issued by the Information-technology Promotion Agency, Japan provide a useful reference for cloud service safety.

Table 3-10 Points to be checked when using the cloud computing services

	Points to check
Procurement	• Is the cloud service provider reliable? • Does the cloud service provider offer support for their users? • Are there any inconsistencies between the security policies of your company and the cloud service? • Are new devices and services introduced together with cloud services?
Contract	• Does the provider indicate their service levels such as service utilization rate, failure frequency, and recovery target time? • Does the provider set the conditions of data handling in the case their service is terminated?
Operation and maintenance	• Are there clear rules for operation of the cloud service separate from the factory's operations? • Is the confidentiality confirmed for the information handled by the cloud service? • Is there a personnel who understands how to use the cloud service? • Do you manage cloud service users appropriately? • Are you prepared with a backup plan and a data restore plan when the cloud service is stopped? • Is the factory system connected to any supplier or external company networks through a cloud service?

- Key confirmation points when using general-purpose products

It is expected that the use of general-purpose products will increase due to smartification. As for general-purpose products, implementing security measures can be challenging for the procurement side. Therefore, it is crucial to verify whether the products have proper security measures in place. Additionally, it is important to understand the responsibilities of the vendor and their response policy in case of any vulnerability detected or incidents that occur after product delivery.

The following points should be confirmed at each stage of procurement, contract, and operation/maintenance of cloud services. Although not many general-purpose products may respond to all incidents, it is important to use them after considering security risks in the event of an unsupported incident[7].

Table 3-11 Points to be checked when introducing general-purpose products

	Points to check
Procurement	● Does the vendor have a product security policy in place and disclose it? ● Is the product security support policy clearly stated? ● Is there a system established to maintain product security (e.g. support contact, vulnerability report contact, incident response system, etc.)? ● Is there a function to ensure product security (such as updates or initialization)? ● Are the security checks and verifications conducted in accordance with the relevant standards? ● Is information about product and component vulnerabilities being collected? ● Is it possible to check information about the security functions and settings of the product? ● Is any additional equipment or services introduced in connection with the product?
Contract	(Assuming that it is a general-purpose product, asking for security requirements through a contract can be difficult.)
Operation and maintenance	● Is the newly introduced product being managed well? ● Have additional security measures been implemented based on the importance of the operation in which the product is being used? ● Is the information regarding product vulnerabilities checked regularly, and are appropriate responses taken when necessary? ● Is there a process established to verify and address any potential security vulnerabilities? ● Have you created a backup plan in case the product becomes unsupported or unavailable?

When procuring general-purpose products, you can confirm if they are certified[8] to meet a certain level of security standards. Adopting these products will be effective enhance the security of factory systems.

In accordance with the Economic Security Promotion Act, core infrastructure providers must confirm compliance with the requirements before conducting procurement.

[7] The *Guidelines for Product Security Measures for Small and Medium-sized Enterprises Developing IoT Devices* published by The Ministry of Economy, Trade and Industry in June 2023 may serve as a useful reference for checking and verifying security functions when procuring devices.

[8] Certification is a process where compliance with specific requirements (criteria, standards, regulations) is evaluated and a third party provides a written guarantee of compliance.

[8] Industrial Cyber Security Study Group Working Group 3 (Commission for Establishment of Security Conformity Assessment System for IoT Products), The Ministry of Economy, Trade, and Industry
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

[Reference] Trends in schemes for IoT security conformity assessment[9]

The Ministry of Economy, Trade and Industry is considering implementing a "Security Conformity Assessment Scheme for IoT Security Products." This scheme is intended to serve as a system to assess and certify IoT products by a third party based on common security criteria when government authorities or companies select and purchase IoT products. It will also assign labels to IoT products that meet minimum security standards, providing people with the confidence to use network services.

- Key confirmation points on the use of software

The use of software in factories is also examined in the process of smartification. It is important to examine both third-party and in-house developed software. This involves paying attention not only to the procurement, contract negotiation, operation, and maintenance of such software, but also to the use of OSS, management of software components, and vulnerability management and response during software development, as illustrated in Step 2.

The following are the points that need to be checked during procurement, contract negotiation, development, operation, and maintenance. There is no need to meet all the following points. However, it is important to consider procuring, introducing or developing software that consider security risks according to the intended usage of software.

