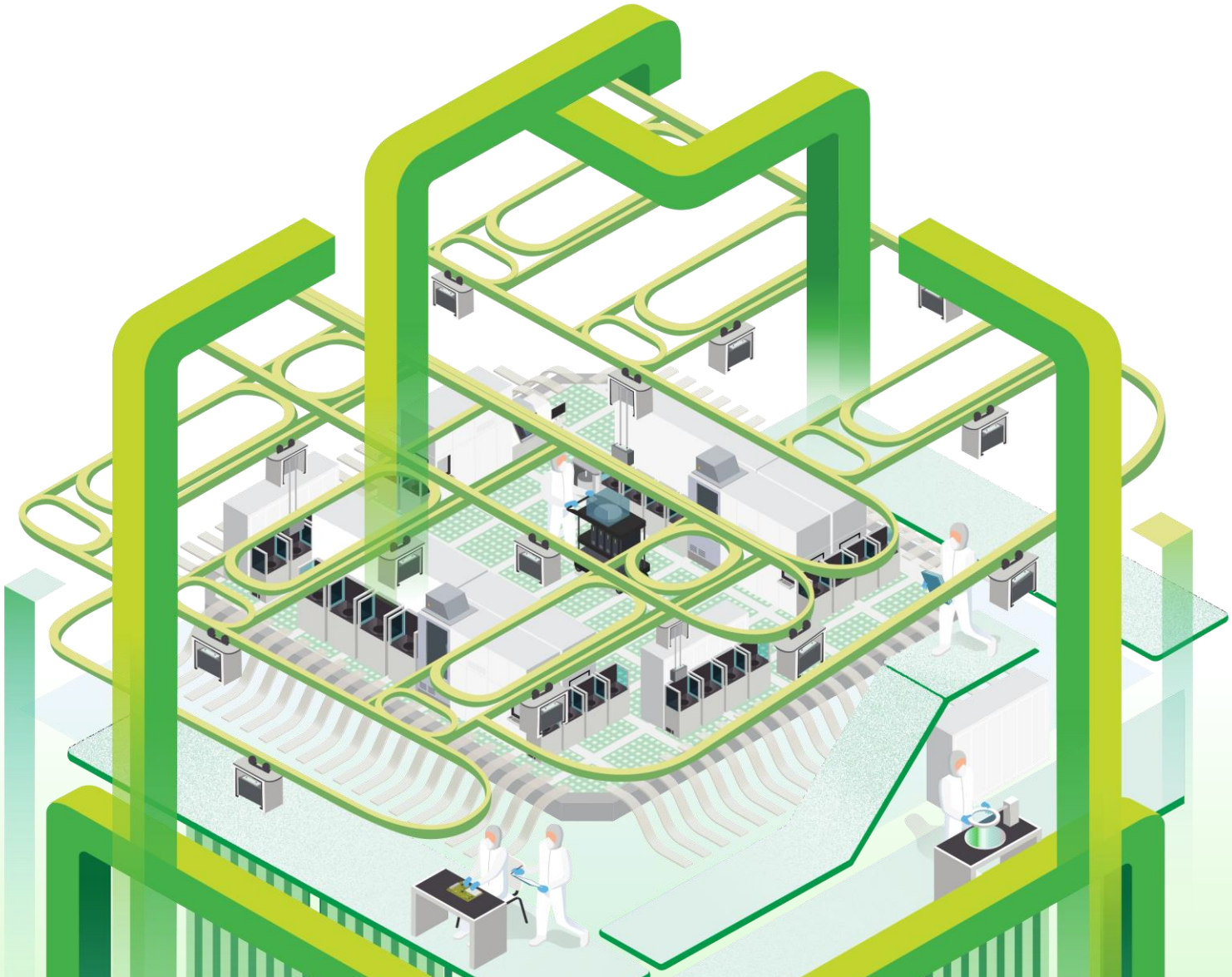
OT Security Guidelines for Semiconductor Device Factories

Ver 1.0



October 24, 2025

Study Group for Industrial Cybersecurity
Working Group 1 (Strengthening Effectiveness and International Collaboration)
Semiconductor Industry Sub-Working Group

Change History

Issue date	Version	Overview
October 24, 2025	Ver1.0	Ver1.0 issued

Table of Contents

1 Background and Purpose of These Guidelines 1

1.1 Background and Purpose 1
1.2 Target Audience of These Guidelines (Intended Readers) 2
1.3 What to Protect Against Cyberattacks During Semiconductor Production 3
1.4 Threats and Risks in Semiconductor Manufacturing Processes 4
1.5 Assumed Attack Actors 5
1.6 Security Measures and Utilization of These Guidelines in Semiconductor Device Factories 6
1.7 Structure of These Guidelines 7

2 Reference Architecture for Semiconductor Device Factories 8

2.1 Reference Architecture for Semiconductor Device Factories 8
2.2 Utilization of the Purdue Model 11
2.3 Utilization of the CPSF's Three Layers 13

3 Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories 15

3.1 Organization into Security Measures Utilizing the Reference Architecture 15
3.2 Risk Analysis Information for Each Area of the OT Zone from the Technical and Physical Aspects of Semiconductor Device Factories 19

3.2.1 Risk Analysis Information for the OT Zone's Fab Area 21
3.2.2 Risk Analysis Information for the OT Zone's Fab System Area 37
3.2.3 Risk Analysis Information for the OT Zone's External Services and the IT/OT DMZ's Separation Control ..... エラー! ブックマークが定義されていません。

3.3 Risk Analysis Information for the Organizational and People Aspects in Semiconductor Device Factories 49

4 Examples of Specific Measures for Semiconductor Device Factories 60

4.1 Asset Management and Vulnerability Assessment of Equipment/Tools 60

4.1.1 Determining the Identification and Configuration Management of Assets (Equipment/Tools) 61
4.1.2 Determining the Degree of Importance of Assets (Equipment/Tools) 64
4.1.3 Methods for Identifying the Vulnerabilities of Equipment/Tools 72
4.1.4 Methods for Collecting Information on Threats to Equipment/Tools エラー! ブックマークが定義されていません。
4.1.5 Vulnerability Assessment of Equipment/Tools and Methods for Determining Response Priority Levels 75

4.2 Additional Defense Measures to Minimize Equipment/Tool Damage and to Prepare for

Early Recovery 77
4.3 Operations (Monitoring, Response, Recovery, and Improvement): FSIRT Operations. 82
4.4 Physical Access Restrictions (People Entering/Bringing Objects in/Making Connections): Physical Measures in the Fab Area 92

Appendix A: Comparison chart of NIST's CSF2.0 and CPSF 96
Appendix B:Glossary/Abbreviations 114
Council of these Guidelines 124

1 Background and Purpose of These Guidelines

1.1 Background and Purpose

Cyberattacks have increasingly becoming diverse and sophisticated, and various control systems with operational technology (OT) have been attacked, causing serious damage such as interruptions of factory production. Additionally, there is also an increasing risk that various confidential information for development (i.e., intellectual property) could be leaked through cyberattacks. Considering the economic and national security importance of the semiconductor industry and the growing cyber threats and risks at present, it is imperative to implement and strengthen security measures, including countermeasures against advanced cyberattacks. This movement is not only starting in Japan, but in many other countries globally as well. The global semiconductor industry association SEMI has formulated E187[1]/E188[2] as a standard for semiconductor manufacturing equipment, and the National Institute of Standards and Technology (NIST) is working on the development of a semiconductor manufacturing profile for its Cybersecurity Framework 2.0 (hereinafter referred to as NIST CSF 2.0)[3].

On the other hand, comprehensive framework for promoting security measures across the entire semiconductor industry has not yet been established in Japan. Therefore, it is urgent to present guidelines for factory security measures by taking into account the status of security measures being implemented within the domestic semiconductor industry and other relevant factors, while maintaining consistency with various security standards that have been established for the global semiconductor industry.

The Ministry of Economy, Trade and Industry has drawn up and issued the Cyber/Physical Security Guidelines for Factory Systems, which are tailored for generic factories that conduct assembly operations. However, semiconductor factories are generally close to the process automation (PA) factories, which are large in scale and have a significant number of manufacturing tool equipment using generic operating systems (OS). Therefore, these Guidelines have been newly formulated specifically for semiconductor device factories.

[1] https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment
[2] https://store-us.semi.org/products/e18800-semi-e188-specification-for-malware-free-equipment-integration
[3] https://www.nist.gov/cyberframework

1.2 Target Audience of These Guidelines (Intended Readers)

Since semiconductor production is comprised of a complex supply chain that includes materials, design, and production (Covering both the pre- process and post- process), the entire supply chain must be protected in order to maintain a stable supply of semiconductors. Therefore, there is a need to pour effort into improving the overall level of cybersecurity measures for all semiconductor industries. These Guidelines aim to enhance security measures for the factories of device manufacturers as a first step. For this reason, the intended readers are primarily personnel working in the manufacturing departments of device manufacturers. Meanwhile, since there are many production tool equipment manufacturers and materials manufacturers in Japanese semiconductor industry, another goal of these Guidelines is to enable such manufacturers to understand what is required of them and to formulate their own measures.

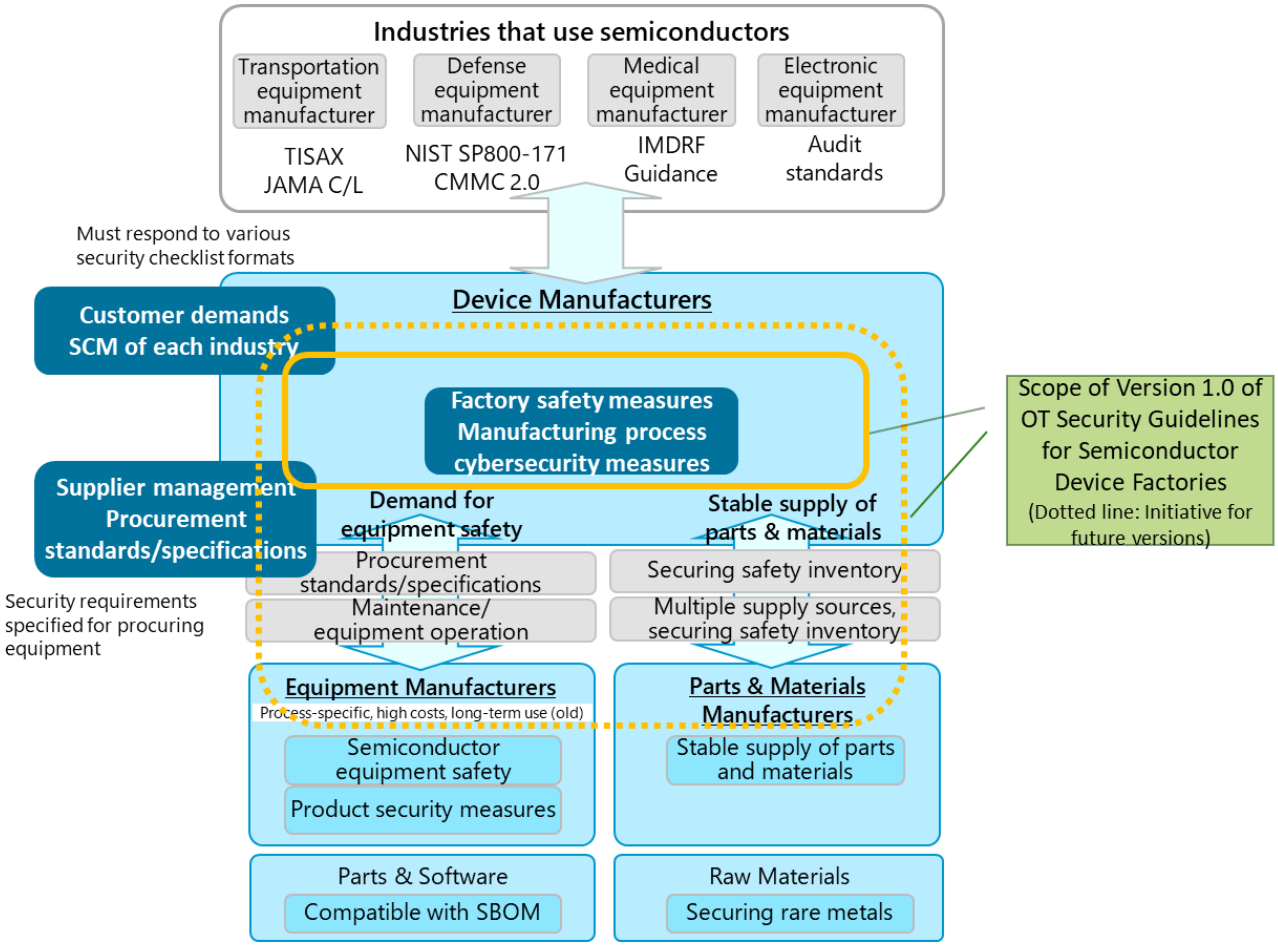


Figure 1-1. Supply Chain of the Semiconductor Industry

1.3 What to Protect Against Cyberattacks During Semiconductor Production

The following five items are listed in NIST's CSF 2.0 Semiconductor Manufacturing Profile as items that must be protected in order to maintain a stable supply of semiconductors.

- Maintain Production Goals (supply responsibilities)
  Manage cybersecurity risks that may negatively impact production goals, throughput, and yields, such as asset damage or unplanned downtime of production lines and equipment. The interdependencies between cybersecurity and production goals must be understood.
- Protect Confidential Information
  Manage cybersecurity risks that may lead to the loss or infringement of the organization's intellectual property, highly confidential data, or regulated data, including information related to semiconductor fabs, Original Equipment Manufacturing (OEM) equipment, and across the entire supply chain.
- Maintain the Quality of Semiconductors
  Manage cybersecurity risks that could negatively impact product quality and production process. One must ensure that the integrity of the semiconductor manufacturing process, OEM equipment, and relevant data across the supply chain is maintained.
- Maintain Environmental Safety
  Manage cybersecurity risks that may negatively impact the environment, such as accidental or intentional damage. One must understand the interdependencies of cybersecurity and environmental safety.
- Maintain Human Safety
  Manage cybersecurity risks that may impact human safety. One must understand the interdependencies between cybersecurity and human safety.

In consideration of economic and national security, these Guidelines especially focus on the following three items among the above items that must be protected: "Maintain Production Goals" (supply responsibilities); "Protect Confidential Information;" and "Maintain the Quality of Semiconductors."

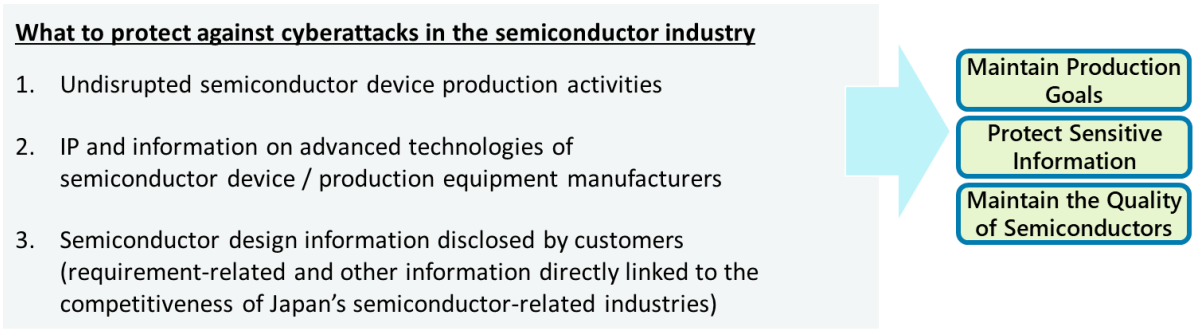


Figure 1-2. What to Protect Against Cyberattacks in the Semiconductor Industry

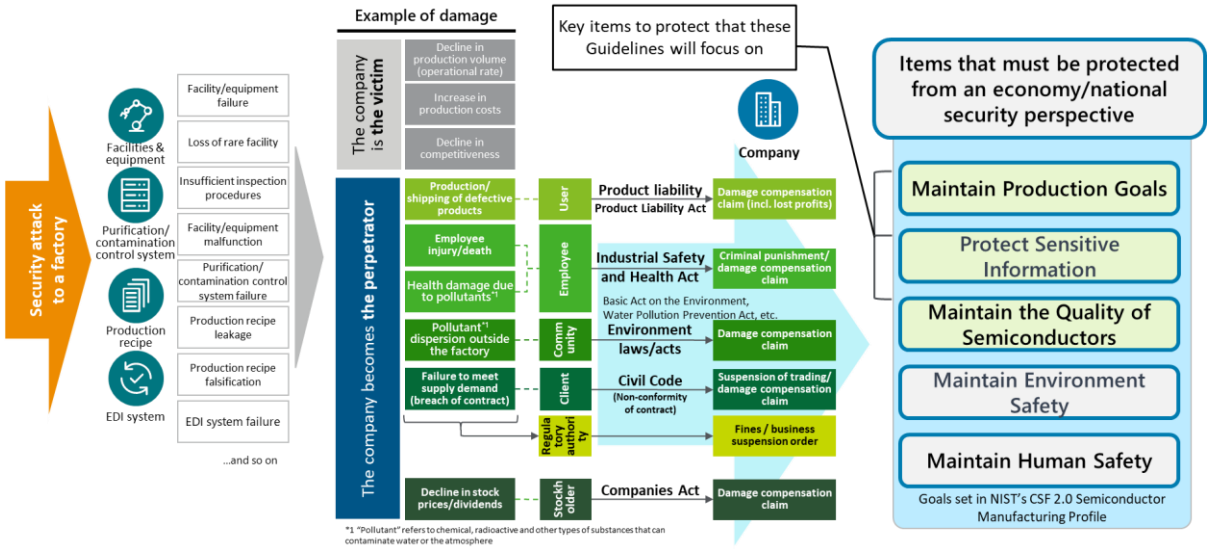


Figure 1-3. Items That Must Be Protected During Semiconductor Production

1.4 Threats and Risks in Semiconductor Manufacturing Processes

The manufacturing process in a semiconductor device factory is largely divided into four stages: the wafer manufacturing process, the photomask manufacturing process, the pre-process, and the post-process. In each process, if cyberattacks occur and cause damage, there is a possibility that they may poses significant risks to the protection of confidential production information and the fulfillment of supply responsibilities.

Confidential production information, for example, includes design information used in the photomask manufacturing process, information on miniaturization technologies and recipes/production processes aimed at yield enhancement in the pre-process stage, as well as production technology information related to layering post-process stage. This type of information is highly confidential (Figure 1-4: "Confidential production information" colored in green). If an infringement causes a leakage of intellectual property, there is a risk that the company will be placed at a disadvantage in the development competition and other types of competitions with competitors.

Each company usually maintains before and after each process, and safety inventory levels based on supply responsibilities and business continuity plans

are taken into account. There is a risk that damage caused by cyberattacks could interrupt production, causing inventories to drop below the safety inventory levels for each process. This would then result in the company's inability to fulfill its supply responsibilities (Figure 1-4: "Inventory" colored in blue).

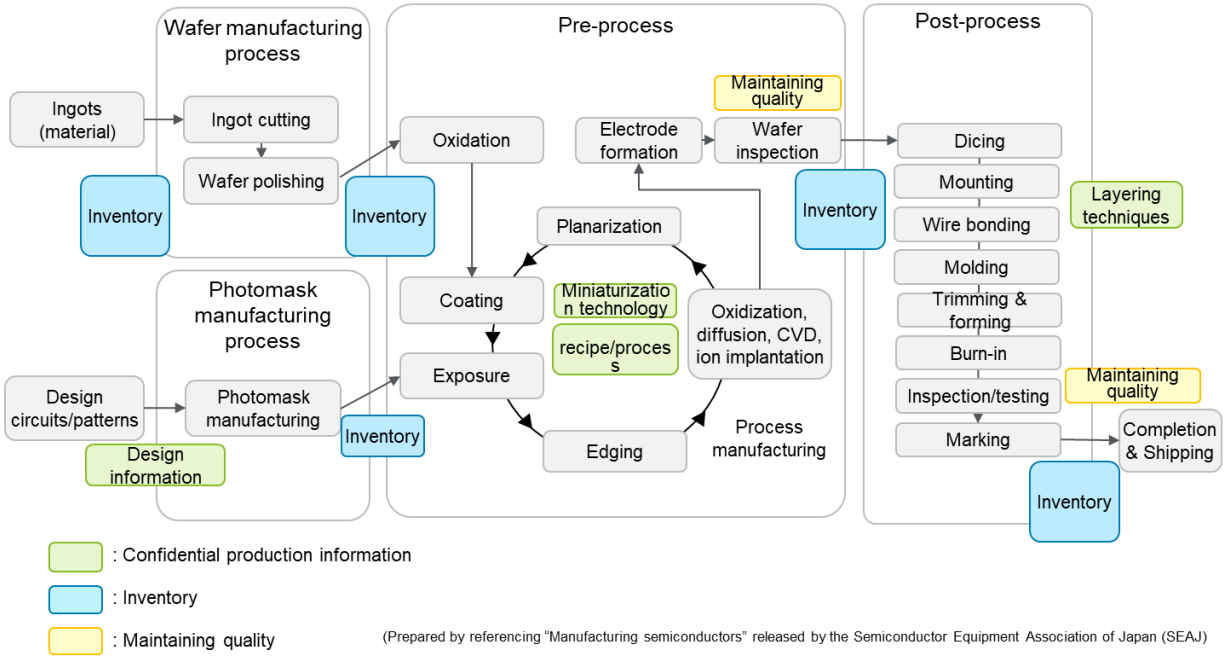


Figure 1-4. Semiconductor Manufacturing Processes

1.5 Assumed Attack Actors

The actors who carry out cyberattacks are generally classified into the following five categories, and the technical level of the attacker is believed to be varied according to the type of attacker. Due to the importance of the entire semiconductor manufacturing supply chain from a national security perspective, a level of measures must be implemented in preparation for the most sophisticated attackers ((1) below) (i.e., SL4 in IEC 62443).

(1) Nation-state cyber actors (APT - Advanced Persistent Threat Attack)):
Characterized by implementing tenacious, sophisticated, and continuous attacks (i.e., an attack group that prioritizes mission achievement without giving thought to the costs incurred).

(2) Cybercriminals (crime-related):
Groups that steal information, data, etc. and draws out cash.

(3) Hacktivists:
A combination of the words, "activist" and "hacker," which refers to a group that focuses on sending out social or political messages by conducting cyberattacks.

(4) Malicious individuals (e.g., criminal for pleasure and trial of skill):

These attacks are carried out by individuals as an extension of their hobbies or research. The attackers are children in many cases.

(5) Industrial spies

Groups that aims to steal intellectual property.

Table 1-1. IEC62443's Security Levels (SL)

Security level	Definition
SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL3	Protection against intentional violation using sophisticated means with moderate resources IACS specific skills and moderate motivation
SL4	Protection against international violation using sophisticated means with extended resources, IACS specific skills and high motivation

*IACS(Industrial Automation Control System)

1.6 Security Measures and Utilization of These Guidelines in Semiconductor Device Factories

In order to achieve the objective of protecting the semiconductor supply chain, cybersecurity measures must be implemented to enable each relevant company to fulfill its supply responsibilities, and they must be consistent with the relevant company's Business Continuity Plan (BCP).

In order to fulfill their supply responsibilities and associated accountability, the company must first conduct a risk assessment and then consider, design, and implement appropriate measures based on the results of the assessment.

These guidelines provide fundamental principles and specific guidance for the integrative protection of cyberspace and physical space through the Cyber-Physical Security Framework[4] (hereinafter referred to as CPSF), as well as risk-based frameworks such as NIST CSF 2.0. It can be utilized as a reference when conducting risk analysis and considering security measures. For specific risk analysis methods for control systems with operational technology in factories, refer to the Information-technology Promotion Agency, Japan's (IPA) Guide for Security Risk Analysis of Control Systems[5].

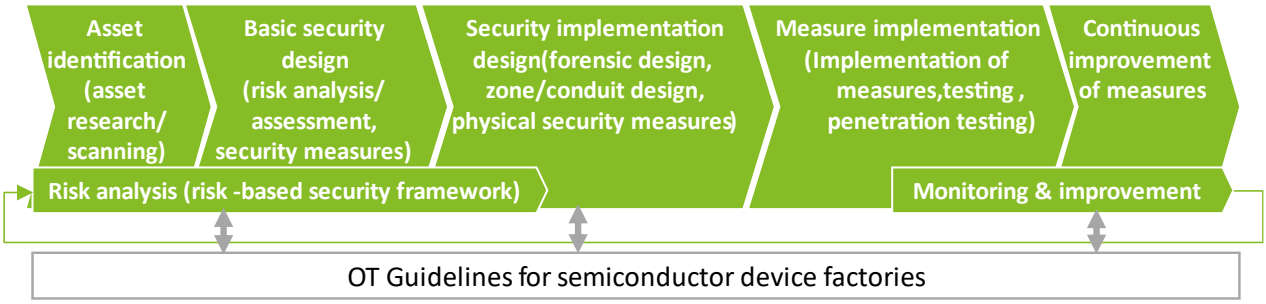


Figure 1-5. Utilization of These Guidelines In the Security Construction Process of Semiconductor Device Factories

[4] https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
[5] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

1.7 Structure of These Guidelines

These Guidelines search for and identify risk sources in semiconductor device factories based on the concept of the Cyber/Physical Security Framework (CPSF) and link the relevant parts of NIST's CSF 2.0 Semiconductor Manufacturing Profile[6] (Published on February 27, 2025, Version) and SEMI E187 - Semiconductor Manufacturing Reference[7] with the measures to counter those risk sources.

(1) Utilizing IEC 62443's[8] Purdue Model, semiconductor device factories are divided into zones and areas, and the six elements of the CPSF for each area are searched for and identified (Chapter 2).

(2) Characteristics of semiconductor device factories related to the aforementioned six elements of the CPSF are organized. Risk sources caused by these characteristics are searched for and identified utilizing the CPSF and are then linked to NIST's CSF 2.0 Semiconductor Manufacturing Profile (Chapter 3).

(3) More detailed examples of measures/methods are introduced for initiatives that are particularly important for semiconductor device factories, such as microsegmentation (Chapter 4).

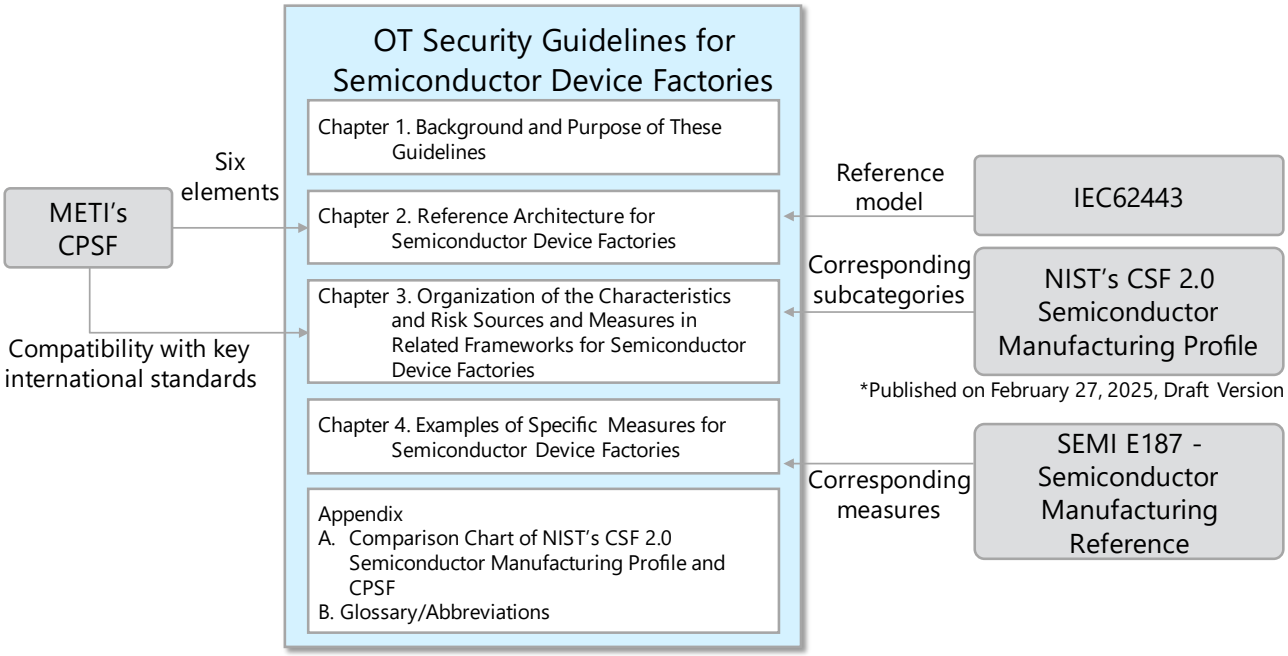


Figure 1-6. Structure of These Guidelines and Their Relationship with Domestic and Foreign Standards

[6] https://csrc.nist.gov/pubs/ir/8546/ipd
[7] https://www.txone.com/blog/unveiling-semi-innovative-cybersecurity-architecture/
[8] https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards

2 Reference Architecture for Semiconductor Device Factories

2.1 Reference Architecture for Semiconductor Device Factories

Chapter 2 organizes and explains the reference architecture for semiconductor device factories (Figure 2-1, Table 2-1) with the aim of making it easier to examine security measures to “Maintain Production Goals” (supply responsibilities), “Protect Confidential Information,” and “Maintain the Quality of Semiconductors,” which are three items that must be protected from cyberattacks as defined in Section 1.3.

(1) The Purdue Model, an architecture designed for industrial control systems (ICS), is applied to generic semiconductor device factories. Specifically, the main areas of a factory are segmented into the IT zone, OT zone, and IT/OT Demilitarized Zone（DMZ）, and then each area is linked to a level (L) ranging from either 0 to 4 or 0 to 5. This segmentation makes it easier to organize security requirements for each area.

(2) Following this, the CPSF is applied to identify risks while taking into account the characteristics of semiconductor device factories and to organize security measures against such risks. A semiconductor device factory is divided into the CPSF’s three layers, and simultaneously the CPSF’s six elements (Organization, People, Components, Data, Procedure, System) are identified.

While taking into account the characteristics of semiconductor device factories, Chapter 3 identifies and enumerates security incidents to be assumed (threats, vulnerabilities, vulnerability IDs) based on the reference architecture for semiconductor device factories and then links them to relevant items in NIST’s CSF 2.0 Semiconductor Manufacturing Profile as security measures to mitigate them. As a result, it is now possible to organize examine the identified risk sources found in semiconductor device factories and measures to mitigate them based on NIST’s CSF2.0 Semiconductor Manufacturing Profile.

Note that this reference architecture is merely an example prepared for typical semiconductor device factories. Therefore, companies should refer to these Guidelines to structure and organize the reference architecture of their own factories, clarify the characteristics of their factories, and identify all possible risk sources. If necessary, it is essential to link those risk sources to relevant items in NIST’s CSF 2.0 Semiconductor Manufacturing Profile.

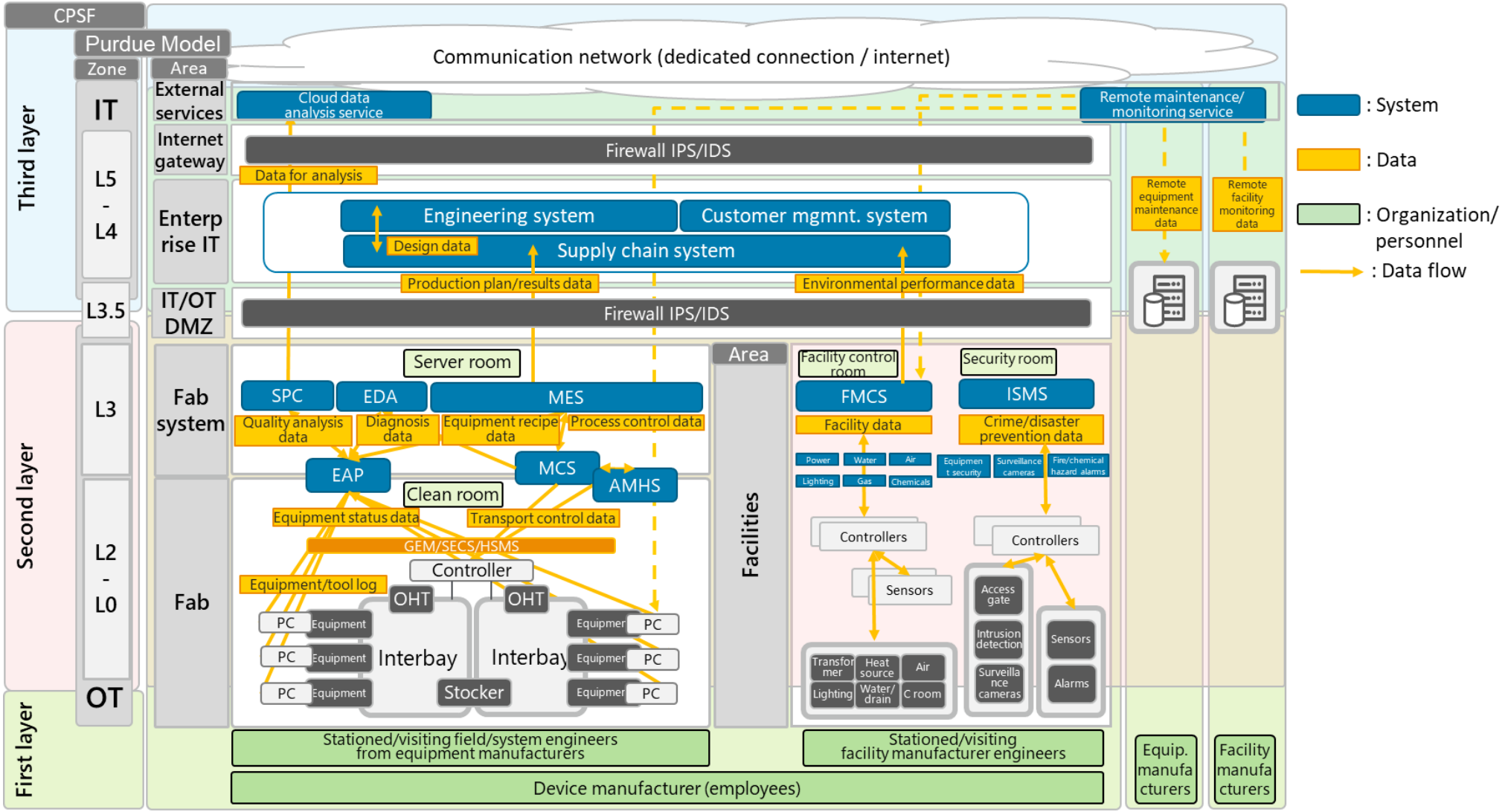


Figure 2-1. Reference Architecture of Semiconductor Device Factory

Table 2-1. The Purdue Model and the CPSF's Six Elements

Purdue Model		CPSF's six elements					
Zone		System	Data	Components	Procedure	Organization and People	
						Device manufacturer	Partner
External service		Cloud data analytics service	Cloud analysis data	Service	Conduct the process for using cloud services via the internet as well as the process for receiving remote monitoring and maintenance services from equipment/facility manufacturers	• The IT Department plays a central role in security management via the internet (including remote access)	• Cloud service provider • Facility manufacturer • Equipment manufacturer
		Remote monitoring and maintenance service	Remote monitoring and maintenance data				
Internet gateway		Internet gateway (RAS)	Communication control data outside the organization	Firewall, IPS/IDS, etc.	Control communications made with the internet and external services	• The IT Department plays a central role in managing the security of the entire enterprise • Design, procurement, sales, HR, book-keeping, administration, etc.	• Outsourcing companies for each department
IT	Enterprise (L4-5)	SCM, ECM, CRM	SCM, ECM, and CRM data	Server, network, PC, smartphone, MFP, etc.	Conduct the IT operation (SCM, ECM, and CRM) process in the semiconductor manufacturing company		
IT/OT DMZ (L3.5)		IT/OT DMZ	Communication control data inside the organization	Firewall, IPS/IDS, etc.	Control communications made between the IT operation and OT operation processes		
OT	Fab system (L3)	MES	Production progress data	Server, storage, network	Conduct the semiconductor manufacturing process, and conduct the quality control process	• The Manufacturing Department plays a central role in managing production, including its security • Quality assurance, process technology, production technology, manufacturing system, etc.	• System service company
		SPC	Quality characteristics/analysis data				
		EDA	Equipment collection/process diagnostic data				
	Fab (L0-2)	EAP	Optimum process flow [confidential], equipment status data, recipe [confidential], transportation/lot control data, lot optimization logic	Equipment/tool (manufacturing, inspection, and measurement), OHT, OHS, stocker, FOUP	Conduct the process using each manufacturing equipment, control transportations made within a process or between multiple processes, and conduct communications via industry-standard GEM/SECS		• Equipment manufacturer • A field engineer is assigned on-site, and an office is available
		AMHS					
		MCS					
	Facility (L0-3)	FMCS	Facility data, environmental data	Each facility, controller, sensor	Conduct the operation/management process for the facility environment for clean rooms used to manufacture semiconductors and for each semiconductor manufacturing equipment	• The Facility Department plays a central role in managing factory facilities, including their physical security	• Equipment manufacturer • There are companies supplying electricity, water supply and drainage, gas, and chemicals, and an office is available
		ISMS	Crime-prevention data, disaster prevention data				

2.2 Utilization of the Purdue Model

Using the Purdue model, the security in a semiconductor device factory is classified into the following zones and areas.

(1) Zones

A factory can be divided into two zones: the IT zone, where enterprise operations are conducted, and the OT zone, where manufacturing operations are conducted. Furthermore, the two zones are separated by a DMZ. Their overviews and functions are as shown below.

- IT zone (Levels 4-5)

  Overview:

  A zone where devices used for office work (PCs, smartphones, printers, servers, etc.) are connected.

  Functions:

  Includes systems that are used to conduct core operations such as production planning, procurement, design, sales, and customer management.

  Areas:

  Includes the enterprise area and the internet gateway within the IT zone.

- OT zone (Levels 0-3)

  Overview:

  A zone where equipment/tools, production/control systems, and facilities are connected.

  Functions:

  Includes equipment/tool control, monitoring, data collection, and manufacturing systems.

  Areas:

  Includes the three areas of: the fab system area (which covers the manufacturing system); the fab area (which covers equipment/tools); and the facility area (which covers facilities).

- IT/OT DMZ (Level 3.5)

  Overview:

  A zone where a firewall separates and connects the IT zone and the OT zone.

  Functions:

  As a security gateway, it controls the communications made between both zones and provides protection from unauthorized access and attacks.

(2) Areas

The IT zone and OT zone of semiconductor device factories are further divided into the following areas based on function and security requirements. The characteristics of security measures are also described for each area of the OT zone.

- IT zone
  - Internet gateway (Level 5)

    Overview:

    A gateway that controls the communications between the enterprise area and the internet environment.

    Functions:

    Authorizes cloud-based communications, controls remote access made for the provision of remote maintenance/support, and provides protection from unauthorized access and cyberattacks from the internet.
  - Enterprise IT area (Levels 4-5)

    Overview:

    An area where employees carry out office work.

    Functions:

    Supply chain systems for production planning and procurement, engineering systems such as CAD and EDA used for designing circuits, and customer management systems for conducting sales, customer management, etc.
- OT zone
  - Fab system area (Level 3)

    Overview:

    An area in which the system that controls the process automation for the entire manufacturing process is placed.

    Functions:

    MES transmits data, such as production plan and results, to supply chain system located in the enterprise area via the DMZ. SPC utilizes cloud-based data analysis to perform faster and more accurate quality analysis. With the advancement of DX, communications from the fab system area to the internet are becoming increasingly common.

    Security measures:

    Although the same server/system measures as those implemented in the IT zone shall be implemented, vulnerability assessments and patch management need to be conducted for each system in the fab system area based on the assumption that said system will be essential for its continuous operation.
  - Fab area (Levels 0-2)

    Overview:

    An area consisting of an extremely sanitary cleanroom

environment, where equipment/tools using advanced technology are placed.

Functions:

These equipment/tools communicate in real-time with control systems such as EAP, MCS, and AMHS. These systems also communicate with MES, SPC, and EDA located in the fab system area.

Security measures:

The equipment/tools in the fab area have several security characteristics including the long-term use of general-purpose operating systems (even after the vendor's support has ended), the use of industry-standard communication protocols that lack encryption and authentication, a large number of equipment/tools due to the use of process automation, and the difficulty of applying patches because of continuous operation.

- Facility area (Levels 0-3)

Overview:

An area in which facility systems for each factory facility (e.g., electricity, water, gas, and chemicals), crime-prevention systems (e.g., security cameras and access control devices), and disaster-prevention systems (e.g., fire detectors) are placed.

Security measures:

As there are similar issues to those general building management systems (e.g., long-term use and multiple stakeholders), the same measures as those implemented for such systems are required.

2.3 Utilization of the CPSF's Three Layers

The CPSF's three-layer structure for semiconductor device factories indicates connections between companies, connections between physical space and cyberspace, and connections within cyberspace.

- First layer (Figure 2-1: Green)
  Indicates connections between companies (organizations/people), primarily focusing on semiconductor device factories.
  Depicts equipment manufacturers and facility manufacturers that support facilities and equipment/tools used in the fab of device factories, as well as field engineers who regularly conduct maintenance in factories or visit factories to conduct maintenance.
- Second layer (Figure 2-1: Pink)
  Indicates connections between physical space and cyberspace within a semiconductor device factory.

This describes the connections from various tool groups installed in the OT zone fab area of the semiconductor device factory to fab systems such as MES, the connections of sensors and controllers within each facility in the facility area, and the connections of systems and data from the fab system area and facility area to the IT zone through the IT/OT DMZ.

- Third layer (Figure 2-1: Light blue)
  Indicates connections that take place within cyberspace when a semiconductor device factory uses external services.
  Depicts the use of data analysis services using cloud-based data analytics service and remote diagnosis services using e-Diagnostics technology provided by equipment manufacturers, among others.

3 Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories

3.1 Organization into Security Measures Utilizing the Reference Architecture

By utilizing the reference architecture defined in Chapter 2, Chapter 3 searches for and identifies security incidents to be assumed (threats, vulnerabilities, vulnerability IDs) based on the characteristics of semiconductor device factories and compiles the security measures of corresponding risk frameworks (i.e., the CPSF and the NIST CSF 2.0). Details of the compilation method are described in the following section.

In Chapter 3, these Guidelines can be used as reference materials for the implementation of risk analyses and the consideration of security measures utilizing risk-based frameworks such as the CPSF and the NIST CSF 2.0. Specifically, the following utilization methods are expected.

(1) Identify characteristics of the six elements of the CPSF, as organized in the reference architecture for semiconductor device factories, and organize the viewpoints to be considered when examining security measures
(2) Utilize the CPSF framework to organize security incidents to be assumed (threats, vulnerabilities, vulnerability IDs) from the viewpoints that must be considered, which is identified under (1)
(3) Based on the vulnerabilities organized in (2), relevant CPSF measure requirement IDs, subcategories of NIST's CSF 2.0 Semiconductor Manufacturing Profile, and/or relevant parts of SEMI E187 - Manufacturing Reference are extracted in accordance with their correspondence relationship with CPSF's major foreign standards, frameworks, and related aspects.

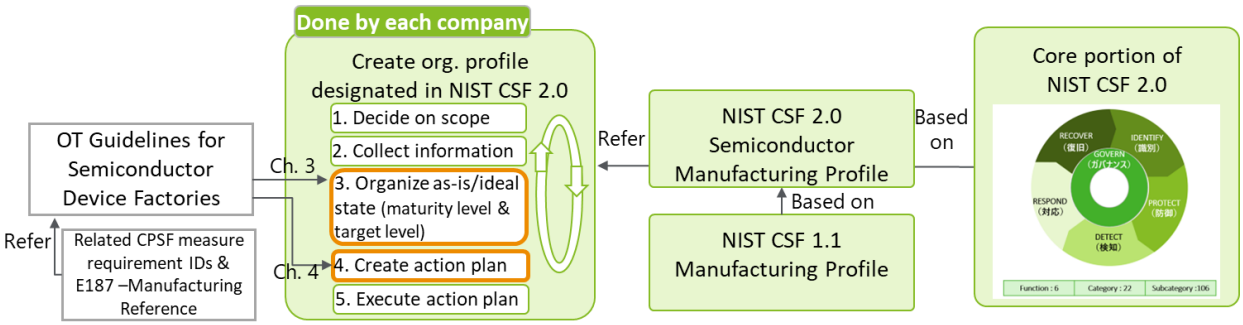


Figure3-1. Usage of These Guidelines

In Chapter 3, the scope of organizing the characteristics and risk sources of semiconductor device factories, as well as measures in related frameworks,

includes fab areas, fab system areas, IT/OT DMZs, and external systems classified by the Purdue Model, along with organizations and people.