Table 3-12 Points to be checked when introducing software

	Points to check
Procurement	• Is it possible to check the security policy of the software? • Is there a system established for maintaining security (e.g. support contact, vulnerability report contact, incident response system, etc.)? • Is there a function to ensure software security (such as updates or initialization)? • Are the security checks and verifications conducted in accordance with the relevant standards? • Is information about software and component vulnerabilities being collected? • Is it possible to check information about the security functions and settings of the software? • Is any additional equipment or services introduced in connection with the software?
Contract	• Is the security support policy clearly stated? • Is the support policy for software failures clearly stated? • Is there a clear policy on disclosing software components? • Is there a clear statement of the software's license information?
Development	• Are the components, including the OSS, used in the software managed properly? • Is the management of software component licenses being handled appropriately? • Is there a daily system in place for managing vulnerabilities and implementing necessary security measures?
Operation and maintenance	• Is the software installed on the system being managed properly? • Have additional security measures been implemented based on the importance of the operation in which the software is being used? • Is the information regarding software vulnerabilities checked regularly, and are appropriate responses taken when necessary? • Is there a process established to verify and address any potential security vulnerabilities? • Have you created a backup plan in case the software becomes unsupported?

Consideration is being given to implementing the Software Bill of Materials (SBOM) to make confirmation of the above points more efficient. SBOM is a parts list of software components used for license and vulnerability management. The Ministry of Economy, Trade and Industry is leading to promote the use of SBOM and has released the "Guide on the Introduction of SBOM (Software Bill of Materials) for Software Management.” The Guide provides information about the benefits of implementing SBOM along with common misunderstandings and facts. It also offers guidance on the necessary steps to be acknowledged and implemented when introducing SBOM, which can serve as a helpful reference.

4 Summary

With the promotion of manufacturing industry DX, the smartification of factories increases security risks due to enhanced connectivity with external networks, data distribution related to factory systems control, and supply chain expansion.

This material is a separate volume of the "Guidelines for Cyber/Physical Security Measures in the Factory System". It provides the key concepts and points to be considered for the security measures needed for factory smartification. The aim of this material is to promote efforts in factory smartification while strengthening the business competitiveness of the manufacturing industry and ensuring security.

Specifically, the following two points are described with case examples, as they need be considered in detail in the process of smartification.

- Concept of Zoning

  In order to reduce risks associated with smartification, it is necessary to take the following measures based on the concept of zoning.

  - Detailed zoning from a viewpoint of operations
  - Review the security risks that exist within a zone and between different zones
  - Implementation of security measures according to security risks

- Dividing responsibilities and roles in line with the expansion of the supply chain

  The integration of external networks due to smartification will increase the number of cases where the company cannot directly manage security measures. Therefore, there is a risk that the company's factory system may be vulnerable to cyberattacks from outside sources, or that cyberattacks on the company may affect outside sources.

  In order to reduce the above-mentioned risks, it is necessary to consider the following measures in the process of smartification.

  - From a procurement, contract, operation, and maintenance viewpoint, confirm and implement both internal and external measures.
  - Establish a PDCA cycle across the entire organization, including internal and external sources.

We hope this additional volume will assist you in promoting security measures during factory smartification.

Annexes

Annex A Examples of zoning

As an example of zoning, we assume that the following two points are the purpose of smartification.

(i) Use of services for manufacturing equipment based on CAD information
(Utilization of new services within the factory)

(ii) Use of external remote maintenance services in automated warehouses
(Utilization of new services outside the factory)

(iii) Improved efficiency of production monitoring functions by upgrading MES servers
(Upgrading of existing functions in the factory)

The outline of the factory zones in this case is shown below.