Internet gateway and enterprise areas are not covered in Chapter 3 because the security measures implemented in those areas are not different from the security measures implemented in ordinary IT zones.

The facility areas within the OT zone are planned to be included in future revisions of these Guidelines, starting from the next edition, to ensure alignment with international standards currently under consideration.

Figure 3-2 shows the details of the risk analyses described in Section 3.2 “Risk Analysis Information for Each Area of the OT Zone from the Technical and Physical Aspects of Semiconductor Device Factories,” and Section 3.3 “Risk Analysis Information for the Organizational and People Aspects in Semiconductor Device Factories.”

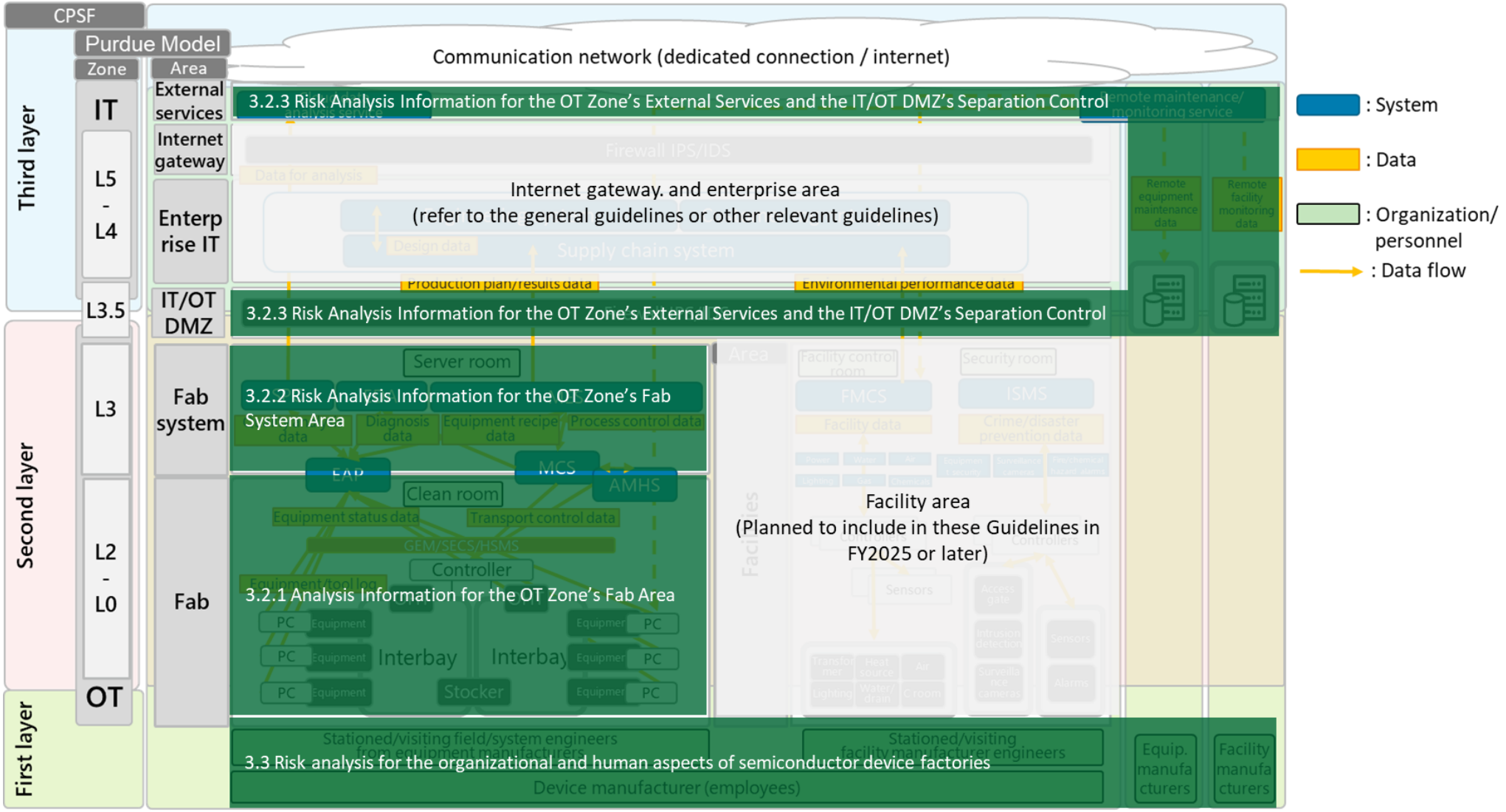


Figure 3-2. Risk Analysis Information for Chapter 3

Table 3-1. The CPSF's Six Elements

Purdue Model		CPSF's six elements					
Zone		System	Data	Components	Procedure	Organization and People	
						Device manufacturer	Partner
External service		**3.2.3 Risk Analysis Information for the OT Zone's External Services and the IT/OT DMZ's Separation Control** Cloud data analytics service Remote monitoring and [illegible]	Cloud analysis data Remote monitoring and [illegible]	Service	Conduct the process for using cloud services via the internet [illegible] receiving remote monitoring and maintenance services from equipment/facility manufacturers	• The IT Department plays a central role in security management via the internet (including remote access)	• Cloud service provider • Facility manufacturer • Equipment manufacturer
Internet gateway		**Internet gateway and enterprise area (Refer to general guidelines, etc.)** Internet gateway (RAS)	Communication control data outside the organization	Firewall, IPS/IDS, etc.	Control communications made with the Internet and external services	• The IT Department plays a central role in managing the security of the entire enterprise • Design, procurement, sales, HR, book-keeping, administration, etc.	• Outsourcing companies for each department
IT	Enterprise (L4-5)	SCM, ECM, CRM	SCM, ECM, [illegible]	[illegible]	Conduct the IT operation (SCM, ECM, and CRM) process in the semiconductor manufacturing company		
IT/OT DMZ (L3.5)		**3.2.3 Risk Analysis Information for the OT Zone's External Services and the IT/OT DMZ's Separation Control** IT/OT DMZ	Communication control data inside the organization	Firewall, IPS/IDS, etc.	Control communications made between the IT operation and OT operation processes		
OT	Fab system (L3)	**3.2.2 Risk Analysis Information for the OT Zone's Fab System Area** MES SPC [illegible] EDA	Production progress data Quality characteristics/analysis data Equipment collection/process diagnostic data	Server, storage, network	Conduct the semiconductor manufacturing process, and conduct the quality control process	**3.3 Risk Analysis Information for the Organizational and People Aspects in Semiconductor Device Factories** • [illegible] production, including its security • Quality assurance, process technology, production technology, manufacturing system, etc.	• [illegible] service company
	Fab (L0-2)	**3.2.1 Risk Analysis Information for the OT Zone's Fab Area** EAP AMHS M[illegible]	Optimum process flow [confidential], equipment status data, recipe [illegible] transportation/lot control data, lot optimization logic	Equipment/tool (manufacturing, inspection, and measurement), OHT, [illegible]er, FOUP	Conduct the process using each manufacturing equipment-, control transportations made within a process or between multiple processes, and conduct communications via industry-standard GEM/SECS		• Equipment manufacturer • A field engineer is assigned on-site, and an office is available
	Facility (L0-3)	**Facility area (Planned to include in these Guidelines in FY2025 or later)** FMCS	Facility data, environmental data	Each facility, controller, sensor	Conduct the operation/management process for the facility environment for clean rooms used to manufacture semiconductors and for each semiconductor manufacturing equipment	• The Facility Department plays a central role in managing factory facilities, including their physical security	• Equipment manufacturer • There are companies supplying electricity, water supply and drainage, gas, and chemicals, and an office is available

3.2 Risk Analysis Information for Each Area of the OT Zone from the Technical and Physical Aspects of Semiconductor Device Factories

Based on the Purdue Model organized in Chapter 2 “Reference Architecture for Semiconductor Device Factories,” the characteristics and viewpoints to be considered from technical and physical aspects are searched for and identified, and summarized from perspectives of security incidents to be assumed and risk sources for each area of the OT zone. Furthermore, their relationship with the CPSF as well as global, semiconductor industry-wide frameworks and references (NIST’s CSF 2.0 Semiconductor Manufacturing Profile and SEMI E187 - Manufacturing Reference) is organized and presented.

The OT zone is the site where devices are manufactured. The organization process will be conducted by dividing the OT zone into the "Fab Area," which is the area where equipment/tools used to process and produce wafers are installed; the "Fab System Area," which is the area where systems used to manage production automation are located; and the "Facility Area," which is the area where infrastructures that support factory operations, such as water, electricity, and gas used for production, are established.

The “IT/OT DMZ,” which separates and controls the OT zone and the IT zone, and “External Services,” where communication connections from the OT zone to external areas take place, will also be organized.

Note that IT enterprise area and the internet gateway that were organized as part of the reference architecture are excluded from the scope of these Guidelines because they are covered by measures implemented in the IT zone. The facility area is also be excluded from the scope of this edition of the Guidelines, as discussions are still ongoing in the global organization from semiconductor industry.

Table 3-2. Zone/Area Characteristics

Zone/area		Zone/area characteristics
External services		External services that analyze cloud-based data are utilized from the fab system are within the OT zone. Regarding the utilization of the cloud, the same cloud service security measures as those implemented in the IT zone are required for connections made from the fab system area.
		Remote diagnostic services (e.g., e-Diagnostics) for equipment/tools in the fab area, which are provided by equipment manufacturers, are utilized, or remote maintenance services for facilities in the facility area, which are provided by facility manufacturers, are utilized. The same security measures as those implemented in the IT zone are required to be implemented for remote access services provided to each OT zone.
Internet gateway		Implement measures in the IT zone (i.e., not covered by these Guidelines).
IT	Enterprise area (L4-5)	
IT/OT DMZ （L3.5）		The IT zone and the OT zone are separated, and communications conducted between them are controlled in accordance with the characteristics of the control system of the OT zone where semiconductors are produced.
OT	Fab system area(L3)	In the fab system area, it is assumed that the same server/system cybersecurity measures as those implemented in the IT zone are applied. However, these systems are characterized by vulnerability assessments conducted based on the assumption of continuous production, patch application, data preservation that takes into consideration business continuity (i.e., mass data backups and restorations), and management of server rooms that store confidential production data.
	Fab area (L0-2)	In the fab area, one of the key security characteristics is the presence of several thousand equipment/tools per factory due to process automation, making management highly challenging. Additionally, the continuous operation of these systems makes it difficult to apply security patches. Equipment/tools are typically used for an average of more than 20 years, and the PCs embedded within them often rely on generic OS, which continue to be used even after vendor support has ended. Furthermore, industry-standard protocols lacking encryption and authentication are widely used between equipment/tools and fab systems, creating additional vulnerabilities. Thus, the fab area requires measures to protect confidential information such as recipes and production processes, which differentiate a company from its competitors. Additionally, it is necessary to manage risks related to supply and production goals, semiconductor quality, and safety (i.e., human life and the environment), caused by unauthorized access or manipulation of equipment/tools. Furthermore, operations must be established to enhance availability even in security-compromised environments.
	Facility area (L0-3) [Excluded from the scope of this edition of the Guidelines]	In the facility area, similar security challenges to those found in data centers and building management systems exist—such as physical measures for managing confidential information within secured areas, long-term equipment operation, and service management for diverse equipment manufacturers. Therefore, similar countermeasures are necessary.

3.2.1 Risk Analysis Information for the OT Zone's Fab Area

The "fab area" is a site where semiconductor devices are manufactured and where equipment/tools for processing and manufacturing wafers are installed. From the two perspectives of "Security measures for equipment/tools in order to achieve production goals and maintain semiconductor quality" and "Protection of confidential production information," this area's characteristics and viewpoints that must be considered will be divided into the following six categories and summarized from each perspective of security incidents to be assumed and risk sou. Furthermore, their relationship with the CPSF as well as global industry-wide frameworks and references (NIST's CSF 2.0 Semiconductor Manufacturing Profile and SEMI E187 - Manufacturing Reference) will be organized and presented.

In the rightmost column of Tables 3-4 through 3-10, relevant categories and subcategories of the NIST CSF 2.0 (e.g., GV.OC-01 and ID.AM-01) and the four zones of the NIST's CSF 2.0 Semiconductor Manufacturing Profile (Fab, Enterprise IT (hereinafter referred to as "E-IT"), Ecosystem (hereinafter referred to as "Eco"), as well as Equipment and Tooling) will be listed under "NIST's CSF 2.0 Semiconductor Manufacturing Profile."

In a similar manner, relevant section titles in Chapter 3 of SEMI E187 - Manufacturing Reference will be listed under "SEMI E187 - Manufacturing Reference."

Table 3-3. Categories of the OT Zone's Fab Area

Security measures for equipment/tools in order to achieve production goals and maintain semiconductor quality	**Protection of confidential production information (for the entire fab area and data stored in equipment)**
(1) Asset management and vulnerability assessment of equipment/tools	(4) Identification and data management of confidential production information
(2) Additional defense measures to minimize equipment/tool damages and to prepare for early recovery	(5) Physical access restrictions (people entering/bringing in devices/making connections)
(3) Procurement and introduction of safe equipment/tools	(6) Logical access restrictions (ID management, authentication, and access control)

Table 3-4. Risk Analysis Information for the OT Zone's Fab Area

<table>
<tr><th colspan="2">Zone/area</th><th>Characteristics and viewpoints that must be considered when implementing security measures (hereinafter referred to as "viewpoints that must be considered")</th><th>CPSF's security incidents to be assumed (threats, vulnerabilities, vulnerability IDs)</th><th>Relevant parts in NIST's CSF 2.0 Semiconductor Manufacturing Profile/CPSF/SEMI E187 - Manufacturing Reference</th></tr>
<tr><td>OT</td><td>Fab area</td><td>(1) Asset management and vulnerability assessment of equipment/tools
Characteristics
In the fab area, where the manufacturing process of semiconductor device factories takes place, equipment/tools from various manufacturers are located in a clean room environment, are seamlessly linked to systems to form a process for conducting automatic, coordinated production.
These equipment/tools, which incorporate technologies for processing wafers with nanometer-scale accuracy, are extremely expensive and are utilized over an extended period, averaging more than 20 years.
A general rule for equipment/tools is that hardware maintenance must periodically be performed, and that the OS and application software must be updated. However, for some equipment/tools, there are restrictions in place when it comes to changing the OS and application software in order to guarantee performance. Security patches cannot be applied to some equipment/tools, or it is difficult to determine the timing at which to apply them due to continuous production.
Various new and old equipment/tools co-exist within the fab area and possess the following characteristics.

<table><tr><th colspan="2">Characteristics of equipment/tools</th></tr><tr><td>1</td><td>A large number of units are being managed
There are thousands of units per factory, and</td></tr></table></td><td>Security incidents to be assumed
• Data that must be protected is tampered with in an area managed by the organization
• Unauthorized input to the device due to unauthorized access to the system that remotely manages the devices results in unpredicted operation

Threats
• Malware infection exploiting security vulnerabilities
• Unauthorized transmission of commands from management systems to devices

Vulnerabilities
• The organization is unclear about the status of the security measure for its devices connecting to information systems and industrial control system.
• The organization does not collect or analyze information about threats and vulnerability related
• The status of security measures (e.g., software configuration information and patch application</td><td>[NIST's CSF 2.0 Semiconductor Manufacturing Profile]
• ID.AM-01 Hardware Management
Fab: identification of interface assets subject to attack
• ID.AM-02 Software Management
• ID.AM-04 Service Management
• ID.AM-05 Importance of Assets
Fab: determination of important assets that impact business operations
• ID.AM-08 Asset Lifecycle Management
Fab: operations that combine legacy assets with cutting-edge assets
• ID.RA-01 Vulnerability Assessment
Fab: vulnerability assessments for large volume / complex assets
• ID.RA-02 Threat Intelligence Collection
Fab: collection of OT threat intelligence
• ID.RA-03 Threat Identification
• ID.RA-04 Probability of Occurrence and Impact of Threats
Fab: assessment of the business impact of continuous operations
• ID.RA-05 Threat Prioritization
Fab: implementation of risk assessments
• ID.RA-06 Risk Management Planning</td></tr>
</table>

			this number is expected to increase in the future due to digital twinning occurring at sites	status) for the organization's devices that are connected to information systems and industrial control systems has not been ascertained • Vulnerabilities that should be handled is left unaddressed in the organization's system • Vulnerabilities that should be addressed in the system are not being addressed properly **Targeted elements** • Components: equipment/tools **[CPSF's vulnerability IDs]** • L1_1_a_SYS • L1_1_b_COM • L2_1_a_ORG • L2_1_b_ORG • L2_1_c_SYS • L2_1_c_ORG • L3_1_a_SYS	and Implementation Fab: risk response planning and implementation • ID.RA-07 Change Management Fab: change management • ID.RA-08 Vulnerability Disclosure Process Fab: establishment of a vulnerability disclosure process **[CPSF's measure requirement IDs]** • CPS.AM-1 • CPS.AM-5 • CPS.AM-6 • CPS.RA (all) **[SEMI E187 - Manufacturing Reference]** 3.4 Vulnerability/Threat Assessment and Patch Management Overview: outlines how to reduce security threats to assets connected to the fab network, such as real-time detection of unauthorized movements and patch application
		2	Hardware and software configurations in equipment/tools are complicated There exists a hardware configuration, which consists of multiple pre-process PCs, DCS, PLC, etc., and a software configuration to conduct controls		
		3	A single equipment/tool is connected to multiple networks for different purposes		
		4	A generic OS is used for the pre-process PC installed inside the equipment (i.e., Windows/Linux)		
		5	Industry standard protocols (i.e., unencrypted/unauthenticated protocols) are used (i.e., GEM/SECS/HSMS) to communicate between equipment systems and between equipment		
		6	Due to the design of some equipment/tools, systems may stop operating during an active scan There is difficulty in implementing vulnerability assessments through active scans		
		7	Software cannot be added to some equipment/tools due to their design (i.e., EPP/EDR)		
		8	Patch applications cannot be implemented on some equipment/tools due to their design		
		9	Some equipment/tools use legacy OS, preventing the implementation of patch		

	applications
10	Patch application time is limited (i.e., line downtime is limited)

Viewpoints that must be considered
As for the assets managed in the fab area, the number of equipment/tools being managed is very large, and the configuration in each equipment/tool is complicated because multiple hardware and software co-exist. Therefore, the scope and collection/management methods of configuration management from a vulnerability assessment viewpoint must be prescribed, ascertained, and monitored.

In addition, the importance of each asset must be classified, and priorities must be set in order to effectively move vulnerability assessments and security measures forward for each asset.
For example, it would be effective to classify the importance of assets in advance based on the importance of equipment/tools in the inspection process, which greatly affects the quality and yield of semiconductor products, and the impact of leaking confidential production information, such as recipes stored in equipment/tools in each process, and to then connect these classifications with security measures and vulnerability assessments to which priorities have been set.

Companies must implement vulnerability assessments targeting production availability, including additional measures (e.g., defense in depth and microsegmentation) that are implemented based on the performance and operational restrictions of equipment/tools.
In terms of the methods for vulnerability assessments targeting production availability, it is necessary to consider

		not only quantitative assessments using CVSS but also assessments using priorities over measures to address production availability such as SSVC. **Examples of specific measures** Specific examples that will serve as reference when considering measures are shown in Section 4.1.		
		(2) Additional defense measures to minimize equipment/tool damages and to prepare for early recovery **Characteristics** A characteristic of the fab area—where there are equipment/tools for which it is difficult to implement vulnerability measures—is that additional defense measures are implemented, such as micro-segmentation and defense in depth which combines physical restrictions and network-based restrictions to prevent the intrusion of attackers and to minimize damage. **Viewpoints that must be considered** Additional measures for equipment/tools are necessary for the purpose of protecting and enhancing production availability. When conducting network segmentation, anomality detection measures must also be considered in addition to micro-segmentation and defense in depth measures, which are necessary to limit and contain the impact of an intrusion on manufacturing by minimizing damages in view of achieving a production availability that enables early recovery or the continuation of limited operations. Defense in-depth is divided into the following three viewpoints, and relevant profiles and references are organized in the following sections. (2)-1 Viewpoints that must be considered for equipment/tools (endpoints)		

		(2)-2 Viewpoints that must be considered for networks (2)-3 Viewpoints that must be considered for physical restrictions **Examples of specific measures** Specific examples that will serve as reference when considering measures are shown in Section 4.2.		
		(2)-1 Viewpoints that must be considered for equipment/tools (endpoints) Security measures for equipment/tools must be considered in accordance with SEMI E187/188. Specifically, after having guaranteed the performance of an equipment, consider measures such as the introduction of security agents, putting into effect anti-malware measures, the implementation of hardening measures (e.g., limiting unnecessary I/O ports and disabling unnecessary services/components/network protocols/ports), and the introduction of anomaly detection tools (e.g., EDR). Since either new software cannot be installed in some of the existing equipment/tools or their settings cannot be changed due to performance guarantee specifications, the implementation of additional measures (e.g., defense in depth and micro-segmentation) using networks must be considered.	**Security incidents to be assumed** • Unexpected behavior of the device due to unauthorized access to its controls by exploiting a vulnerability results in unpredicted operation • Unexpected behavior of the device due to unauthorized access to its controls by impersonation of an authorized user results in unpredicted operation **Threats** • Malware infection that takes advantages of an device's vulnerability • Identity spoofing using a stolen ID/password of a proper user **Vulnerabilities** • Devices in use do not have adequate security functions. • The organization has not implemented technical measures considering risks, or cannot confirm such implementation.	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • ID.AM-08 Asset Lifecycle Management Fab: operations that combine legacy assets with cutting-edge assets • PR.DS-01 Security Protection of Stored Data Fab: increased complexity in accessing data • PR.DS-10 Security Protection of Used Data Fab: protection of operational data • PR.DS-11 Data Backups Fab: backing up confidential operational data • PR.PS (all); Platform Security • PR.IR-02 Protection of Technical Assets from Environmental Threats Fab: clean room environment management • PR.IR-03 Ensuring Resilience Fab: ensuring resilience • PR.IR-04 Securing Resource Capacity Fab: securing resource capacity • DE.CM-03 Monitoring Personnel and Technology Usage Fab: monitoring personnel activities

			• Some settings are not robust enough in terms of security (e.g., passwords, ports). • The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises **Targeted elements** • Components: equipment/tools **[CPSF's vulnerability IDs]** • L1_1_a_SYS • L1_1_c_SYS • L2_1_a_COM • L2_1_b_COM • L3_1_a_SYS • L3_3_a_SYS • L3_3_d_SYS	• DE.CM-06 Monitoring External Service Providers Fab: monitoring external service providers • DE.CM-09 Monitoring Computers and Data **[CPSF's measure requirement IDs]** • CPS.IP-2 • CPS.IP-3 • CPS.IP-7 • CPS.PT-2 • CPS.PT-3 • CPS.DS-10 • CPS.DS-13 • CPS.DS-15 **[SEMI E187 - Manufacturing Reference]** 3.5 Tool Network and Application Integration Overview: describes defense in depth security measures for equipment/tools that limit the implementation of vulnerability assessments and patch applications
		(2)-2 Viewpoints that must be considered for networks For some equipment/tools, security measures such as patch application and anti-malware measures cannot be applied, while for others, patch application takes time due to operational restrictions. Therefore, it is necessary to consider additional measures using networks. In order to protect and enhance production availability, it is necessary to limit and contain the impact of an intrusion on manufacturing by minimizing damages, and to	**Security incidents to be assumed** • The system dealing with the data of its own organization stops due to a denial of service attack, ransomware infection etc. • Device with low quality is connected to a network, causing	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • ID.AM-03 Network Data Flow Management Fab: complex data flow management • PR.DS-02 Security Protection of Transmitted Data Fab: protection of M2M communication data

<table>
<tr>
<td></td>
<td></td>
<td>implement segmentation and put into place communication restrictions (i.e., zone/conduit segmentation) for the purpose of enabling an early recovery or the continuation of limited operations. Specifically, the following considerations must be made based on the security architecture (i.e., the Purdue Model) for semiconductor device factories described in Chapter 2.
<table>
<tr><th colspan="2">Viewpoints that must be considered for networks</th></tr>
<tr><td>1</td><td>The OT network is separated from the IT network by establishing a DMZ using a firewall or the like to control communications. (The OT zone is separated from the IT zone’s network and the internet)</td></tr>
<tr><td>2</td><td>The OT network is divided into the fab system area, the fab area, and the facility area, and communications between them are restricted.</td></tr>
<tr><td>3</td><td>In the fab network of the fab area, all data flows between equipment/tools and with each fab system (e.g., data sent between equipment systems for the purpose of controlling processes, image and video data used to check the quality of products, and data used to coordinate with failure prediction/detection sensors) are searched for, identified, and appropriately separated to restrict communications.</td></tr>
<tr><td>4</td><td>If security measures cannot be implemented for certain equipment/tools, then micro-segmentation or measures to prevent the occurrence and spread of damages should be considered. The unit of micro-segmentation must take into consideration product availability and</td></tr>
</table>
</td>
<td>failures, transmission of inaccurate data or transmission to unauthorized entity
• Data that must be protected is tampered with in an area managed by the organization

Threats
• DoS attacks on computer equipment and communication devices (e.g., servers) that comprise a system
• Inappropriate data from authorized components and system that have been tampered with
• Man-in-the-middle attacks to falsify data on communication paths

Vulnerabilities
• The system does not identify or authenticate the person on the other end of communication when the communication starts
• Communication to devices, servers, etc. are not properly controlled
• Data are not protected enough in communication paths
• The system cannot properly detect and block unauthorized outbound communication from the organization
• Communication channels are</td>
<td>• PR.PS-04 Log Record Management
Fab: log management of legacy devices
• PR.IR (all): Resilience of Technical Infrastructure
• DE.CM-01 Monitoring Networks
Fab: specialized monitoring solutions
• DE.CM-03 Monitoring Personnel and Technology Usage
Fab: monitoring personnel activities
• DE.CM-06 Monitoring External Service Providers
Fab: monitoring external service providers

[CPSF’s measure requirement IDs]
• CPS.AM-4
• CPS.AM-5
• CPS.AC-3
• CPS.AC-7
• CPS.AC-8
• CPS.DS-6
• CPS.DS-9
• CPS.AE-1

[SEMI E187 - Manufacturing Reference]
3.5
Tool Network and Application Integration
Overview: describes defense in depth security measures for equipment/tools that limit the implementation of vulnerability assessments and patch applications</td>
</tr>
</table>

			not properly protected • The system does not have a mechanism to quickly detect and respond to anomalies on the network (eg, spoofing, message tampering) **Targeted elements** • Components: OT network **[CPSF's vulnerability IDs]** • L1_1_b_DAT • L1_1_b_SYS • L1_1_c_SYS • L2_1_a_COM • L3_2_b_DAT • L3_3_a_SYS	3.10 Security Key Performance Indicators Overview: outlines security KPIs for achieving sustainable security operations/management
		(2)-3 Viewpoints that must be considered for physical restrictions For equipment/tools for which it is difficult to implement security measures, it is necessary to consider measures to restrict physical tampering and to limit access to connections and prevent the interception of communications. Since field support and maintenance personnel from multiple equipment manufacturers are stationed at or visit factories, measures that limit physical access to entrances and operation boxes must be considered. Examples: Network devices in the fab area are managed by storing them in racks or boxes that can be locked. If the connection port of an unused fab network is accessible by anyone in the vicinity, then physical port locking measures should be implemented. For wireless communications used within the fab area, the	**Security incidents to be assumed** • Causing failure, transmission of inaccurate data or transmission to unauthorized occurs due to physical interference • Data that must be protected is leaked from an area managed by the organization **Threats** • Physical intrusion by an unauthorized person into areas that need to be protected • Fraudulent falsification by internal or external people with malicious intent • Tampering with sensor readings, threshold, and settings	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • PR.AA-06 Physical Access Management Fab: clean room access control • PR.PS-04 Log Record Management Fab: log management of legacy devices • PR.IR-02 Protection of Technical Assets from Environmental Threats Fab: clean room environment management • DE.CM-02 Monitoring the Physical Environment **[CPSF's measure requirement IDs]** • CPS.AC-2 • CPS.IP-5 • CPS.CM-2

5	The network anomaly detection mechanism must be introduced in important parts.

		range of wave emissions both inside and outside the facility area, as well as waves that may be received from outside the facility area, should be checked, and appropriate countermeasures should be implemented.	**Vulnerabilities** • Physical unauthorized acts to devices by internal or external people cannot be prevented • The organization does not take physical security measures such as access control and monitoring of areas where its devices are installed • The system does not cope with physical interference (e.g. jamming waves) to devices and servers • It is not properly detected that an unauthorized device is connected to the network of the organization **Targeted elements** • The fab area **[CPSF's vulnerability IDs]** • L1_1_a_SYS • L1_1_c_SYS • L2_3_b_SYS • L2_3_b_PEO • L2_3_c_SYS • L2_3_d_SYS • L3_1_a_SYS	
		(3) Procurement and introduction of safe equipment/tools **Characteristics** Equipment/tools are extremely expensive, and they are devices that are used for an extended period of time averaging more than 20 years. Therefore, companies	**Security incidents to be assumed** • A security event occurs in the channel for product / service provisioning, causing unintended quality deterioration	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • GV.SC-01 Establishment and Agreement of a Risk Management Framework Fab: measures to address single-

		must reflect security by design—which prepares them for implementing security operations in the fab environment—into specifications and confirm it at the time of introduction. In 2021, SEMI E187 and E188 were issued as safety standards for the industry's equipment/tools. **Viewpoints that must be considered** In order to introduce safe equipment/tools to the fab area, companies must, upon procurement, consider how the equipment/tools will be operated in the fab area and check in advance with equipment vendors or other related parties, factors such as the status of OS support, security updating procedures, the implementation status of vulnerability diagnoses, necessary information for the use of secure protocols and for restricting communications, and the status of access control functions, security log functions, etc. based on SEMI E187 titled Specification for Cybersecurity of Fab Equipment.	such as malfunction of a device **Threats** • Malware infection that takes advantage of device's vulnerability • Inappropriate acts against transcription function by people with malicious intent **Vulnerabilities** • The organization does not confirm the trustworthiness of products and services at the time of procurement • There is no procedure, at the time of procurement, for checking whether the goods have appropriate levels of security functions • The organization's staff in charge of procurement are not fully aware of security risks related to procurement • There is no procedure for confirming the qualification of procured goods at the time of procurement of products and services • The organization does not check whether the devices have proper levels of safety functions at the time of procurement • The organization does not check whether the products are trustworthy in the measurement security at the time of	supplier dependence • GV.SC-02 Establishment of Roles and Responsibilities • GV.SC-04 Supplier Identification • GV.SC-05 Establishment of Risk Requirements Fab: defining purchase specifications/SLAs • GV.SC-06 Risk Assessment and Plan Execution Fab: assessment of the importance of suppliers • GV.SC-07 Supplier Risk Management • GV.SC-09 Monitoring Security Practices • GV.SC-10 Post-Agreement Rules of Conduct Fab: assessment of the feasibility of best practices • ID.AM-04 Service Management • ID.RA-09 Assessment of Authenticity and Integrity Fab: ensuring component authenticity • ID.RA-10 Supplier Assessment Fab: specialized supplier assessment **[CPSF's measure requirement IDs]** • CPS.SC-1 • CPS.SC-2 • CPS.SC-3 • CPS.SC-4 • CPS.SC-5 • CPS.SC-6 • CPS.AM-7 • CPS.DP-1 • CPS.PT-3

			procurement of devices **Targeted elements** • Components: equipment/tools **[CPSF's vulnerability IDs]** • L1_1_d_ORG • L1_1_d_PRO • L2_1_a_PRO • L2_2_a_ORG • L2_3_c_ORG • L2_3_c _PRO • L2_3_d_ORG	• CPS.DS-12 • CPS.CM-3 **[SEMI E187 - Manufacturing Reference]** 3.1 Secure by Design Overview: outlines key points of procurement requirements that must be pre-confirmed with equipment vendors or other related parties in order to introduce safe equipment/tools to the fab area 3.2 Tool Configurations Overview: outlines the recommended specifications to be considered by semiconductor device manufacturers when procuring equipment/tools, such as the installation of firewalls and the separation of communications
		(4) **Identification and data management of confidential production information** **Characteristics** Confidential production information in the fab area includes, for example, information on designs used in the photomask manufacturing process, information on miniaturization technologies and yield enhancement production recipes / production processes applied in the pre-processing stage, as well as production technology information concerning layering techniques applied in the post-processing stage. The characteristics of this type of information are that it is extremely confidential, and that if an infringement causes a leakage of intellectual property, a company will be placed at a disadvantage in the	**Security incidents to be assumed** • Data that must be protected is tampered with in an area managed by the organization **Threats** • Protected data has been taken out improperly by a mallicious entity • Physical destruction of media • Identity spoofing	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • GV.OC-03 Management of Legal and Regulatory Requirements • ID.AM-05 Importance of Assets Fab: determination of important assets that impact business operations • ID.AM-07 Metadata Management Fab: management of metadata for process recipes • ID.AM-08 Asset Lifecycle Management Fab: operations that combine legacy assets with cutting-edge assets

		development competition and other types of competitions with competitors. **Viewpoints that must be considered** Confidential production data in the OT zone is mainly stored in the fab system area. However, since confidential production data exists in the fab area itself as well as in equipment/tools, confidential data must be also managed in the fab area. Many factories deem the set-up inside a cleanroom, including visual information such as the configuration of production processes and the types and numbers of equipment/tools used, as confidential production information. Therefore, factories must consider placing restrictions on the recording of images and videos in the fab area and the bringing in of recording devices into the area. Confidential production information such as recipes and quality information are stored in equipment/tools. Factories must treat confidential production data stored in each equipment as information assets, obtain knowledge on what data is stored where, and restrict access to the confidential production information during normal operations. At the same time, access controls must be placed over said data and restrictions must be placed on taking it out during maintenance. When an equipment/tool is replaced or removed, it is necessary to ensure that confidential data preserved in the storage area inside the equipment/tool is erased.	**Vulnerabilities** • Classification concerning protection of data is not clear • Settings in the system where the data to be protected is stored are not secure • Responsibility in the organization for managing data to be protected is not identified **Targeted elements** • Data: confidential production data • People: people who enter the fab area • People who have access to equipment/tools **[CPSF's vulnerability IDs]** • L1_1_a_DAT • L1_1_a_SYS • L1_1_b_SYS • L1_1_c_SYS • L3_1_a_DAT • L3_1_a_ORG • L3_4_a_ORG • L3_4_b_SYS	• PR.DS (all): Data Security • PR.IR-02 Protection of Technical Assets from Environmental Threats Fab: clean room environment management **[CPSF's measure requirement IDs]** • CPS.DS-1 • CPS.DS-2 • CPS.DS-3 • CPS.DS-4 • CPS.DS-5 • CPS.DS-9 • CPS.DS-11 • CPS.DS-14 • CPS.AM-6 • CPS.GV-3 • CPS.IP-6 **[SEMI E187 - Manufacturing Reference]** 3.3 Move-in/Move-Out/Transfer Overview: outlines key points that must be checked when installing, removing, or relocating equipment/tools, especially to protect confidential production information 3.7 Secure Data Exchange Overview: outlines key points that must be checked when installing, removing, or relocating equipment/tools, especially to protect confidential production information

		(5) Physical access restrictions (people entering, bringing in devices and making connections) **Characteristics** A clean room is categorized as a fab area, and its set-up, including visual information such as the configuration of production processes and the types and numbers of equipment/tools used is deemed as confidential production information. Since it is difficult for a single security measure to cover all equipment/tools, it is necessary to limit entry into the fab area to only people who have been granted permission and to restrict the bringing in and connecting of devices. In addition, since proprietary equipment/tools of various manufacturers are used in the production process conducted in the fab area and production continues unceasingly, maintenance agreements are concluded with many equipment manufacturers. The fab area is characterized by the frequent implementation of maintenance/operation work by field engineers of each equipment manufacturer who are stationed there or visit the factory (e.g., in 2018, a leading Taiwanese semiconductor company suffered major damage from a malware infection via a device that was brought in during maintenance). **Viewpoints that must be considered** Since confidential production information is handled inside the fab area, control over physical access to the area must cover the route starting from the entrance of the device factory to the clean room entrance. Furthermore, factories must consider placing restrictions on the recording of images and videos and the bringing in of recording devices. At the same time, since automated transport equipment such as OHTs are operated via wireless communication, it is also necessary to restrict the bringing in of devices that	**Security incidents to be assumed** • Causing failure, transmission of inaccurate data or transmission to unauthorized occurs due to physical interference • Data that must be protected is leaked from an area managed by the organization **Threats** • Physical intrusion by an unauthorized person into areas that need to be protected • Tampering by internal or external people with malicious intent • Tampering with sensor readings, thresholds, and settings **Vulnerabilities** • The organization does not take physical security measures such as access control and monitoring of areas where its devices are installed • It is not properly detected that an unauthorized device is connected to the network of the organization • Network communications (wired or wireless) from unauthorized devices cannot be prevented • The organization does not take physical security measures such as access control and monitoring of areas where its devices are installed	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • DE.CM-01 Monitoring Networks Fab: specialized monitoring solutions • DE.CM-02 Monitoring the Physical Environment • DE.CM-03 Monitoring Personnel and Technology Usage Fab: monitoring personnel activities • DE.CM-09 Monitoring Computers and Data **[CPSF's measure requirement IDs]** • CPS.CM-2 • CPS.CM-6 • CPS.MA-2 **[SEMI E187 - Manufacturing Reference]** 3.3 Move-in/Move-Out/Transfer Overview: describes key points that must be checked when installing, removing, or relocating equipment/tools, especially to protect confidential production information 3.4 Vulnerability/Threat Assessment and Patch Management Overview: outlines how to reduce security threats to assets connected to the fab network, such as real-time detection of unauthorized movements and patch application

		generate radio waves which may interfere with wireless communication. In order to conduct maintenance work, connecting new equipment/tools (including sensor peripheral devices) to the fab network when introducing them to the fab area, and connecting devices brought in for maintenance work to existing equipment/tools via USB, serial, or network connections. Procedures for making such connections must be set up to ensure that the designated security checks are conducted before devices are connected. In terms of the security checks implemented at the time of connecting devices to conduct maintenance work, factories must consider checking not only the bringing in of malicious programs such as malware but also checking the taking out of confidential production information such as recipes and quality information found in equipment/tools. **Examples of specific measures** Specific examples that will serve as reference when considering measures are shown in Section 4.4.	**Targeted elements** • People: equipment maintenance personnel • Data: confidential production data • Components: brought-in devices **[CPSF's vulnerability IDs]** • L1_1_a_SYS • L2_3_b_SYS • L2_3_c_SYS • L2_3_d_SYS • L3_1_a_SYS	
		(6) Logical access restrictions (ID management, authentication, and access control) **Characteristics** Since confidential data such as recipes are stored in equipment/tools, strict identity management, authentication, and access control are required. Accounts used for equipment/tools include those used during normal operations and those used during maintenance. In addition, maintenance agreements of equipment/tools are concluded with equipment manufacturers, and field support personnel are stationed at or visit factories to conduct maintenance. There are also cases when remote diagnosis services using e-Diagnostics technology are provided by equipment manufacturers. A characteristic of	**Security incidents to be assumed** • Data that must be protected is leaked from an area managed by the organization **Threats** Identity spoofing using a stolen ID/password of a proper user **Vulnerabilities** • Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • GV.RR-04 Security of Human Resource Processes Fab: prevention of unauthorized accesses • PR.AA-01 Management of ID and Authentication Information Fab: access control for industrial control/IT systems • PR.AA-02 Mutual ID Authentication Fab: mutual context • PR.AA-03 User Authentication Fab: implementation of authentication mechanisms on all

		account management of equipment/tools is that it must cover accounts used by maintenance personnel of equipment manufacturers with whom outsourcing agreements have been concluded. **Viewpoints that must be considered** Unauthorized accesses to equipment/tools can lead to production stoppages, leakage of confidential production information, falsification of recipes, etc. Therefore, it is important to manage accounts and privileged authorities as part of an appropriate identity and access management (IAM) scheme. Account management shall involve implementing appropriate approval by the device manufacture, the continuous monitoring of all access events, and audit processes throughout the account lifecycle (i.e., creation, modification, and deletion of accounts). Privileged accounts, which are accounts used during maintenance that require many privileged authorities, must especially be managed more strictly than general accounts used during operations. For remote diagnosis services using e-Diagnostics technologies that have been introduced in the industry, it is necessary for device manufactures to implement and operate secure solutions and process including monitoring, logging, and encryption to prevent impersonation and protect against the leakage of confidential production data.	confidentiality of such information Data protection at a predefined level of confidentiality is not implemented Segregate duties and areas of responsibility properly (e.g. segregate user functions • from system administrator functions) **Targeted elements** • People: people who have access to equipment/tools • **[CPSF's vulnerability IDs]** • L1_1_a_SYS • L1_1_b_SYS • L1_1_a_DAT • L2_1_c_SYS • L3_1_a_DAT	devices • PR.AA-04 ID Assertion Fab: ID assertion between the fab system and equipment • PR.AA-05 Principles of Least Privilege and Separation of Duties Fab: control over access to a different area • PR.AA-06 Physical Access Management Fab: clean room access control **[CPSF's measure requirement IDs]** • CPS.AC-1 • CPS.AC-4 • CPS.AC-5 • CPS.AC-6 • CPS.AC-9 • CPS.IP-1 • CPS.IP-9 **[SEMI E187 - Manufacturing Reference]** 3.6 Local & Remote Accesses Overview: outlines key points of account management and privileged authority management in order to prevent unauthorized accesses

3.2.2 Risk Analysis Information for the OT Zone's Fab System Area

An assumption concerning the "fab system area," where systems for managing the automation of semiconductor device manufacturing are located, is that the same cybersecurity measures as those implemented for server systems are implemented, as is the case in the IT zone. Among these measures, the following three categories will be summarized from the perspective of security incidents to be assumed and risk sources as viewpoints that must be considered and characteristics that differentiate the semiconductor device factory's OT zone from its IT zone. Furthermore, their relationship with the CPSF as well as global frameworks and references (NIST's CSF 2.0 Semiconductor Manufacturing Profile and SEMI E187 - Manufacturing Reference) will be organized and presented.

Table 3-5. Categories of the OT Zone's Fab System Area

Categories	Overviews
(1) System availability	Operational considerations including patch applications implemented during continuous production
(2) Data preservation	Large-volume backups for videos and images and early restoration to continue business
(3) Physical measures for server rooms	Physical measures to safe-keep server rooms as confidential data storage areas

Table 3-6. Risk Analysis Information for the OT Zone's Fab System Area

Zone/area		Characteristics and viewpoints that must be considered	CPSF's expected security incidents/risk sources (threats, Vulnerabilities, Vulnerability IDs)	Relevant parts in NIST's CSF 2.0 Semiconductor Manufacturing Profile / CPSF / SEMI E187 - Manufacturing Reference
OT	Fab system area	**(1) System availability (during continuous production) Characteristics** The each of fab system area's MES, SPC, and EDA control the production process and quality of the fab area's equipment/tools, consist of servers, storage, networks, etc. As for the security measures for the fab system area, measures to manage vulnerability assessments and patch applications are to be implemented, which are the same as those implemented in the IT zone, but these measures must be conducted based on the assumption that production will continue unceasingly, and that system coordination checks will be conducted. Specifically, companies are required to conduct patch applications online and while services are continuously provided, which is similar to the situation of e-commerce sites. However, some patches that are applied to fab systems cannot be applied online due to factors such as the necessity of conducting system coordination checks. Therefore, a characteristic of such patches is that application must be planned and executed during limited opportunities within a single year in which lines are shut down to conduct maintenance work. **Viewpoints that must be considered** For the fab system area, there is a time lag between implementing a vulnerability assessment and executing a patch application. (The timing for applying patches where lines are shut down to conduct maintenance work occur once in several months or once a year.)	**Security incidents to be assumed** • DoS attacks on communication devices that comprise a system. **Threats** • DoS attack on computing devices such as servers, communication devices, etc. • A device with low quality connected to a network. **Vulnerabilities** • Safety instrument is not considered in the system being operated • A system that does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity) with low quality connected to a network **Target components** • Systems: MES, SPC, EDA, etc.	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • PR.IR-03 Ensuring Resilience Eco: implementation of recovery mechanisms E-IT: maintaining access to business systems • PR.IR-04 Securing Resource Capacity Eco: securing resource capacity E-IT: securing resource capacity **[CPSF's measure requirement IDs]** • CPS.DS-7

<table>
<tr>
<td></td>
<td></td>
<td>It would be effective to consider concrete measures such as limiting communications between the IT zone and the fab system area by separating them using an IT/OT DMZ, detecting anomalies using IPS/IDS, and applying virtual patches.</td>
<td>• Components: servers, storage, networks

[CPSF’s vulnerability IDs]
• L1_1_c_SYS
• L2_1_d_SYS
• L3_3_c_SYS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) Data preservation (high-volume backups and restorations)
Characteristics
Fab systems require high-capacity storage to provide instructions for process-based automatic control, to determine quality using high-resolution image and video data, and to store records.
Furthermore, in preparation for system shutdowns or damage incurred to production data, the system is configured so that it takes into consideration the time required to restore data from backup data in order to ensure early restoration as well as the fulfillment of supply responsibilities.