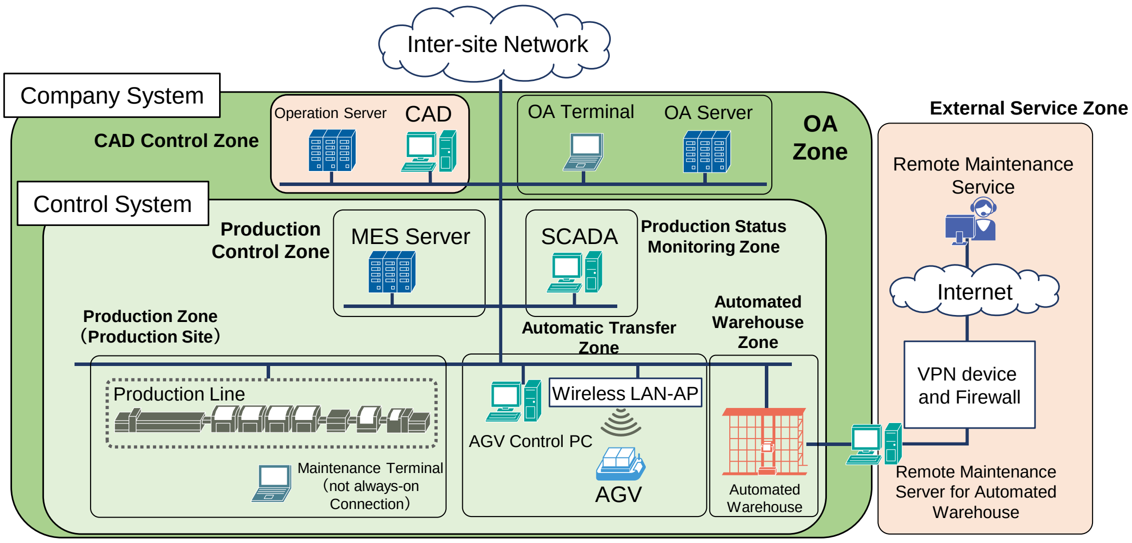


Figure C-1 Assumed zones in a factory

Table C-1 Outline of the assumed zones in a factory

	Name	Overview	Related protected targets	New/existing
1	Production zone (Production site)	• Production line for manufacturing products. Zone consisting of control equipment and devices	• Production line • Maintenance terminal console • Router • Parts inventory (at production site)	Existing
2	Automatic transport zone	• Zone for operating AGVs that transport parts and finished products.	• Control PC for AGVs • Wireless LAN-AP • AGV	Existing
3	Automated warehouse Zone	• Zone that operates the automatic equipment for storage and retrieval while storing components	• Remote maintenance server for automated warehouse • Automated warehouse • Parts inventory (at production site) • Material inventory (warehouse)	Existing
4	Production control Zone	• Zone with servers responsible for managing production plans, traceability data, and other related functions.	• MES server • Production instructions • Production recipe • Production performance	Existing
5	Production status monitoring zone	• Zone equipped with systems that acquire and visualize the production status and equipment-related information.	• SCADA • Production performance • Equipment status • Equipment program / parameters / drawings	Existing
6	OA zone	• Zone performing operations that are not directly related to production.	• OA server • OA terminal • Production planning • Production instructions	Existing
7	CAD control zone	• Zone responsible for managing CAD data to automatically control the production zone	• CAD • Operation server	New
8	External services zone	• Zone where external services are running to remotely monitor automated warehouses	• VPN device and firewall	New

① Use of services for manufacturing equipment based on CAD information

1. Divide factory zones in details from the viewpoint of operations

In this case, the production zone was divided into two zones based on a detailed analysis of operations, a viewpoint that differs from a conventional factory approach.

- Parts manufacturing zone
- Product manufacturing zone

* This example shows the case of the processing and assembly industry, which the production zone can be divided in detail based on operations. On the other hand, it can be challenging to divide production zones in the material industry due to the operational process. Each company and factory need to be examined individually.

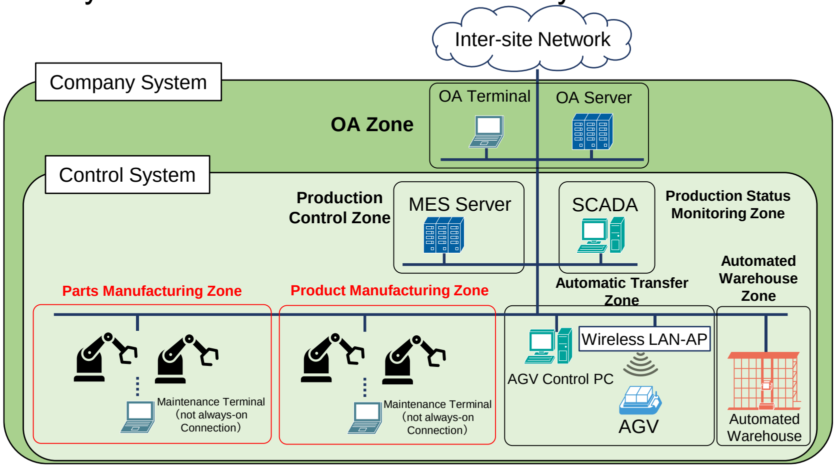


Figure C-2 Details of zones in case (1)

2. Add a new service to the existing zone, and check the data flow

In this case, a new service is introduced, which can automatically operate the parts manufacturing zone based on the CAD information. The CAD and dedicated servers required for the service are installed as part of the OA system. New data flow is assumed to be as follows.