Viewpoints that must be considered
Fab system backups require high-capacity storage, and it is important to select a backup method that takes into account the restoration time required in order to ensure early recovery. Simultaneously, companies must consider implementing security measures such as authority separation and prevention of tampering (such as storing them offline or adopting the WORM function) so that the backup data is not affected by ransomware damages. It is also important to select backup methods that take recovery into consideration for data stored within device tools, such as configuration information, calibration values, and security logs</td>
<td>Security incidents to be assumed
• The organization’s security incidents prevent their business from continuing properly

Threats
• Attacks on devices that save data
• A device with low quality connected to a network

Vulnerabilities
• Data necessary to continue the business at the time of the security incident has not been properly backed up, or has been backed up but does not function properly

Target components
• Systems: backup systems for fab systems
• Components: backup servers, storage,</td>
<td>[NIST’s CSF 2.0 Semiconductor Manufacturing Profile]
• PR.DS-11 Data Backups
Eco: verification of backup data
E-IT: regularly backing up critical data
• PR.IR-03 Ensuring Resilience
Eco: implementation of recovery mechanisms
E-IT: maintaining access to business systems
• PR.IR-04 Securing Resource Capacity
Eco: securing resource capacity
E-IT: securing resource capacity
• RC.RP-03 Verification of Backup Consistency
Eco: verification of backup consistency
E-IT: verification of backup consistency

[CPSF’s measure requirement IDs]
• CPS.IP-4</td>
</tr>
</table>

			backup media **[CPSF's vulnerability IDs]** • L1_3_a_DAT • L2_1_d_SYS • L3_3_c_SYS	
		(3) Physical measures for server rooms **Characteristics** Since fab systems require high-capacity storage and equipment/tools installed in the fab area as well as fab systems such as MES need to be connected by a high-speed network to avoid distance delays, a server room must be established inside the factory. Within the server room of a factory, fab systems—which consist of redundant servers, storage, etc. that support the continuous production of devices—are installed, and they must be operated in-house. Furthermore, since confidential production information is stored in the servers and storage devices of fab systems, the server room that manages them must be operated and managed as a confidential data storage area. **Viewpoints that must be considered** Since confidential production information is stored in server rooms, server rooms must be treated as confidential data storage areas and measures must be implemented accordingly. Specifically, companies must consider placing access controls on people entering and exiting the room (i.e.,	**Security incidents to be assumed** • Data that must be protected is leaked from an area managed by the organization **Threats** • Physical intrusion by an unauthorized person into areas that need to be protected • Physical intrusion by an unauthorized entity • Protected data has been taken out improperly by a malicious entity of the organization	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • PR.AA-06 Physical Access Management Eco: monitoring the entries and exits of personnel E-IT: ensuring physical security of the development environment • PR.PS-04 Log Record Management Eco: continuous monitoring of logs E-IT: integration of system log formats • PR.IR-02 Protection of Technical Assets from Environmental Threats Eco: protection against environmental threats E-IT: protection of servers from environmental threats • DE.CM-02 Monitoring the Physical Environment Eco: monitoring unauthorized accesses to confidential zones E-IT: protection against unauthorized physical accesses

		work rules for maintenance contractors), utilizing monitoring systems (i.e., monitoring and recording images/movements using CCD cameras, and utilizing sensor detection), and managing devices (including backup media) brought into and taken out of the server room, among others.	**Vulnerabilities** • The organization does not take physical security measures such as access control and monitoring of areas • Data protection at a level of confidentiality is not implemented **Target components** • Components: server rooms **[CPSF's vulnerability IDs]** • L1_1_a_SYS • L1_1_c_SYS • L2_3_b_PEO • L2_3_b_SYS • L2_3_c_SYS • L2_3_d_SYS • L3_1_a_SYS	**[CPSF's measure requirement IDs]** • CPS.AC-2 • CPS.IP-5 • CPS.CM-2

3.2.3 Risk Analysis Information for the OT Zone's External Services and the IT/OT DMZ's Separation Control

Initiatives utilizing "external services" provided to the OT zone are being considered in order to promote the early improvement of yield quality and to reduce costs. The external services will run in combination with the "IT/OT DMZ" function, which separates, controls, and protects the OT zone from the IT zone and the internet. Their characteristics and viewpoints that must be considered will be summarized into the following three categories from the perspective of security incidents to be assumed and risk sources. Furthermore, their relationship with the CPSF as well as global frameworks and references (NIST's CSF 2.0 Semiconductor Manufacturing Profile and SEMI E187 - Manufacturing Reference) will be organized and presented.

Table 3-7. Categories of the OT Zone's External Services and the IT/OT DMZ's Separation Control

Categories	Overviews
(1) Utilization of external services (cloud services)	Utilization of data in OT fab systems for cloud-based data analytics services
(2) Utilization of external services (use of remote diagnosis services)	Utilization of remote diagnosis services (e-Diagnostics, etc.) from equipment manufacturers to diagnose equipment/tools installed in the fab area
(3) IT/OT DMZ	The IT/OT DMZ which separates, controls, and protects the OT zone

Table 3-8. Risk Analysis Information for the OT Zone's External Services and the IT/OT DMZ's Separation Control

Zone/area		Characteristics and viewpoints that must be considered	CPSF's security incidents to be assumed (threats, vulnerabilities, vulnerability IDs)	Relevant parts in NIST's CSF 2.0 Semiconductor Manufacturing Profile / CPSF / SEMI E187 - Manufacturing Reference
OT	External services	**(1) Utilization of external services (cloud services)** **Characteristics** In order to improve yield quality and reduce costs, efforts are being made to link the quality data stored in OT fab systems to services using cloud-based data analysis technologies. **Viewpoints that must be considered** The same measures as those implemented in the IT zone (CSPM, CWPP, CASB, CIEM, SSPM, etc.) must be implemented as cybersecurity measures upon using cloud services. The system administrator of the OT zone using the cloud services must implement measures (including policy checks, etc.) in cooperation with the cloud security manager of the IT zone. In particular, when using the cloud to analyze quality data,	**Security incidents to be assumed** • Data that must be protected is leaked from a cloud-based storage area managed by the organization • A security event occurs in the channel for service provisioning, causing unintended quality deterioration such as malfunction of a device.	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** *Implement cloud security measures conducted in the IT zone

		which is deemed as confidential production data, the implementation of cloud security measures must be considered while paying attention to data protection (i.e., using encryption when transmitting or storing data) and access controls.		
			Threats • Malware infection using an attack tool that takes advantage of an device's vulnerability **Vulnerabilities** • The organization is unclear about how its components, systems, and/or data have been working with other organizations in cyberspace • The system has no mechanism for detecting and handling any abnormality related to security as soon as it	**[CPSF's measure requirement IDs]** * Implement cloud security measures conducted in the IT zone

			arises • The organization does not confirm the trustworthiness of service supplier's organizations, systems, etc. before and after signing contracts **Targeted elements** • Systems: cloud services	
		(2) External services (use of remote diagnostic services) Characteristics The utilization of remote diagnostic/maintenance services (e.g., e-Diagnostics) provided by equipment manufacturers for equipment/tools located in the fab area is being promoted **Viewpoints that must be considered** If an external network line is connected to the fab area or OT zone, a joint risk assessment must be implemented with the information security manager regarding the connection configuration and usage method of the line, the scope of managerial responsibilities, and other aspects, including the terms and conditions of the agreement concluded with the connection provider or the business user, and the same security measures as those implemented in the IT zone must be implemented. For remote network connections, risk assessments must be implemented by searching for, identifying, and targeting not only those made through conventional wired communication networks such as dedicated lines, internet networks and telephone networks, but also connections made through wireless communication networks, including cellular network	**Security incidents to be assumed** • As a result of the intrusion of a malicious external entity into an area managed by the organization, protected data is leaked and the systems responsible for handling the data are rendered inoperable **Threats** • An intrusion attack that takes advantage of a system's vulnerability • Protected data has been taken out improperly by a malicious entity • Identity spoofing using a stolen ID/password of a	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** * Implement remote access measures conducted in the IT zone

		used by mobile routers, WiFi wireless networks, and satellite communication networks.. With regard to the remote maintenance of equipment/tools installed in the fab area, security measures for equipment/tools that operate continuously are insufficient. Therefore, companies must establish a jump server environment with the most up-to-date security measures in the IT/OT DMZ zone and other relevant areas. They must also implement measures such as monitoring and recording details of remote operations, enhancing authentication strength (e.g., by using multi-factor authentication (MFA)) to prevent users from spoofing, and limiting the connection environment by limiting communication destinations and communication/network ports. In addition, secure solutions and processes—including monitoring, logging, and encryption—must be implemented and operated to prevent leakage of confidential information.	proper user **Vulnerabilities** • The organization is unclear about how its components, systems, and/or data have been working with other organizations in cyberspace • The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises • The organization does not confirm the trustworthiness of service supplier's organizations, systems, etc. before and after signing contracts **Targeted elements** • Systems: remote diagnostic services	**[CPSF's measure requirement IDs]** * Implement cloud security measures conducted in the IT zone **[SEMI E187 - Manufacturing Reference]** 3.6 Local & Remote Accesses Overview: outlines key points of account management and privileged authority management in order to prevent unauthorized accesses
		(3) Separation control via the IT/OT DMZ Characteristics In order to protect the OT zone—which continuously manufactures products by commanding several thousand equipment/tools using manufacturing systems and automatic controls—from cybersecurity threats, a DMZ must be established to separate it from the IT zone's network and the internet.	**Security incidents to be assumed** • Causing failure, transmission of inaccurate data or transmission to unauthorized occurs due to physical interference	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • ID.AM-03 Network Data Flow Management Fab: complex data flow management • PR.DS-02 Security Protection of Transmitted Data Fab: protection of M2M communication data

		Viewpoints that must be considered For communications between the OT zone, the IT zone and external services such as the internet, it is necessary to clarify data flows and to control communications pursuant to the deny-by-default policy and the principle of least privilege and conduct regular audits and continuous reviews to ensure the effectiveness. Furthermore, companies must consider introducing the function of detecting and preventing abnormal behavior in the traffic sent and received.	**Threats** • Inappropriate data from authorized components and system that have been tampered with **Vulnerabilities** • The system does not identify or authenticate the person on the other end of communication when the communication starts • Data are not protected enough in communication paths • The system cannot properly detect and block unauthorized outbound communication from the organization **Targeted elements** • Components: IT/OT DMZ devices **[CPSF's vulnerability IDs]** • L2_3_c_SYS • L3_2_b_DAT • L3_3_a_SYS	• PR.PS-04 Log Record Management Fab: log management of legacy devices • PR.IR-01 Protection Against Unauthorized Logical Accesses Fab: protection against unauthorized logical accesses • PR.IR-02 Protection of Technical Assets from Environmental Threats Fab: clean room environment management • PR.IR-03 Ensuring Resilience Fab: ensuring resilience • PR.IR-04 Securing Resource Capacity Fab: securing resource capacity • DE.CM-01 Monitoring Networks Fab: specialized monitoring solutions • DE.CM-03 Monitoring Personnel and Technology Usage Fab: monitoring personnel activities • DE.CM-06 Monitoring External Service Providers Fab: monitoring external service providers **[CPSF's measure requirement IDs]** • CPS.AM-4 • CPS.AM-5 • CPS.AC-3 • CPS.AC-7 • CPS.AC-8 • CPS.DS-6 • CPS.DS-9 • CPS.AE-1

				[SEMI E187 - Manufacturing Reference] 3.10 Security Key Performance Indicators Overview: outlines security KPIs for achieving sustainable security operations/management

3.3 Risk Analysis Information for the Organizational and People Aspects in Semiconductor Device Factories

To achieve risk management aligned with the business objectives of semiconductor device factories, the characteristics and considerations from the organizational and people's perspectives are summarized into the following seven categories, based on security incidents to be assumed and risk sources. The relationship with global countermeasure frameworks and references (NIST CSF 2.0 Semiconductor Manufacturing Profile, SEMI E187 Manufacturing Reference) as well as CPSF is organized and presented.

Table 3-9. Categories for the Organizational and People Aspects of Semiconductor Device Factories

(1)	Governance (understanding the business environment and establishing roles, responsibilities, and authorities)
(2)	Compliance with laws, regulations, and industry standards (protecting human lives and maintaining environmental safety)
(3)	Fulfilling supply responsibilities as a part of the supply chain (achieving production goals and maintaining product quality)
(4)	Protection of confidential production information
(5)	Risk management/policy/resilience
(6)	Operations (monitoring / response / recovery / improvement)
(7)	Awareness raising and training

Table 3-10. Risk Analysis Information for the Organizational and People Aspects of Semiconductor Device Factories

Zone/area	Characteristics and viewpoints that must be considered	CPSF's security incidents to be assumed (threats, vulnerabilities, vulnerability IDs)	Relevant parts in NIST's CSF 2.0 Semiconductor Manufacturing Profile / CPSF / SEMI E187 - Manufacturing Reference
Organizational response	**(1) Governance (understanding the business environment and establishing roles, responsibilities, and authorities)** **Characteristics** Given that the semiconductor industry faces high cybersecurity risks, such as government-sponsored APT attacks including industrial espionage, semiconductor device	**Security incidents to be assumed** • The organization's security incidents prevent their business from continuing properly	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • GV.OC-01 Understanding the Mission of the Organization Eco: understanding organizational goals and processes • GV.OC-02 Understanding Stakeholders

	factories bear legal responsibilities to protect confidential production information (i.e., that of their own as well as other companies), avoid people damage, and consider the environmental impact of their business activities in addition to protecting production availability and quality as well as fulfilling supply responsibilities. It is necessary for the factories to understand the environment in which they operate and establish roles, responsibilities, and authorities that enable them to fulfill their responsibilities. **Viewpoints that must be considered** Semiconductor device factories need to understand their business environment in which the risks and importance of the OT zone (i.e., fabs, fab systems, and facilities) are high/great, and must establish roles, responsibilities, and authorities for the OT zone. In order for OT security measures to be positioned not as mere technical challenges but as business risk management, it is necessary to secure strong commitment from management. Furthermore, as OT security specialists, it is required to secure and develop personnel who have not only IT security knowledge but also a deep understanding of semiconductor manufacturing processes.	**Threats** • All Threats **Vulnerabilities** • The organization has not established a framework for accurately detecting security incidents • The organization is unclear about how it has been working with other organizations (e.g., suppliers) **Targeted elements** • Organizations: device manufacturers **[CPSF's vulnerability IDs]** • L1_1_a_ORG • L1_3_a_ORG • L1_3_b_ORG • L1_3_c_ORG	Eco: understanding stakeholder requirements • GV.OC-05 Understanding Organizational Performance and Capabilities Eco: defining and coordinating supply chain roles • GV.RR-01 Cybersecurity Responsibilities of the Organization Eco: clarifying and supporting the organizational direction • GV.RR-02 Cybersecurity Management Eco: clarifying roles, responsibilities and, authorities • GV.RR-03 Resource Allocation Eco: allocation of resources to cyber strategies • GV.SC-02 Establishment of Roles and Responsibilities Eco: aligning supplier expectations with organizational goals • RC.CO-03 Communicating the Recovery Status Eco: communicating the recovery status **[CPSF's measure requirement IDs]** • CPS.AM-7 • CPS.BE-1 • CPS.BE-2 • CPS.GV-1 • CPS.RM-1 • CPS.DP-1 • CPS.CO-3

	(2) Compliance with laws, regulations, and industry standards (protecting human lives and maintaining environmental safety) **Characteristics** Semiconductor device factories must comply with laws (i.e., the Industrial Safety and Health Act and environmental laws) to address the impact of risks to human life and the environment caused by combustible and toxic gases, hazardous chemical substances such as strong acids and strong alkaline solvents, radiation such as X-rays and ultraviolet rays, high voltage, high temperature, and operating equipment (e.g., entanglement, pinching, or collision), among others. In the future, compliance with the EU's Cyber Resilience Act, which aims to protect consumers from cybersecurity threats generated by products containing digital elements. In particular, it will become necessary to implement measures for important digital products such as microprocessor controllers equipped with security-related functions and tamper-resistant microprocessor controllers. **Viewpoints that must be considered** It is necessary to continuously monitor the latest trends in domestic and international laws, regulations, and international standards related to security in the semiconductor industry, and establish and operate internal rules with customers' industry standards (e.g., the automotive industry's TISAX).	**Security incidents to be assumed** • Security measures that satisfy the legal requirements for a system cannot be implemented **Threats** All threats **Vulnerabilities** • The organization is unaware of legal systems with which it should comply, or it has not developed, or is not operating internal rules that conform to the legal systems • People are unaware of legal systems with which it should comply, or they do not follow internal rules that conform to the legal systems • Established internal procedures are not designed to ensure compliance with laws and regulations **Targeted elements** • Organizations: device manufacturers **[CPSF's vulnerability**	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • GV.OC-03 Management of Legal and Regulatory Requirements Eco: compliance with industrial frameworks **[CPSF's measure requirement IDs]** • CPS.GV-2 • CPS.GV-3 • CPS.DP-2

		IDs] • L1_1_a_SYS • L1_2_a_ORG • L1_2_a_COM • L1_2_a_SYS • L1_2_a_PRO • L1_2_a_DAT	
	(3) Fulfilling supply responsibilities as a part of the supply chain (achieving production goals and maintaining product quality) **Characteristics** Semiconductors are used by various industries and are considered important products from an economic and national security perspective. Furthermore, organizations must satisfy customers' quality requirements for semiconductor chips such as performance specifications and accuracy, and while also fulfilling supply responsibilities, which include providing accountability that production is carried out in a safe environment (customers will expect such accountability). Semiconductor device factories use clean rooms and facilities, as well as equipment/tools and transport equipment that comprise fully automatic process production. Construction costs per factory exceeds JPY 10 billion, which is extremely high, limiting the industry's production capacity (adjusting the number of factories is not feasible).	**Security incidents to be assumed** • The organization's security incidents prevent their business from continuing properly • Other relevant organizations cannot continue their business properly due to the organization's security incidents • The organization's security incidents prevent the business of other relevant organizations from continuing properly	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • GV.OC-04 Understanding External Stakeholders Eco: improving the defense capabilities of an organization • GV.RM-05 Establishment of a Communication Line Eco: supply chain risk management process • GV.SC (all) Cyber Supply Chain Risk Management • ID.AM-04 Service Management Eco: maintaining inventory • PR.IR-03 Ensuring Resilience Eco: implementation of recovery mechanisms

	Semiconductor production lead times are relatively long, ranging from three to five months. Therefore, measures must be implemented, and levels of risk tolerance must be set that take into account the impact of losses incurred in the event production lines are shut down at device factories. **Viewpoints that must be considered** In terms of fulfilling supply responsibilities, an organization must establish a safety inventory level (e.g., 20 days-worth of products) that takes into account the impact of a production line shutdown, and it must then implement cybersecurity measures suitable for the situation. Simultaneously, it must develop measures, operational structures, etc. to minimize the scope of damage inflicted on production when an incident occurs and to limit its impact on supplies. When the supply responsibilities of an organization are large, it must step up its monitoring of behaviors as well as its ability to detect anomalies, and it must consider enhancing risk measures by implementing measures such as micro-segmentation, which minimizes the scope that is impacted. Furthermore, considering its role as a part of the supply chain, it must provide accountability that products fulfilling the quality expected by customers are being produced based on a safe design and in a safe environment. (For hardware Trojans, which are malicious functions or circuits intentionally incorporated into semiconductors, organizations must implement measures based not only on the assumption that it may occur during the design stage, but also during the manufacturing process. Hardware Trojans must also be searched for and detected during the inspection process.)	**Threats** All threats **Vulnerabilities** • Security risks are not managed and other organizations needed are not involved in risk management • A security incident causes damage to components (products) and/or services • The organization does not retain the records of components (products) delivered to/from the organization **Targeted elements** • Organizations: device manufacturers **[CPSF's vulnerability IDs]** • L1_1_a_ORG • L1_1_a_PRO • L1_1_b_ORG • L1_1_b_PRO	**[CPSF's measure requirement IDs]** • CPS.SC (all) • CPS.BE-3 • CPS.RP-4 • CPS.AM-2 • CPS.AM-3
	(4) Protection of confidential production information Characteristics In addition to confidential data such as circuit designs, product roadmaps, and customer agreements, semiconductor	**Security incidents to be assumed** • Data that must be protected is tampered	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • ID.AM-05 Importance of Assets Eco: importance of assets

	device companies handle and strictly manage confidential production information that is important for maintaining the competitiveness of production technologies, such as recipes, processing patterns (e.g., flows and requirements), yields related to the profits generated by production, and the number of customers acquired leveraging manufacturing feasibility. **Viewpoints that must be considered** Confidential production information includes such as equipment/tools installed in clean rooms (i.e., manufacturer model numbers), the physical layout of how/where they are set up, and data contained inside the equipment for configuration purposes. Therefore, it is necessary to establish protective processes and conduct monitoring and audits, such as restricting and authorizing entry and exit to the factory and implementing regulations on photography Equipment/tools containing confidential production information require strict identity management, authentication, and access control, since on-site, visiting, or remotely working field support members have access to equipment/tools using the maintenance authorities granted to them under the maintenance agreements concluded with equipment/tool manufacturers.	managed by organization **Threats** • Protected data has been taken out improperly by a mallicious entity of the organization • Physical destruction of media • Identity spoofing of a proper user **Vulnerabilities** • Data protection at a predefined level of confidentiality is not implemented • The organization does not confirm the safeness of data storage organizations and/or systems before and after signing contracts • Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information **Targeted elements** • Organizations: device manufacturers • Organizations: contract	• PR.IR-02 Protection of Technical Assets from Environmental Threats Eco: protection against environmental threats • RC.RP-04 Establishment of Operational Rules Eco: establishment of operational rules **[CPSF's measure requirement IDs]** • CPS.AM-6 • CPS.BE-3 • CPS.DS-8

<table>
<tr><td></td><td></td><td>maintenance manufacturers (e.g., manufacturers of equipment, facilities, parts, and materials)

[CPSF's vulnerability IDs]
• L1_1_a_DAT
• L1_1_a_SYS
• L1_1_b_SYS
• L3_1_a_DAT
• L3_1_a_SYS
• L3_1_c_ORG</td><td></td></tr>
<tr><td></td><td rowspan="2">(5) Risk management/policy/resilience Characteristics
In a semiconductor device factory, the impact of cybersecurity is particularly high in the OT zone, and thus the company must assess risks in order to accurately understand the situation of its OT zone. It then must manage those risks, develop risk policies, and incorporate cybersecurity measures into its BCP.