- CAD sends its data to SCADA
- Send instructions from SCADA to the parts manufacturing zone according to CAD data

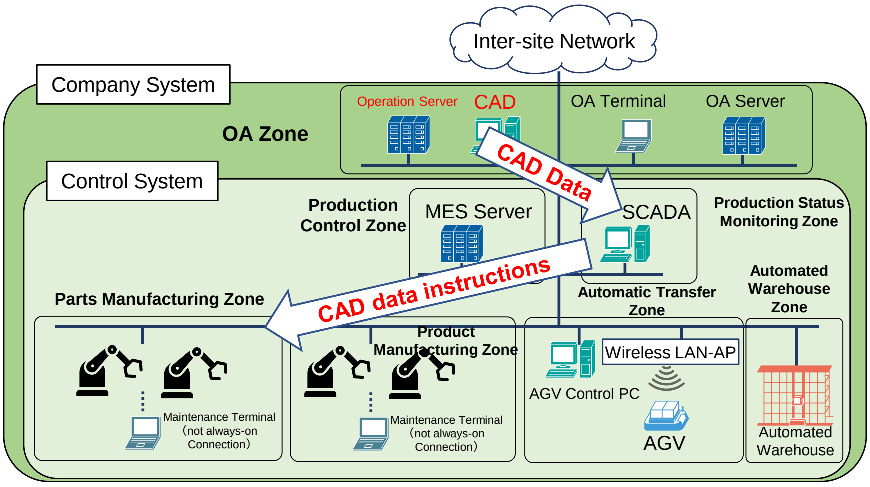


Figure C-3 Organization of new services and data flow in case (1)

3. <u>Review zoning based on the relationship between new services and operations</u>

   In this case, the CAD data can directly operate the parts manufacturing zone without human intervention. Therefore, this zone needs to meet other security requirements and is divided from the OA zone which does not send control instructions.

   In addition, it is necessary to review security requirements between zones since data related to control instructions is transmitted and received.

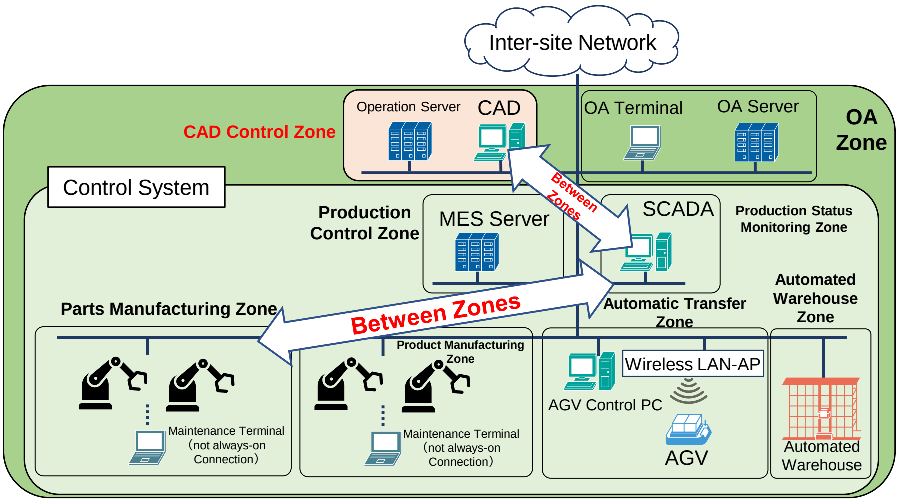


Figure C-4 Security between the new zone and the zone to be considered in case (1)

② Use of external remote maintenance services in automated warehouses

1. Divide factory zones from a viewpoint of operations
   It is possible to further divide the production zone based on the viewpoint of operations. For this case, however, it does not apply and will be treated as a single production zone.

2. Add a new service to the existing zone, and check the data flow
   In this case, an external remote maintenance service is introduced for an automated warehouse. Add a new service as part of the automated warehouse zone, as it will be connected with automated warehouse operations
   The data flow is assumed as follows:
   - Data and inventory status of incoming and outgoing items are sent from the automatic warehouse to the remote maintenance service.

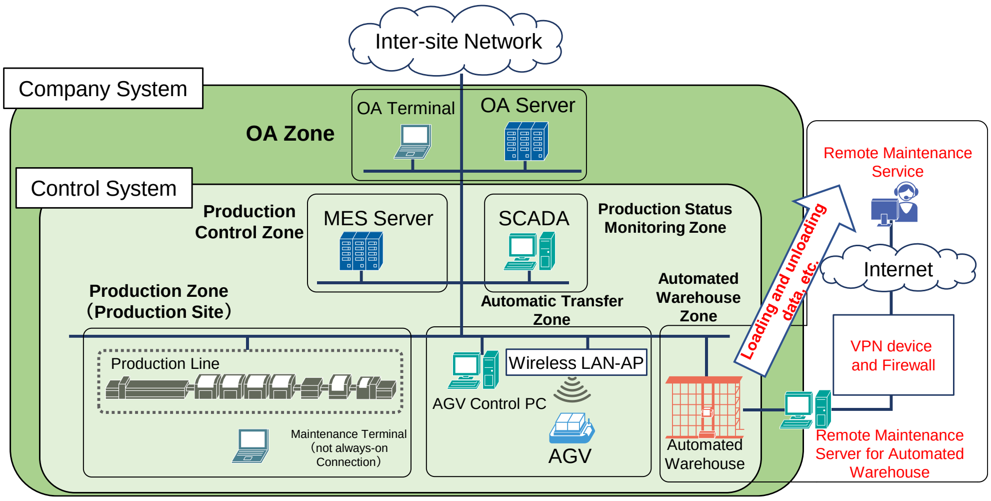


Figure C-5 Organize new services and data flow in case (2)

3. Review zoning based on the relationship between new services and operations
   This case involves the use of external services, which makes it difficult to request security requirements similar to those for the automated warehouse zone from the external service provider. Therefore, the remote maintenance service is separated from the automated warehouse zone. When separating the zone, it is important to consider the boundary of the separation. It is necessary to check the division of responsibility when considering the boundary of the separation.
   It is necessary to review the security requirements between different zones to guarantee the safe transmission and reception of sensitive data, such as inventory and in-and-out data.
   ※ This example assumes the use of an external service, so it was set as a separate zone. However, it is not necessary to make all services into separate zones. For example, the following cases can be categorized as similar zones.
   - Introduce a cloud service (private cloud) into enterprise systems
   - Necessary security measures are included in the external cloud service contract.

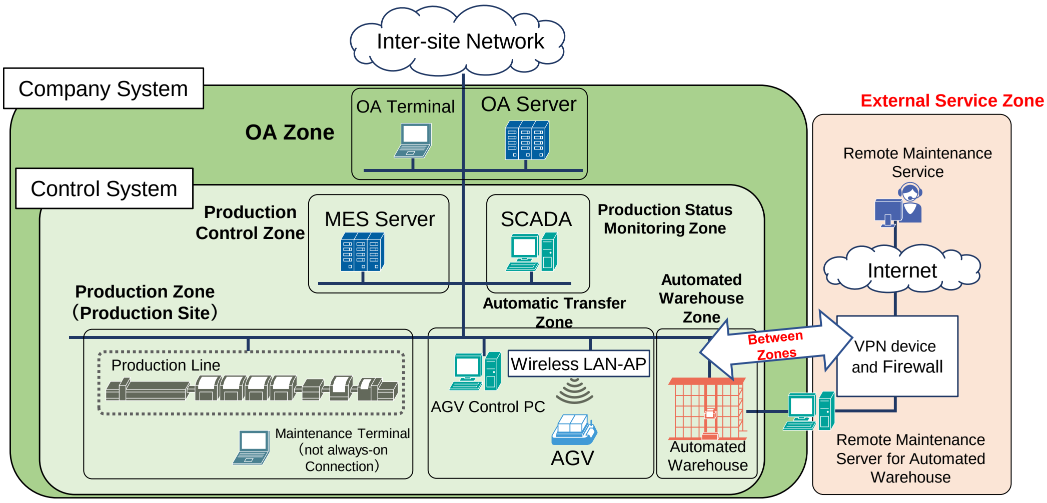


Figure C-6 Security between the new zone in case (2) and the zone to be reviewed

③ Improved efficiency of production monitoring functions by upgrading MES servers

1. Divide factory zones from a viewpoint of operations

In this case, the production zone was divided into the following two zones based on a detailed analysis of operations, a viewpoint that differs from a conventional factory approach.