Viewpoints that must be considered
Companies must implement risk management, risk policies, and BCP in accordance with their own business situation, after taking into account the characteristics and viewpoints that must be considered for semiconductor device factories.</td><td>Security incidents to be assumed
• The security incidents prevent their business from continuing properly</td><td rowspan="2">[NIST's CSF 2.0 Semiconductor Manufacturing Profile]
• GV.RM (all): Risk Management Strategies
• GV.PO (all): Policies
• GV.OV (all): Supervisors
• ID.IM (all): Improvements</td></tr>
<tr><td>Threats
All threats

Vulnerabilities
• Appropriate procedures for security risk management have not been established
• Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management</td></tr>
<tr><td></td><td></td><td></td><td>[CPSF's measure requirement IDs]
• CPS.GV (all)
• CPS.RA-4
• CPS.RA-6
• CPS.GV-4
• CPS.RM (all)
• CPS.SC-6
• CPS.SC-7
• CPS.SC-11
• CPS.IP-7</td></tr>
</table>

		Targeted elements • Organizations: device manufacturers **[CPSF's vulnerability IDs]** • L1_1_a_ORG • L1_1_a_PRO • L1_1_b_ORG • L1_1_b_PRO • L1_1_c_ORG • L1_1_c_PRO	• CPS.DP-4 • CPS.RP-3 • CPS.CO-2 • CPS.CO-3 • CPS-IM (all)
	(6) Operations (monitoring / response / recovery / improvement) **Characteristics** With the goal of mitigating the impact of an incident on business operations, monitor networks and systems to identify of security breaches and analyze data to determine whether there are any occurrence of threats or incidents. Appropriate action must also be taken to contain incidents and ensure early restoration. **Viewpoints that must be considered** The goals of cyberthreat detection and measures are to respond to early alerts to prevent data loss, minimize their impact, and resume business as quickly as possible. In addition, factories must implement security defense measures for important assets involving the acquisition of logs related to incident detection and tracking, and must build an incident response framework (i.e., FSIRT) designated for their OT zone. **Examples of specific measures** Specific examples that will serve as reference when	**Security incidents to be assumed** • The security incidents prevent their business from continuing properly **Threats** • All threats **Vulnerabilities** • The organization has not established a framework for accurately detecting security incidents • The organization has not established a framework for accurately handling security incidents • People are unable to take appropriate action when a security incident	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • DE.AE (all): Analysis of Adverse Events • RS.MA (all): Incident Management • RS.AN (all): Incident Analysis • RS.CO (all): Incident Reporting and Communication • RS.MI (all): Incident Mitigation • RC.RP (all): Execution of an Incident Recovery Plan • RC.CO (all): Incident Recovery Communication **[CPSF's measure requirement IDs]** • CPS.AE (all) • CPS.DP-2 • CPS.DP-3 • CPS.RP (all) • CPS.CO (all)

	advancing the consideration of measures are shown in Section 4.3.	arises • The organization has not developed internal procedures for security incident handling • Security incidents are not treated in the business continuity plan. This means a highly hazardous security incident hinders the organization's business continuity when it occurs **Targeted elements** • Organizations: device manufacturers **[CPSF's vulnerability IDs]** • L1_3_a_ORG • L1_3_a_PEO • L1_3_a_DAT • L1_3_a_PRO • L2_1_b_PRO • L2_1_c_PRO • L2_2_a_PRO	• CPS.AN (all) • CPS.MI (all) **[SEMI E187 - Manufacturing Reference]** 3.8 Prevent, Detect and Respond Overview: outlines key points to protect the fab area, including security monitoring as well as cyberattack detection, containment, and recovery
	(7) Awareness raising and training Characteristics Semiconductor device factories face a high risk of being targeted by industrial espionage and other types of government-sponsored APT attacks due to the scale of impact a factory stoppage could have on businesses	**Security incidents to be assumed** • The security incidents prevent their business from continuing properly	**[NIST's CSF 2.0 Semiconductor Manufacturing Profile]** • PR.AT (all): Awareness Raising and Training • ID.IM-02 Recognition of Points that Need to be Improved

	operations as well as the fact that confidential production information, which affects their competitiveness, is handled in the factories' fab areas. Semiconductor device factories are supported by an extremely large number of people, including employees who support the production process and contractors/subcontractors, which includes employees of equipment manufacturers and facility manufacturers who are stationed on-site. **Viewpoints that must be considered** Cybersecurity risks are taken into account in business continuity plans, and companies must provide cybersecurity education and training that also covers the OT zone to all parties (e.g., employees and contractors/subcontractors) involved with the OT zone, in order to prepare for attacks targeting vulnerable areas. The content of cybersecurity education and training covering the OT zone should be periodically reviewed to address cybersecurity threats and vulnerabilities affecting the business. By providing personnel responsible for OT security with regular practical training and simulations, their incident response capabilities can be continuously improved. In addition, developing a skill map enables ongoing enhancement of on-site capabilities and helps prevent dependence on specific individuals.	**Threats** All threats **Vulnerabilities** • People are not fully aware of the security or safety risks that may concern them • People involved are not fully aware of how the organization's protected data should be handled for security reasons • People are unable to take appropriate action when a security incident arises **Targeted elements** • Organizations: device manufacturers **[CPSF's vulnerability IDs]** • L1_1_a_PEO • L1_1_b_PEO • L1_1_c_PEO • L3_3_a_PEO • L3_4_a_PEO • L3_4_b_PEO	Eco: recognition of points that need to be improved throughout the supply chain **[CPSF's measure requirement IDs]** • CPS.AT (all) • CPS.SC-9 **[SEMI E187 - Manufacturing Reference]** 3.9 User Awareness Training Overview: outlines key points for user education and training aimed at enabling them to appropriately respond to new threats

4 Examples of Specific Measures for Semiconductor Device Factories

Chapter 4 introduces specific examples that serve as reference when considering measures to be implemented at semiconductor device factories, based on the reference architecture defined in Chapter 2 and the measures of related frameworks organized in Chapter 3.

Table 4-1. Specific Countermeasure Examples

Specific countermeasure examples	
4.1	Asset management and vulnerability assessment of equipment/tools (3.2.1-(1))
4.2	Additional defense measures to minimize equipment/tool damage and to prepare for early recovery (3.2.1-(2))
4.3	Operations (monitoring, response, recovery, and improvement): FSIRT operations (3.3-(6))
4.4	Physical access restrictions (people entering/bringing objects in/making connections): physical measures in the fab area (3.2.1-(5))

4.1 Asset Management and Vulnerability Assessment of Equipment/Tools

In the OT zone's fab area of a semiconductor device factory, which is equivalent to a clean room environment, an extremely large number of equipment/tools (i.e., more than 2,000 units per factory) are continuously manufacturing products while automatically coordinating with systems and with other equipment. In order to achieve the production goals that are set for the factory, maintain semiconductor quality, protect confidential production information, and protect human lives and the environment, the factory must thoroughly search for and identify all assets that need to be managed from among the large number of equipment/tools installed in the fab area. Measures can effectively be implemented by weighing the degree of each asset's importance based on the scale of damage that it is assumed to incur. For each asset, the factory must obtain information concerning its vulnerabilities and threats, conduct an assessment, and determine its response priority level.

The interior of an equipment/tool asset is complicated as it is comprised of multiple hardware devices and software components. Meanwhile, more than 40,000 vulnerabilities of equipment/tools are discovered annually. Against this backdrop, specific examples of measures will be presented by dividing factors of effective equipment/tool asset management and vulnerability assessment into the following five categories.

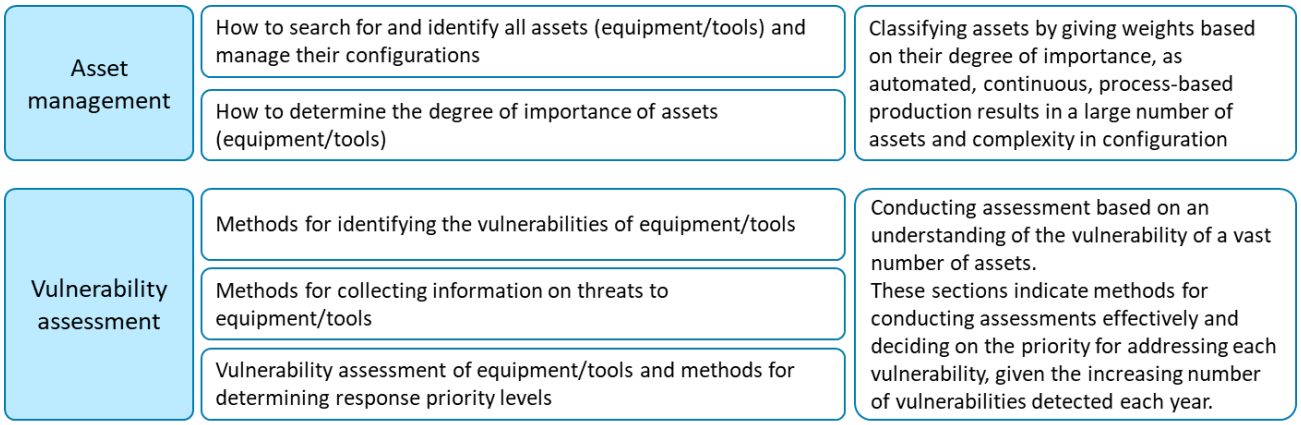


Figure 4-1. Effective equipment/tool asset management and vulnerability assessment

4.1.1 Determining the Identification and Configuration Management of Assets (Equipment/Tools)

In semiconductor device factories, more than 400 processes steps per factory, and an extremely large number of equipment/tools (numbering in the thousands), including those used for transferring items between processes, are coordinated and controlled by systems to carry out manufacturing. In order to satisfy the performance function of each process, each equipment/tool is comprised of a large number of hardware devices (note that transport equipment includes OHTs, stockers, FOUPs, etc.) such as a front PCs(Factory Facing Components), DCS, PLC, actuators, and sensors as well as software components for coordinating with multiple systems and controlling internal devices. Furthermore, confidential production information such as design information and recipes are stored and managed in equipment/tools. Examples of measures for searching for and identifying all equipment/tool assets that are to be managed and for managing their configurations are presented below.

As for the asset management carried out in the fab area, since the number of core equipment/tools is large and the internal configurations of those assets are complex, resulting in asset configurations that include contain confidential production information. Therefore, factories must prescribe their scope of management from the aspects of hardware devices, software components, confidential information, and security measure information. In order to implement effective asset management for security measures, it is important to define configuration management targets that facilitate the efficient operation of vulnerability assessments.

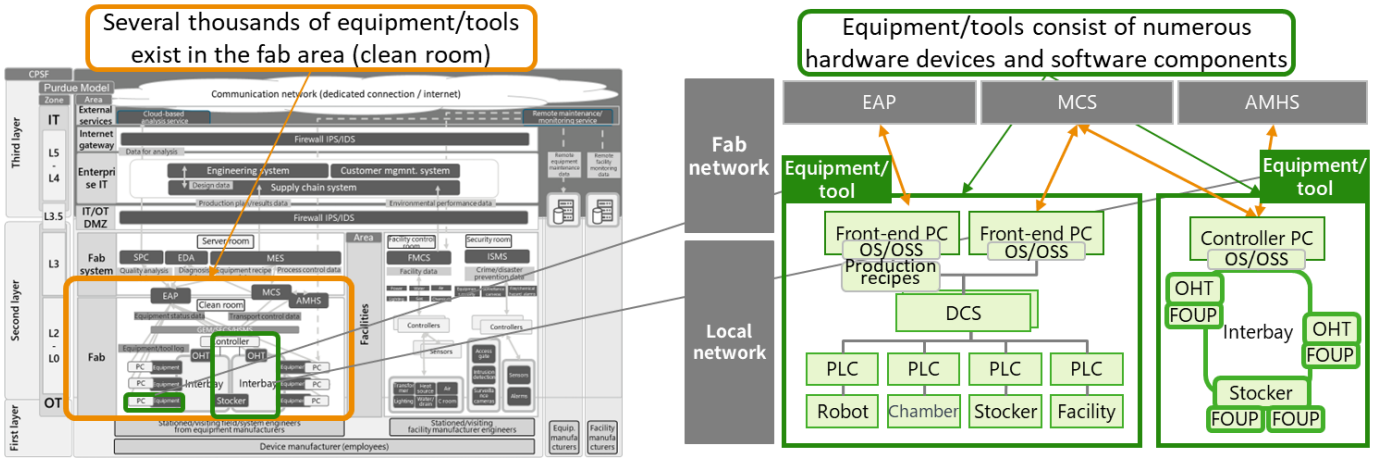


Figure 4-2. Configurations of Fab Area Assets

In the fab area, all equipment/tool assets related to the manufacturing process must be searched for and identified. Factories are then required to obtain knowledge about and manage the configurations of hardware devices, software components, confidential information, and security measure information found in the identified equipment/tools assets from a vulnerability management perspective.

- Hardware devices equipped with any of the following functions inside equipment/tools are subject to management: the fab network connection function; the console operating function; the storage medium connection function; the confidential information storage function; and the security measure function. The front PCs and controller PCs inside equipment/tools and the firewall connected to the fab network inside the equipment shall, in principle, be subject to management, but hardware equipped with the above functions, such as DCS and PLC, shall also be subject to management by taking into consideration cyber risks caused by maintenance work.
- The scope of software components subject to management include the OS and open-source software (OSS) of the targeted hardware devices found inside the above equipment/tools. In accordance with the security requirements for computer operating systems mentioned in SEMI E187:7 (i.e., E187.00-RQ-00001-00 and E187.00-RQ-00002-00), information on software package dependencies and software compatibilities provided by equipment manufacturers are subject to management.
- Confidential information covers confidential production information stored in equipment/tools. Circuit design information, recipes, process configurations, etc. are subject to management.
- Security measure information covers how SEMI E187's baseline requirements are applied to the body of an equipment/tool. In SEMI E187's baseline requirements, the requirements for implementing efficient vulnerability assessments are subject to management, such as patch application conditions, anti-malware measures (i.e., EPP and hardening measures), access control (i.e., privilege separation

management), network management (i.e., microsegmentation and communication control conditions), and security monitoring (i.e., event logs, EDR, and NDR).

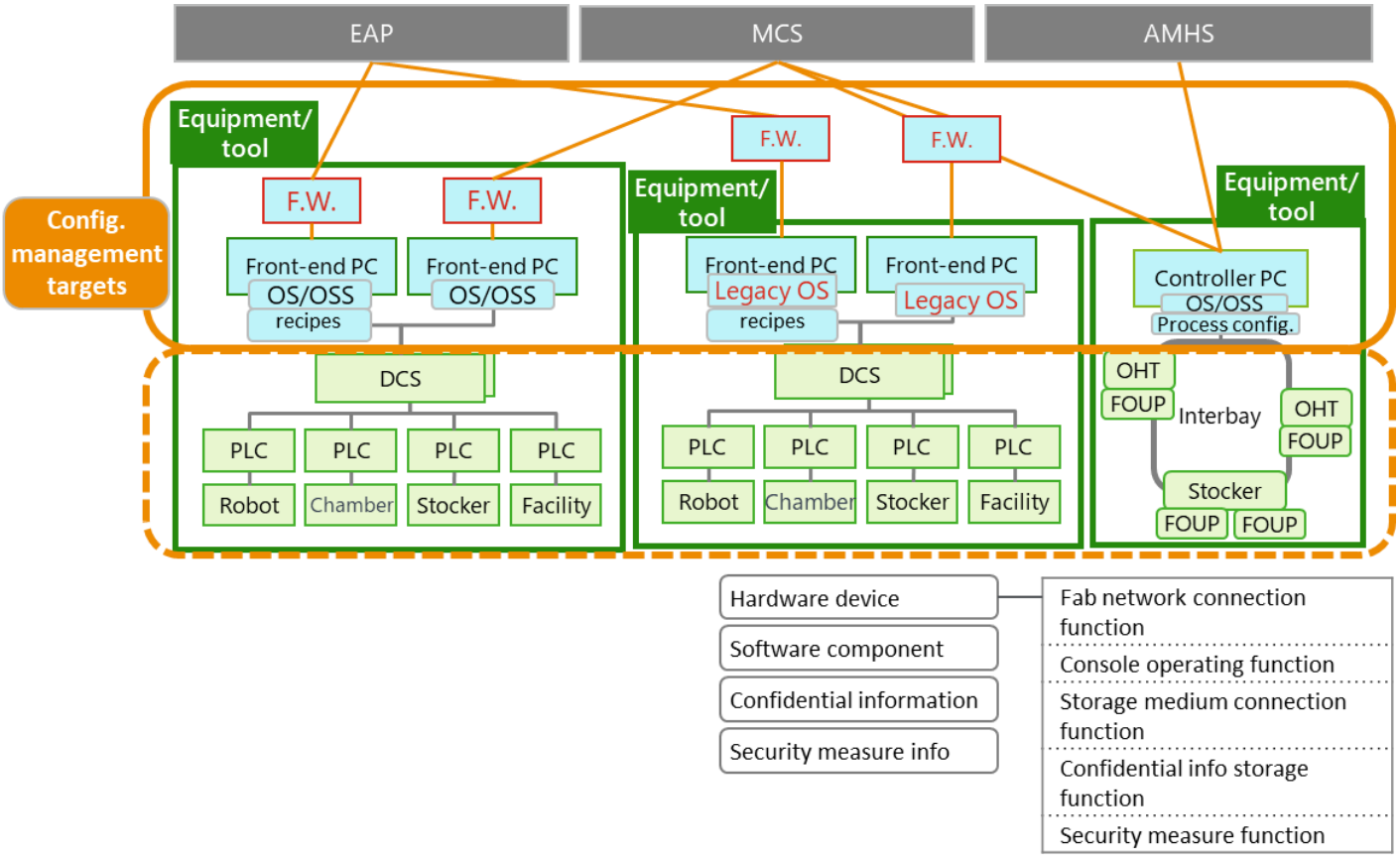


Figure 4-3. Configuration Management Targets in the Fab Area

Equipment/tools are used for an extended period of time, averaging more than 20 years. During this period, hardware devices and software components may be modified due to functional improvements, enhancements, or security measures for the equipment. Therefore, it is necessary to continuously review and update configuration management accordingly.

Although the hardware devices and software components targeted for equipment/tool configuration management are narrowed down from a vulnerability perspective with the aim of performing asset management effectively, it is desirable that factories confirm the configuration management methods (i.e., scope of providing SBOM information, implementing vulnerability assessments, and providing security patches) of security measures for equipment/tools written in the field support/maintenance agreements outlined in device manufacturers and equipment manufacturers and operate accordingly.

In October 2024, the industry group, SEMI, standardized a framework for acquiring cybersecurity status report information, such as OS information, for computer devices installed in equipment/tools that are connected to fab

networks (i.e., SEMI E191[9]) to serve as reference information, and the implementation of a function to provide this report by equipment/tools is expected to grow in the future.

For guidance on how to approach configuration management for equipment/tools, refer to Section 4-1, "Clarification of the Scope of SBOM Application"[10] of the Ministry of Economy, Trade and Industry's Guide of Introduction of Software Bill of Materials (SBOM) for Software Management.

4.1.2 Determining the Degree of Importance of Assets (Equipment/Tools)

Nation-state APT attacks are also occurring in the semiconductor industry, and attackers always have a specific target in mind when implementing cyberattacks. To prepare for cyberattacks, semiconductor device factories must clarify which assets should be protected and must determine the degree of importance of each asset in advance by ascertaining to what degree the business will suffer damage in the event a cyber incident occurs. Effective risk assessments, defense measures, vulnerability assessments, and operational responses can be implemented by treating the degree of importance assigned to an asset as the level of priority the asset should be given.

Each company shall decide how to determine the degrees of importance of factory assets in light of its business risk requirements, but this section will provide countermeasure examples on the criteria for determining the degrees of importance of assets that must be protected from the risk of cyberattacks occurring at semiconductor device factories and how to efficiently prescribe the degrees of importance.

Criteria for determining the degrees of importance of assets in semiconductor device factories

The criteria for determining the degrees of importance are divided into the risk areas shown below for a semiconductor device factory to achieve its production goals, maintain semiconductor quality, protect confidential production information, and protect human lives and the environment. Reference examples of the degrees of importance (i.e., high, medium, and low) are also indicated below.