- Parts manufacturing zone
- Product manufacturing zone

* This example shows the case of the processing and assembly industry, which the production zone can be divided in detail based on operations. On the other hand, it can be challenging to divide production zones in the material industry due to the operational process. Each company and factory need to be examined individually.

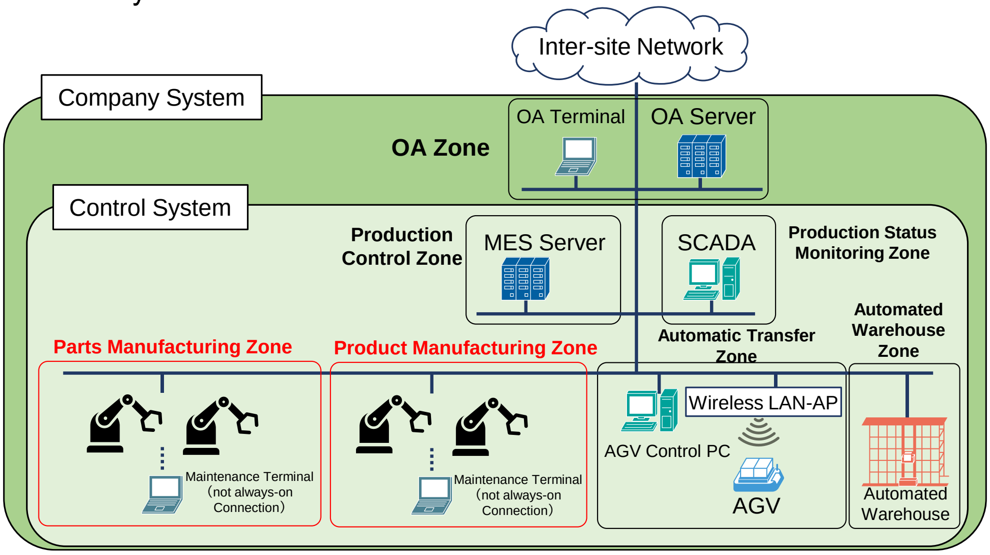


Figure C-7 Details of zones in case (3)

2. Add a new service to the existing zone, and check the data flow

In this case, the MES server will be upgraded and new data will be obtained from each production zone. Upgrading existing functions eliminates the need to set a new zone, but a new data flow is assumed as follows.

- Send new production status data from the parts manufacturing zone and the product manufacturing zone to the production management zone

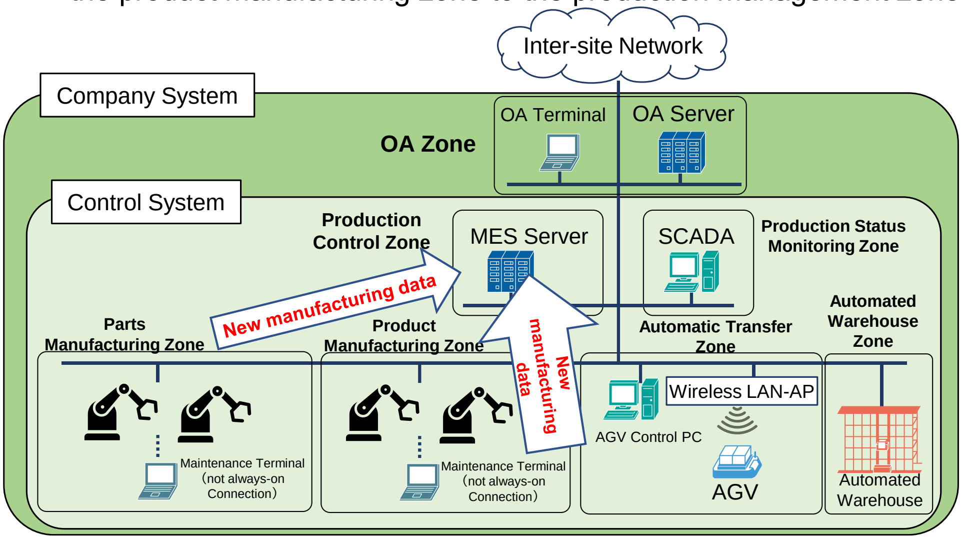


Figure C-8 Organize new services and data flow in case (3)

3. Review zoning based on the relationship between new services and operations
   In this case, new sensitive information is sent to the production management zone. Therefore, it is not necessary to change the zoning. Instead, the security requirements of the production management zone should be reviewed.
   In addition, it is necessary to examine security requirements between different zones as new manufacturing data is sent and received.