(1) Determining the degrees of importance for achieving production goals and fulfilling supply responsibilities

The production lead time in semiconductor device factories is relatively long (e.g., three to six months), and limited production capacity within the industry. Therefore, if a production stoppage causes inventories to drop below the safety inventory levels, factories will not be able to fulfill their supply responsibilities to semiconductor users/customers, posing

[9] https://store-us.semi.org/products/e19000-semi-e191-specification-for-computing-device-cybersecurity-status-reporting
[10] https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

risks of impacting the supply chain. In particular, during the pre-process stage, where circuits are repeatedly formed on silicon wafers through process-based manufacturing, incidents such as prolonged performance degradation or equipment/tool stoppages in critical processes can prevent factories from achieving their planned production targets. This may lead to significant business impacts, such as failing to meet delivery deadlines. Furthermore, once production is halted, substantial time and costs may be required to resume operations, and all in-process wafers may be discarded, resulting in total losses.

In cases where target assets are damaged, it is effective to assess their importance based on the number of days production is suspended in relation to production goals, as well as the number of days market supply is disrupted with respect to supply responsibilities.

(2) Determining the degrees of importance for maintaining semiconductor quality

As for inspection equipment/tools used to inspect quality in each semiconductor manufacturing process, factories must take into consideration reliability (i.e., that products are manufactured correctly) (e.g., unauthorized installation of hardware Trojans into chips during the manufacturing process) in addition to the quality assurance of semiconductors, including the Product Liability Act (“PL Act”).

It would be effective to determine the degree of importance of a target asset based on the yield rate with regard to yield impact and based on the presence or absence of market quality defects or the impact of the PL Act with regard to market quality impact that would result in the case that the asset is damaged.

Each country has its own laws and regulations related to quality, such as the Product Liability Act (“PL Act”) and the EU’s Cyber Resilience Act (CRA). Therefore, factories must also take into consideration the risk of facing damages or punitive measures due to a violation.

(3) Determining the degrees of importance for protecting human lives and the environment as well as complying with laws

As for equipment/tools used in the semiconductor production process, factories must conduct safety and security checks regarding the use of inorganic compounds and radioactive substances that pose risks to human health and the environment, water pollution caused after cleaning wafers, and air pollution caused by exhaust gases emitted after plasma production. Factories also check the direct impact of such equipment/tools on laws and regulations such as environmental laws and the Industrial Safety and Health Act.

It would be effective to determine the degree of importance of a target asset in light of the risk of sustaining injury with regard to human life, the impact on the local community with regard to the environment, and the impact on the Industrial Safety and Health Act and environmental

laws with regard to laws and regulations that would result in the case that the asset is damaged.
The Safety and Security Requirements Consideration Guide for Control Systems[11] has been published by the IPA regarding safety.

(4) Determining the degrees of importance for protecting confidential production information

Recipe information that affects product quality and yield, confidential information that affects the competition with other companies such as configuration parameters, as well as confidential production information such as technical information of other companies and design information, are stored in each equipment/tool. Therefore, factories must take into consideration the impact on business and the losses incurred in the event confidential production information managed by any equipment/tool is leaked to a competitor.
It would be effective to determine the degree of importance of a target asset based on the estimated loss amount with regard to the protection of confidential production information that would result in the case that the asset is damaged.

(5) Determining the degrees of importance in terms of the financial impact of equipment/tools

Since the equipment/tools are technically configured to utilize nanotechnology, they are considered assets with a high asset value per unit. Therefore, factories must determine degrees of importance by simulating the destruction of these assets (e.g., equipment/tools used for the exposure process—whose technology is increasingly being miniaturized—have asset values higher than that of equipment/tools used for other processes).

As reference information for fleshing out determination criteria, examples of how to measure the importance of the results of typical risk analyses indicated in Annex A.2.3.3.7 of IEC 62443-2-1 (Table A.2 – Typical consequence scale) and Section 4.2 titled “The Degree of Importance of Assets” of the IPA’s Security Risk Analysis Guide[12] for Control Systems are shown in Table 4-2.

This table categorizes the risk (severity of damage) when an asset is attacked and damage occurs into three levels. It serves as a criterion for defining the importance of the asset based on these values.

Furthermore, the details of management resource damage caused by cybersecurity attacks must be taken into consideration.

[11] https://www.ipa.go.jp/archive/digital/iot-en-ci/mieruka/20180319.html
[12] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

Table 4-2. Degrees of importance of equipment/tools

Risk area	Expected business damage and impact on business continuity in the event an asset receives a cyberattack							Value as a system asset	
	Business continuity (availability)		Semiconductor quality (integrity)		Safety of industrial activities (HES)		Compliance with laws, regulations, etc.	Information leakage (confidentiality)	Financial impact
Degree of importance	Production stoppage	Impact on supplies	Impact on yield	Impact on market quality	Work-related accident	Environmental damage		Leakage of confidential production information	Damage to an equipment/ tool
High	1 day or more	7 days or more	Impact: Yield rate of below 50%	Results in market quality defects and will be subjected to the PL Act	Death	Serious incident of the region	Strict oversight and restrictions due to serious violations of government regulations or industry standards	Affects competitive advantage Loss of 5% or more in revenue	
Medium	1 hour or more	2 days or more	Impact: Yield rate of 50% to 70%	Results in market quality defects but will not be subjected to by the PL Act	Leave of absence or a severe injury	Complaints or an impact on the local community	Oversight due to serious violations of government regulations or industry standards	Affects competitive advantage Loss of 1% to 5% in revenue	
Low	Less than 1 hour	Less than 1 day	Impact: Yield rate of 70% or more	Will not result in market quality defects	First aid or an injury that must be recorded	No complaints	No effect on compliance with laws and regulations	Does not affect competitive advantage No impact on revenue	

(Reference) Details of management resource damages caused by cybersecurity attacks

Management resource	Damage details
People	Occurrence of a work-related accident (i.e., death or injury of an employee) due to a malfunctioning equipment/tool or facility
Components	Damage to an equipment/tool or facility, total loss and disposal of silicon wafers, or deterioration of product quality (or yield), safety, etc.
Money	Loss of profit opportunities, or incurring damages or expenses
Data	Leakage of important information assets, such as confidential production information (e.g., recipes, etc.) or information on new processes and technologies
Reputation	Lack of moral responsibility, breach of contract with business partners, undermining a relationship of trust, or a negative impact on the brand image

In order to efficiently determine the degree of importance of a large number of assets subject to management in a semiconductor device factory, instead of making individual decisions for each asset, factories are able to divide all assets into business units based on business risk as in a BCP, group assets with the same function within each business unit as an asset group unit, and then determine the degree of importance of each asset group.

For equipment/tool assets in the fab area, where assets are particularly abundant, it would be efficient to divide them into production line units (i.e., lines by wafer size) by treating supply responsibilities as business units, further group each business unit's equipment/tools that are used in the same production process (e.g., oxidation, coating, exposure, and inspection, which are considered functional units) as an asset group unit, and then set the degree of importance for each asset group.

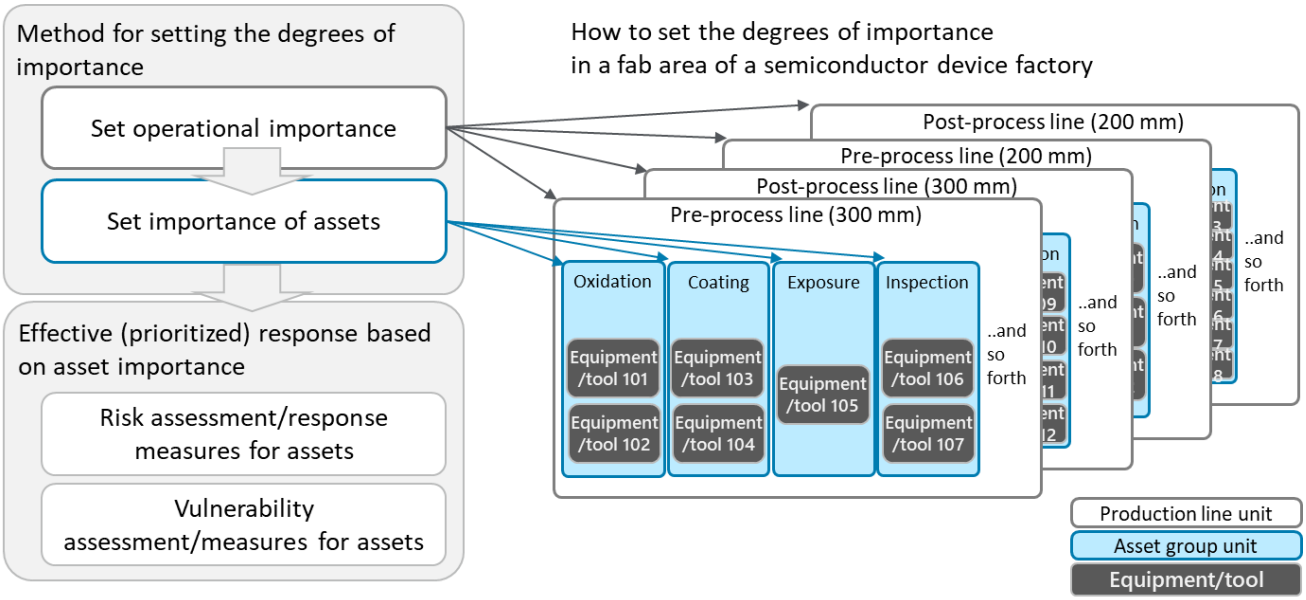


Figure 4-4. Efficiently Setting Degrees of Importance

An example for calculating the degrees of importance of equipment/tool assets installed in the fab area of a semiconductor device factory is shown below.

Equipment/tool assets in the fab area are first grouped into production lines, defined as business units, and the assets of each production line are further divided into process units grouped by function. The degrees of importance of assets are calculated for each of the risk areas prescribed as the standards for the degrees of importance.

For asset groups grouped by production line and by process, it would be effective to determine their degrees of importance by referring to the following internal information that is currently being used by the company.

- Business continuity: Business continuity planning information
- Semiconductor quality and safety of industrial activities: process quality management information (process FMEA)

- Compliance with laws and regulations: process quality management information and confidential information management
- Confidential information: confidential information management
- Financial impact: fixed asset information

Risk areas				Expected business damage and impact on business continuity in the event an asset receives a cyberattack (operations, asset)							Value as a system asset	
By operation: Production line		By asset group: Process		Business continuity (availability)		Semiconductor quality (integrity)		Safety of industrial activities (HES)		Compliance with laws, regulations, etc.	Information leakage (confidentiality)	Financial impact
Wafer size	Line	Process/ equipment group	# of equipment/ tools	Production stoppage	Impact on supplies	Impact on yield	Impact on market quality	Work-related accident	Environmental damage		Leakage of production information	Damage to an equipment/ tool
300 mm	Pre-process	Oxidation	2	Medium	Medium	Low	Low	**High**	**High**	**High**	Medium	
		Coating	2	Medium	Medium	Medium	Low	Medium	Medium	Medium	Medium	
		Exposure	1	**High**	**High**	Medium	Low	Medium	Medium	Medium	**High**	
		Inspection	2	Medium	Medium	**High**	Low	Low	Low	Low	**High**	
	Post-process	Dicing	4	Medium	Low	Low	Low	Low	Low	Low	Low	
		Bonding	4	Medium	Low	Low	Low	Low	Low	Low	Low	
		Inspection	4	Medium	Low	**High**	**High**	Low	Low	Low	Medium	
200 mm	Pre-process	Oxidation	3	Low	Low	Low	Low	**High**	**High**	**High**	Low	
		Coating	3	Low	Low	Medium	Low	Medium	Medium	Medium	Low	
		Exposure	3	Low	Low	Medium	Low	Medium	Medium	Medium	Medium	
		Inspection	3	Low	Low	**High**	Low	Low	Low	Low	Medium	
	Post-process	Dicing	6	Low	Low	Low	Low	Low	Low	Low	Low	
		Bonding	6	Low	Low	Low	Low	Low	Low	Low	Low	
		Inspection	6	Low	Low	**High**	**High**	Low	Low	Low	Low	

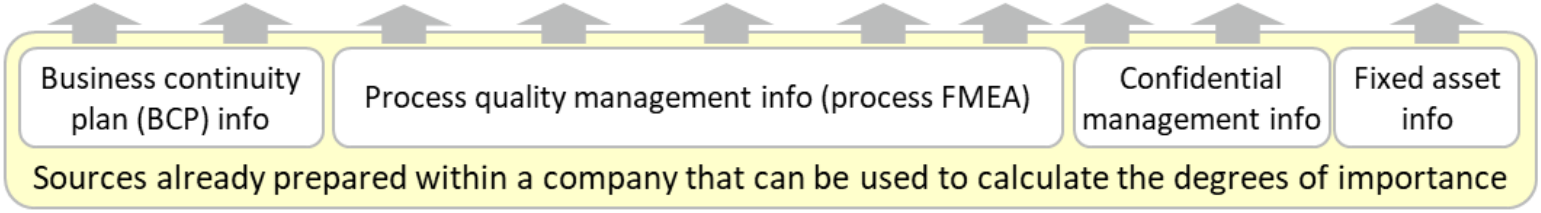


Figure 4-5. Example for Calculating the Degrees of Importance of Equipment/Tool Assets

On how to set degrees of importance, refer to Subsection 3.1, Step 1. titled "Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc." under Section 3 titled "How to proceed with planning and introduction of security measures" of the Ministry of Economy, Trade and Industry's The Cyber/Physical Security Guidelines for Factory Systems[13], among others.

4.1.3 Methods for Identifying the Vulnerabilities of Equipment/Tools

As basic information for assessing the vulnerabilities of an equipment/tool, factories must obtain vulnerability information by identifying the weaknesses of the component targeted in the configuration management of the equipment/tool. Examples are shown below such as sources of vulnerability information and advice on how to narrow down methods for identifying the vulnerabilities of equipment/tools from the information on vulnerabilities discovered, which annually exceeds 40,000 cases.

Sources of vulnerability information include:

- Identification from vulnerability information publicly disclosed by government agencies or public institutions such as CVE, NVD and JVN
- Identification from security vendor information (e.g., MSRC) and open source information (e.g., OpenSSF)
- Identification from vulnerability information provided by equipment manufacturers
- Identification using a vulnerability scanning tool (e.g., SCAP scanner)

In identifying the vulnerabilities of equipment/tools, effective methods are identifying not only vulnerability information obtained in the IT zone, but also using the vulnerability information provided by equipment manufacturers (which are provided by taking into consideration security measures for the equipment/tools) or using a vulnerability scanning tool (i.e., SCAP scanner), which are considered more efficient methods.

Since there is a large number of equipment/tool assets, factories must implement effective measures that take into account operational man-hours. The following considerations can be made to achieve this:

(1) Identifying the vulnerabilities in highly important assets and prioritize them accordingly
(2) Narrowing down the targets for vulnerability identification by leveraging security measure information obtained during the management of equipment/tool assets (e.g., microsegmentation or application execution permission-based measures)
(3) Obtaining vulnerability information by narrowing down target assets after having conducted a vulnerability assessment

[13] https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

Based on vulnerability information provided by equipment manufacturers, it is possible to include vulnerability management requirements in field support and maintenance agreements with equipment manufacturers by referring to the basic requirements for addressing vulnerabilities of equipment/tools recommended in SEMI E187 and SEMI E188. This approach enables the efficient establishment of operations and a framework for identifying vulnerabilities. (refer to Section 9.2 of "Vulnerability Mitigation" of SEMI E187 and Section 9.2 of SEMI E188 and "Checking for Vulnerabilities on the Manufacturing Equipment").

In addition, given the large number of equipment/tools and components, one effective method is to identify remaining vulnerabilities using a vulnerability scanning tool (i.e., SCAP scanner) in order to identify how vulnerabilities are currently being treated, including whether additional defense measures are being implemented. Another effective method would be to identify remaining vulnerabilities referring the recommendations for vulnerability scanners provided in SEMI E187 COMPLIANCE GUIDANCE[14] and in accordance with the basic requirements of SEMI E188 (see "E187.00-RQ-00005-00E187.00-RQ-00008-00" of SEMI E187 COMPLIANCE GUIDANCE and Section 9.4 titled "NIST Security Content Automation Protocol (SCAP)" of SEMI E188).

When using a vulnerability scanning tool, some equipment/tools may experience performance issues (i.e., Stopping or degradation) when an active scanning system tool is used, factories must, prior to using a vulnerability scanning tool, determine operational details, such as deciding the scanning method to be used and coordinating the scanning date and time.

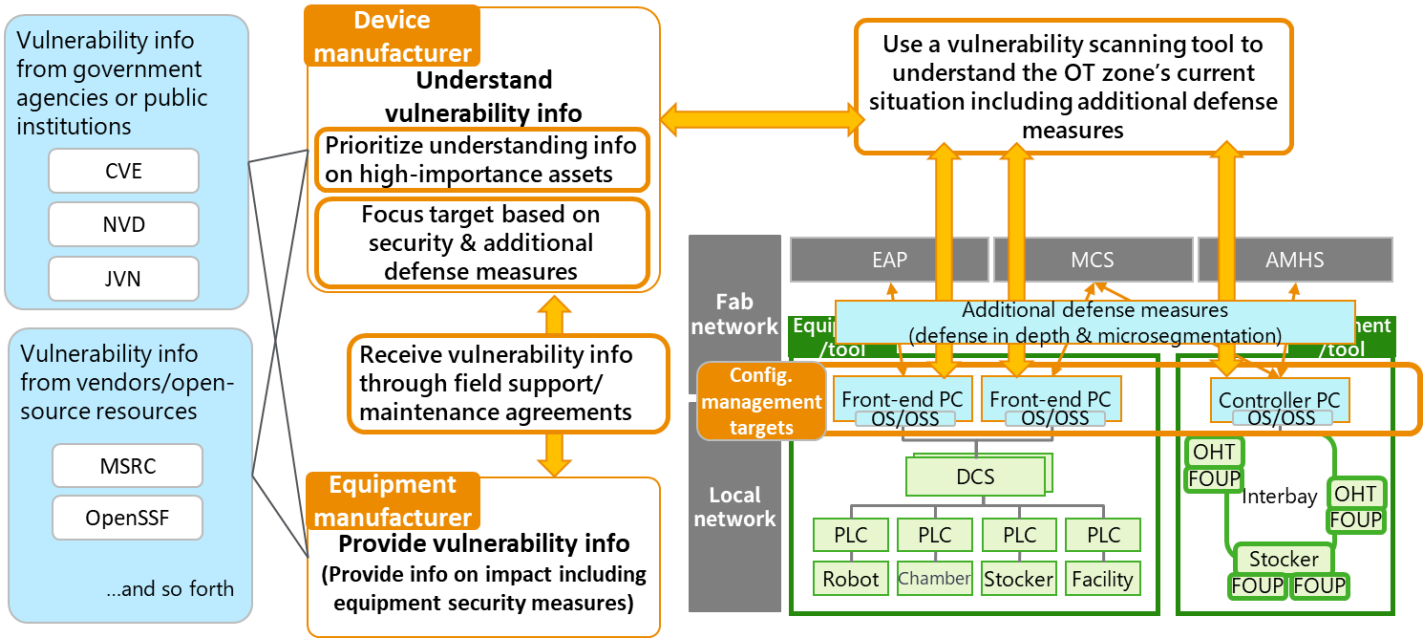


Figure 4-6. Methods for Identifying the Vulnerabilities of Equipment/Tools

[14] https://www.semi.org/en/standards-watch-2025-aug/navigating-semi-e187-new-cybersecurity-white-paper

4.1.4 Methods for Collecting Information on Threats to Equipment/Tools

The semiconductor industry is a high-risk industry from an economic security perspective, which includes the threat Nation-state APT attacks. There is a need to collect information on attacks targeting the industry (i.e., execution details of attack codes targeting critical vulnerabilities) as well as incidents occurrence information (including detected attack information) and to then leverage such information to assess vulnerabilities and implement preventive measures.

The following are methods for collecting threat information:

- Collecting information from government agencies or public institutions such as NISC, JPCERT/CC, IPA, CISA, US-CERT, ENISA, and CERT-EU
- Collecting information from CISA's Known Exploited Vulnerabilities (KEV) list and FIRST's Exploit Prediction Scoring System (EPSS), as well as leveraging the combined use of KEV and EPSS through the LEV framework
- Collecting information from industry-wide threat information sharing platforms, including, IT-ISAC Semiconductor Industry SIG, and J-CSIP[15] Semiconductor Industry SIG
- Collecting information obtained from the results of analyses conducted on the company's attack/incident information

Furthermore, regarding the collection of industry threat information, the IT-ISAC Semiconductor Industry SIG is active in the United States, while in Japan, the IPA's J-CSIP Semiconductor Industry SIG has begun its activities.

In addition to traditional methods of collecting information, such as public information disclosed by government agencies or public institutions, information on confirmed exploited vulnerabilities, and analysis results of the company's own attack and incident data, leveraging the details obtained from industry-wide threat information sharing allows companies to track the occurrence of attack codes (i.e., exploit codes) targeting vulnerabilities remaining in equipment/tools within the OT zone and fab area. It also enables the sharing of information on attack trends (i.e., monitoring results/updates) within the industry, which can then be utilized for vulnerability assessment and the implementation of preventive measures.

As a reference for identifying vulnerability information, the IPA updates "Control System Vulnerability Information Disclosed by CISA (for the Latest Month)"[16] every Monday, allowing companies to monitor the occurrence attack codes (i.e., exploit codes) are being used.

[15] https://www.ipa.go.jp/security/j-csip/about.html
[16] https://www.ipa.go.jp/security/controlsystem/icsadvisories.html

With the cooperation of the Ministry of Economy, Trade and Industry, the IPA's J-CSIP (Initiative for Cyber Security Information sharing Partnership of Japan) was established in 2011 to prevent the escalation of damage caused by cyberattacks. It primarily serves as an information sharing and early response platform for manufacturers of devices used in critical infrastructures such as heavy industry products and heavy electric machinery. Starting in April 2025, its Semiconductor Industry SIG will begin operations.

For information regarding KEL, EPSS, and LEV, the NIST Cybersecurity White Paper titled "NIST CSWP 41 Likely Exploited Vulnerabilities"[17] serves as a useful reference.