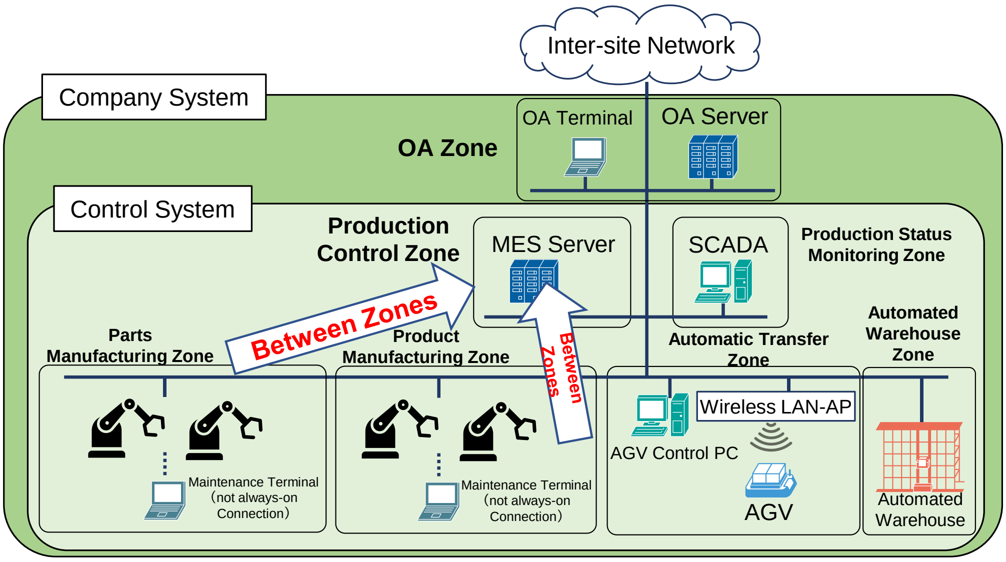


Figure C-9 Security between the new zone and the zone to be reviewed in case (3)

Annex B Reference guidelines for each step

Here are the reference guidelines for each step to consider security measures, based on the concept of this separate volume. If needed, it is suggested to refer to the appropriate source.

Step	Reference guidelines
Step 1:	● "Smart Factory Roadmap" -Toward the realization of manufacturing in line with the Fourth Industry Revolution- by the Chubu Bureau of the Ministry of Economy, Trade and Industry (https://www.chubu.meti.go.jp/b21jisedai/report/smart_factory_roadmap/roadmap.pdf) ● Guideline for Establishing Safety Principles for Ensuring Cyber Security of Critical Infrastructure Protection, by National Center of Incident Readiness and Strategy For Cybersecurity (NISC) (https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf) ● Basic Guidelines for Securing the Stable Provision of Specified Social Infrastructure Services by Preventing Specified Interfering Activities, by the Cabinet Office (https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf) ● Security Risk Assessment Guide for ICS, by IPA (https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf) ● Security Risk Assessment Survey on Smart Factories, by IPA (https://www.ipa.go.jp/security/controlsystem/ug65p90000019e7c-att/000098863.pdf)
Step 2:	● Examples of system security measures for smart factories, by Information-technology Promotion Agency, Japan (IPA) (https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html) ● Cyber/Physical Security Framework '(CPSF) by the Ministry of Economy, Trade and Industry (METI) (https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html) ● NIST、NIST Cybersecurity Framework (https://www.nist.gov/cyberframework)
Step 3:	● Guidance on Secure Use of Cloud Services for Small and Medium Enterprises by IPA (https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf) ● Information Security Management Guidelines for Using Cloud Services by METI (https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf) ● Guidance for the Introduction of SBOM (Software Bill of Materials) for Software Management Ver. 1.0 by METI (https://www.meti.go.jp/press/2023/07/20230728004/20230728004-1-2.pdf) ● Industrial Cyber Security Study Group Working Group 3 (Commission for Establishment of Security Conformity Assessment System for IoT Products) , The Ministry of Economy, Trade and Industry (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html)

Council of this Guideline

Study Group for Industrial Cybersecurity WG1
(Systems, Technologies and Standardization)
Factory SWG members
* Honorific titles omitted, in alphabetical order, as of March 29, 2024

Akihiko Iwasaki	Senior Manager for Security Japan Electronics and Information Technology Industries Association
|Chair| Hiroshi Esaki	Professor Graduate School of Information Science and Technology The University of Tokyo
Hiroshi Sasaki	Director Business Development Fortinet Japan G.K.
Hirotada Takahashi	Senior Manager OT Security Business Trend Micro Incorporated
Ichiro Murase	Executive Director Technology Research Association Control System Security Center
Kenji Watanabe	Professor Nagoya Institute of Technology Department of Architecture, Civil Engineering and Industrial Management Engineering
Kouichi Saita	Manager IT Division, Information System Department FANUC CORPORATION
Masahiko Kuwata	Director Security Business Department NEC Corporation
Masue Shiba	Chief Specialist Cyber Security Technology Center Toshiba Corporation
Takeo Enomoto	Member of Specialized Committee on Electrical and Safety Standards Standardization Subcommittee Technical Committee Japan Machine Tool Builders’ Association（JMTBA） (Manager, NAGOYA WORKS, Drive system Dept. MITSUBISHI ELECTRIC CORPORATION)
Takeshi Fujiwara	Vice General Manager Machine Tool Control Development Division Connectivity Department
Toshihiko Nakano	Security Evangelist Control System Platform Division Hitachi, Ltd. Visiting Professor Nagoya Institute of Technology
Yuji Ichioka	General Manager

	FA Software Systems Dept., Nagoya Works, Mitsubishi Electric Corporation
Yutaka Matsubara	Associate Professor Nagoya University Graduate School of Informatics

Study Group for Industrial Cybersecurity WG1
(Systems, Technologies and Standardization)
Factory SWG task force members
※ Honorific titles omitted, in alphabetical order, as of March 29, 2024

<Core members>

Hiroshi Sasaki	Director Business Development Fortinet Japan G.K
Hirotada Takahashi	Senior Manager OT Security Business Trend Micro Incorporated
Ichiro Murase	Executive Director Technology Research Association Control System Security Center
Katsunari Oobayashi	Professional Security Business Department NEC Corporation
|Subcommittee Chairperson|	
Kenji Watanabe	Professor Nagoya Institute of Technology Department of Architecture, Civil Engineering and Industrial Management Engineering
Kouichi Saita	Manager IT Division, Information System Department FANUC CORPORATION
Masahiko Kuwata	Director Security Business Department NEC Corporation
Masue Shiba	Chief Specialist Cyber Security Technology Center Toshiba Corporation
Nori Matsuda	General Manager Information Security Technology Dept., Information Technology R&D Center MITSUBISHI ELECTRIC CORPORATION
Taiga Okayama	Professional Security Business Department NEC Corporation
Toshihiko Nakano	Security Evangelist Control System Platform Division Hitachi, Ltd. Visiting Professor Nagoya Institute of Technology
Yohei Ogawa	Senior Specialist Security Business Department NEC Corporation
Yoichi Shibata	Head Researcher Information Security Technology Dept., Information Technology R&D Center MITSUBISHI ELECTRIC CORPORATION

<Members>

Hiroki Tamada	Associate General Manager Production Technology Division MITSUBISHI GAS CHEMICAL
Hironori Asahina	Senior Manager OT Security Business Development Dept. MITSUBISHI ELECTRIC CORPORATION
Katsutoshi Suzuki	Associate General Manager Maintenance Technology Department Production Technology Division MITSUBISHI GAS CHEMICAL
Masaharu Nozawa	Deputy General Manager Cyber Security Center TEPCO Power Grid, Inc
Masahiko Katsuta	Manager Digital Systems & Services Division Hitachi, Ltd.
Megumi Kinoshita	Chief Researcher IT Security Center, IT Security Countermeasures Department Information technology Promotion Agency, Japan
Motohiro Tamura	Associate General Manager Information Systems Division MITSUBISHI GAS CHEMICAL
Noriaki Gotoh	Manager Information System Division Mitsui Chemicals Inc.
Taisuke Kobayashi	Cyber Security Management Dept. JFE Steel Corporation
Takeshi Yabiku	Information Systems Division MITSUBISHI GAS CHEMICAL
Tomoshige Nagamatsu	Associate General Manager Process Technology Department Production Technology Division MITSUBISHI GAS CHEMICAL
Toshiro Fujii	Director Information Security Department Tokyo Electron Limitid
Cisco Systems G.K.	