4.1.5 Vulnerability Assessment of Equipment/Tools and Methods for Determining Response Priority Levels

When vulnerability information for equipment/tools is obtained, it is necessary to identify the vulnerabilities of equipment/tools, assess their severity in the context of potential threats from attackers, and determine the appropriate response strategy (e.g., mitigate, avoid, or accept the vulnerabilities) as well as the timing of such actions. In addition, it is required to dynamically review the assessment of existing assets and vulnerabilities in response to new threats and environmental changes (e.g., the introduction or modification of equipment and tools), and to always make decisions based on the latest risk situation. In terms of the vulnerability assessment performed in the IT zone, vulnerability assessments are typically conducted using a quantitative approach based on the CVSS base score for discovered vulnerabilities. This allows for the adjustment of patch application timing and the implementation of interim mitigation measures before patches are applied. However, in the OT zone, applying patches to equipment/tools often faces constraints due to potential impacts on performance and operational limitations. As a result, it is often necessary to consider alternative measures, such as avoidance or mitigation strategies, instead of relying solely on patch application.

Particularly in the OT zone of semiconductor device factories, where a large number of equipment/tool assets are present, it is essential to adopt efficient and effective evaluation methods to enable appropriate decision-making during vulnerability assessments.

Examples of measures for performing effective vulnerability assessments:

To identify vulnerability information, cooperation with equipment manufacturers to pinpoint vulnerabilities that require countermeasures, thereby narrowing down the priorities for addressing them. Next, by using a vulnerability scanner to identify residual vulnerabilities after implementing countermeasures (including simulations), it becomes possible to evaluate their impact by

[17] https://csrc.nist.gov/pubs/cswp/41/likely-exploited-vulnerabilities-a-proposed-metric/final

incorporating environmental assessment criteria. Furthermore, for threat information collection, industry-specific threat intelligence provided by the J-CSIP Semiconductor Industry SIG and the IT-ISAC Semiconductor Industry SIG can be utilized. By integrating threat assessment criteria into the evaluation process, the selection of vulnerabilities that need to be addressed can be further refined based on their impact.

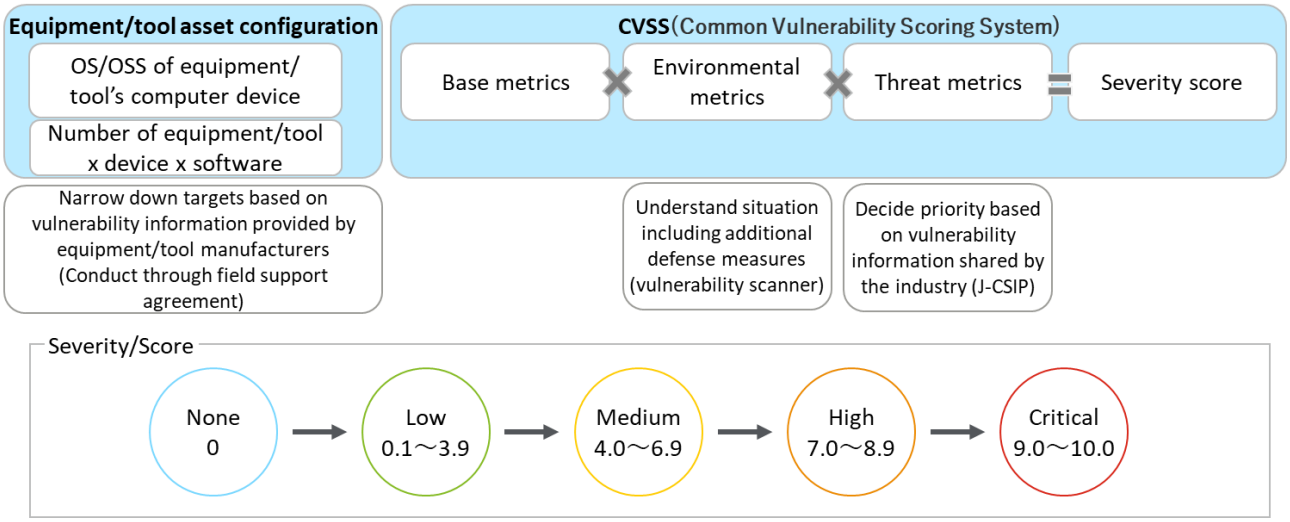


Figure 4-7. Vulnerability assessment using CVSS

(Reference) There are 18,000 components that constitute equipment/tool assets that must be managed
(2,000 equipment/tools x 3 computer devices x 3 software components = 18,000)
In 2024, there were over 40,000 CVE data (up 38% year-on-year), of which 231 were rated 10.0 (severity: critical)

SSVC makes it possible to make response decisions by taking environmental characteristics into account. Based on a vulnerability's exploitation status ("Exploitation"), defense status ("Exposure"), attack benefits ("Utility"), and business impact ("Impact"), one of the following responses ("Priority") that takes environmental characteristics into account is chosen: urgent response ("Immediate"), unscheduled response ("Out-Of-Cycle"), scheduled response ("Scheduled") or no response ("Defer").

As a result, factories can now objectively indicate and determine what responses to take toward highly severe vulnerabilities (i.e., an attack may occur whose attack code has already been created and whose impact on business would be significant) and perform assessments. Note that these vulnerabilities occur several times a year in the OT zone, and it is usually difficult to determine what responses to take toward them. When it comes to actual emergency responses, unscheduled responses, or scheduled responses, vulnerability avoidance (i.e., applying a patch or deactivating the attack route) or mitigation (i.e., adding detection items or enhancing monitoring capabilities) is implemented.

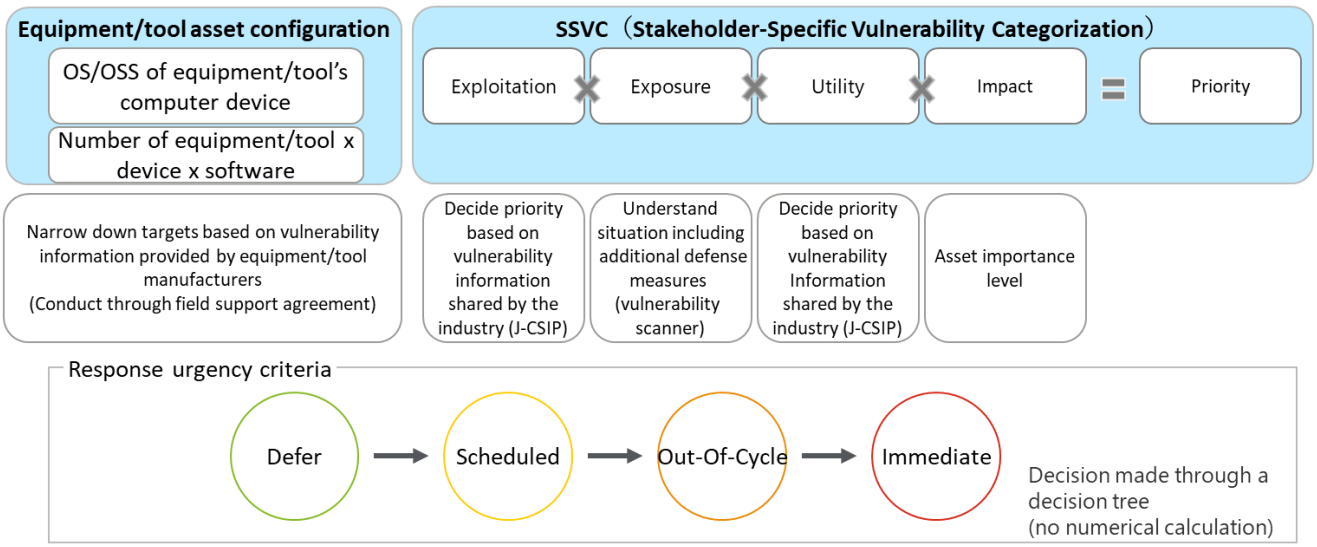


Figure 4-8. Vulnerability assessment using SSVC

4.2 Additional Defense Measures to Minimize Equipment/Tool Damage and to Prepare for Early Recovery

The OT zone contains a large number of assets. Equipment/tools for which it is difficult to address vulnerabilities are run in vulnerable situations, such as being unable to apply patches as a result of running on legacy OS over an extended period of time or for performance assurance reasons, or because patch application timings are limited due to continuous production. Communications between equipment/tools and the fab system and communications between equipment/tools are carried out using unencrypted/unauthenticated industry standard protocols that are prescribed as industry standards. Therefore, additional defense measures are required to safely operate equipment/tools and fab networks, which are important for continuous production.

The examples of measures below describe additional defense measures for producing devices safely, such as defense in depth, microsegmentation, and network-based security monitoring.

- Defense in depth is not limited to counter-intrusion measures implemented at entry points of cyberattacks. It also minimizes the forensic scope that needs to be covered in the event an incident occurs by protecting the internal area by dividing it into smaller zones or conduits depending on its use, function, or how security measures are being implemented after taking into account vertical and horizontal movements the attacker is expected to make after intrusion. In addition, it enables early recovery by containing the impacted area by dividing the internal area into multiple zones. Four examples of separation/division measures are shown below using the zones and areas defined in the

reference architecture for semiconductor device factories that was described in Chapter 2.

- Microsegmentation protects and enables the safe use of equipment/tools to which patches cannot be applied by dividing the internal area into multiple zones or changing conduit settings.
- By conducting security monitoring of the divided zones, network-based security monitoring enables the detection of cyberattacks at the initial stage and prevents the occurrence of damage caused by incidents.

Table 4-3. Overview of Network Security Measures

Network-based defense in depth, microsegmentation, and security monitoring			
1	Separation and communication restrictions by zone	Defense in depth: Reduces the ease of cyberattack intrusions and the spread of damage	Separates the entrance of the OT zone (i.e., separates it from the IT zone and internet zone by establishing a DMZ)
2	Separation and communication restrictions by area		Functions of fab systems, fabs (equipment/tools), and facilities
3	Separation and communication restrictions within an area		For each production plan (i.e., the process for each building/floor) in the fab area
4	Separation and communication restrictions by system use		Within an equipment's interface (I/F) system (e.g., for process/transportation purposes, for quality purposes, and for maintenance purposes)
5	Microsegmentation protecting equipment/tools	Microsegmentation	Additional security measures implemented by the equipment/tool itself
6	Network-based security monitoring	Security monitoring	Detects cyberattacks at the initial stage and prevents damage caused by incidents

Table 4-4. Detailed Network Security Measures

Network-based defense in depth, microsegmentation, and security monitoring	
1	**Separation and communication restrictions by zone** The OT zone network is separated from the IT zone network by establishing a DMZ using a firewall or the like, and communications between the two networks are restricted. (The OT zone is separated from the IT zone network and the internet.) （Orange frameworks in Figure 4-9）
2	**Separation and communication restrictions by area** In the OT zone network, the fab system area, the fab area, and the facility area are divided and communications between them are restricted. （Blue frameworks in Figure 4-9）
3	**Separation and communication restrictions within an area** Communications are restricted after dividing the network by system

	in the fab system area and by facility service in the facility area. Green frameworks in Figure 4-9 For the fab area, communications are restricted after dividing the network by process for which a production plan is created and executed. （Green frameworks in Figure 4-10）
4	**Separation and communication restrictions by system use** Even after dividing the fab area network into multiple processes, communications within the network are further divided and restricted by system use, such as those used for controlling processes between equipment systems, sending images and videos to check the quality of products, and coordinating with prediction/detection sensors. （Purple frameworks in Figure 4-11）
5	**Microsegmentation protecting equipment/tools** Zone division via microsegmentation is conducted for devices for which security measures cannot be implemented due to the use of a legacy OS or since patches cannot be applied in the equipment/tools, among other reasons. （Red frameworks in Figure 4-12） Consider applying virtual patches to equipment/tools that are more important.
6	**Network-based security monitoring** An anomaly detection tool (i.e., NDR) is installed in the divided network to log anomaly alerts and to monitor and detect anomalies.

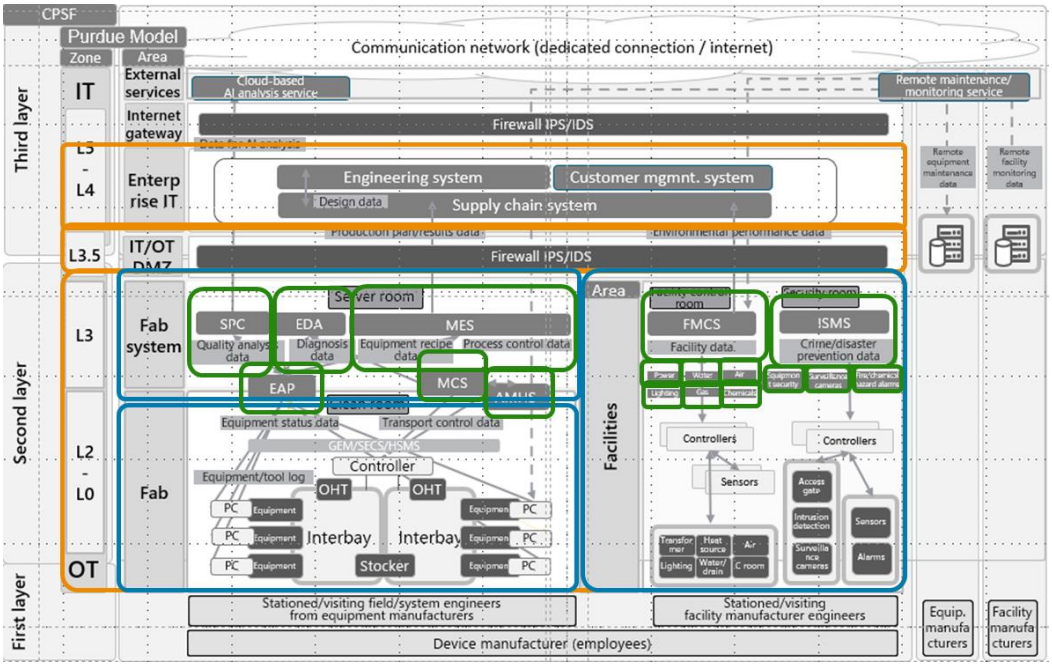


Figure 4-9. Overview of Network Segmentation (Zone and Area Level)

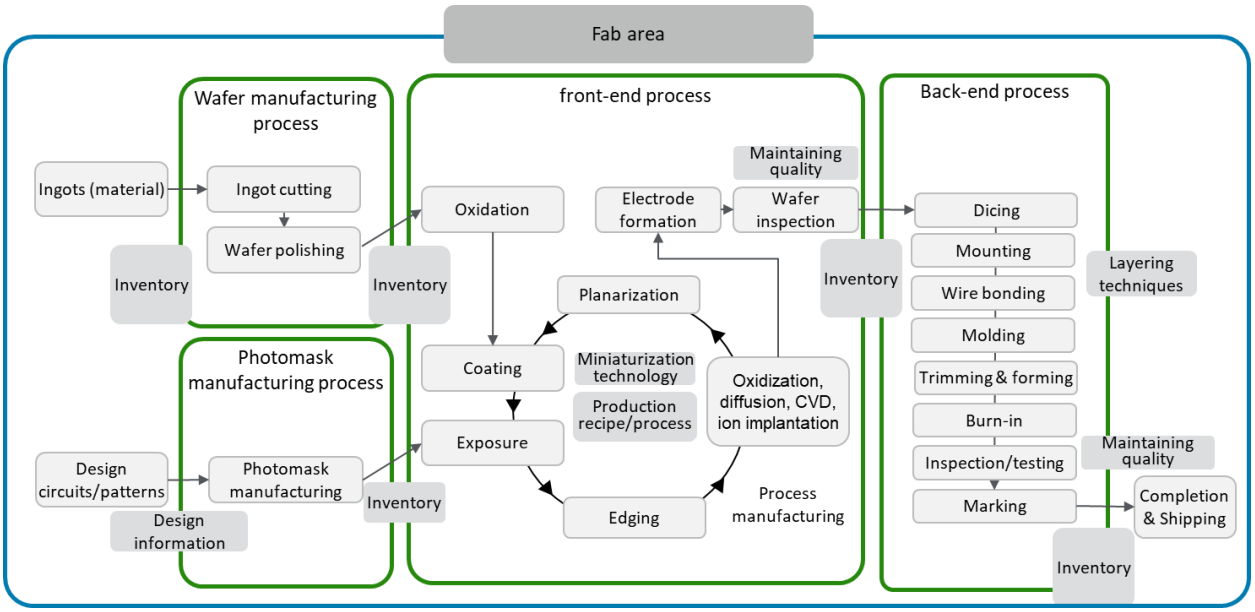


Figure 4-10. Detailed Network Segmentation in Fab Area (Process Level)

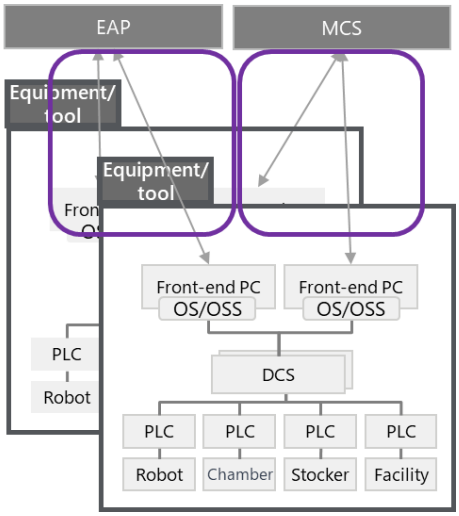


Figure 4-11. Detailed Network Segmentation for Equipment Systems

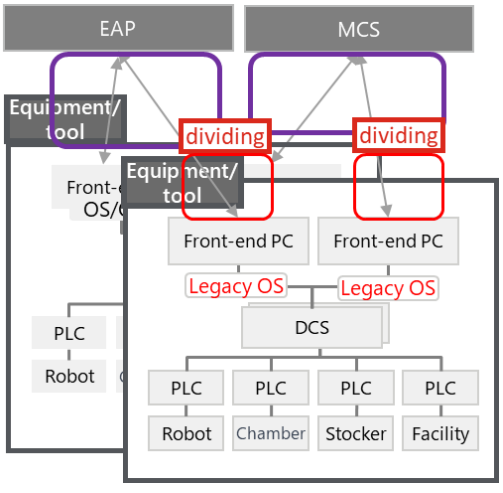
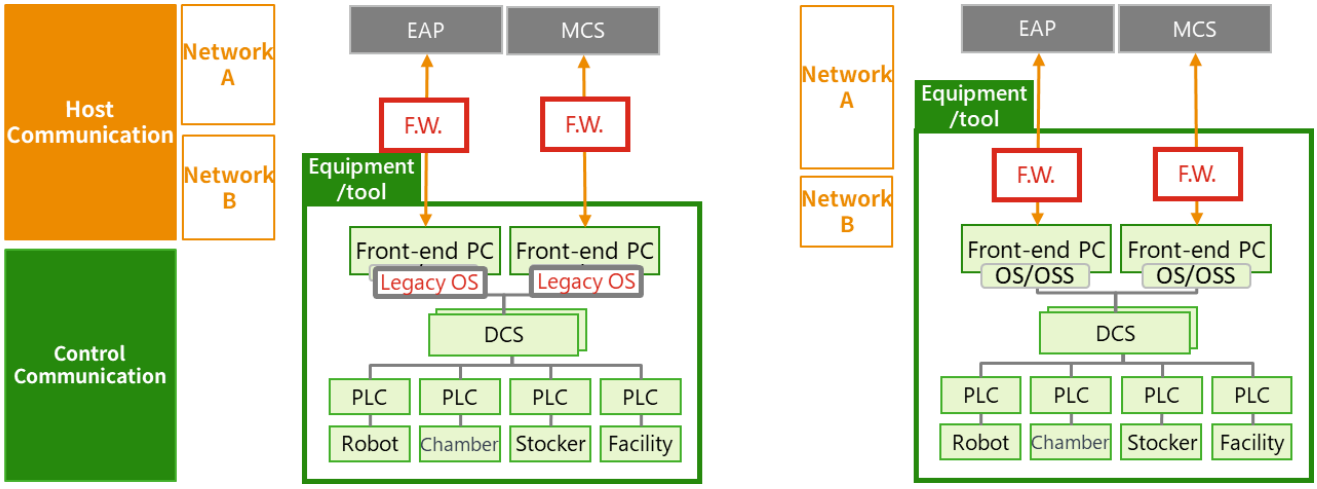


Figure 4-12. Example Configuration of Microsegmentation for Equipment/Tools

For equipment/tools in which a legacy OS is installed and run or equipment/tools to which security patches cannot be applied, it would be effective to conduct microsegmentation in which each computer device such as a pre-process PC and controller PC found inside the equipment/tools is treated as one zone.

Due to the cybersecurity enhancement of equipment/tools promoted by SEMI E187 and 188, which are standards for which the industry is currently implementing compliance measures, there are expectations that in the future, efforts will be made to make equipment/tools secure by enabling microsegmentation to be implemented in those equipment/tools. Companies will be expected to introduce/implement measures to respond to this change (including the installation of devices outside existing equipment/tools that are currently running) by confirming security measures and operations (e.g., recommended configurations, setting details, and operation methods) with equipment manufacturers and including these details in procurement specifications and field support/maintenance agreements.



Referred to Section 3.2 titled “Tool Configurations” of SEMI E187 - Manufacturing Reference (Cybersecurity Reference Architecture for Semiconductor Manufacturing Environments)

Figure 4-13. Components and Selection Criteria for Microsegmentation Configuration

When selecting the location of the firewalls (F.W.) shown in Figure 4-13, a firewall, router ACL, IPS, IDS, UTM, etc. must be selected and specified from the viewpoint of protecting the equipment/tool against threats based on its degree of importance. Functions such as VLAN, packet control, stateful, payload, anomaly, signature detection, virtual patch, etc., should be carefully evaluated to determine the required extent, taking costs into consideration. These decisions must then be reflected in procurement specifications and field support/maintenance agreements.

4.3 Operations (Monitoring, Response, Recovery, and Improvement): FSIRT Operations

In order to safely operate a manufacturing device factory and provide a stable supply of semiconductors, a company must clarify its own risks and implement measures in a planned manner, and it must also build a safety management framework necessary for making incident responses should a cyberattack occur. This section presents an example of a semiconductor device factory's Factory Security Incident Response Team (FSIRT), which is responsible for detecting cyberattacks occurring in the factory's OT zone, and for responding to and recovering from such cyberattacks. (This corresponds to three of the six core functions of the NIST CSF 2.0: "detect," "respond," and "recover.")

FSIRT, which is responsible for the factory's OT zone, shall respond appropriately to cyberattacks should they occur and prepare for such attacks during ordinary times by closely coordinating and cooperating with the Computer Security Incident Response Team (CSIRT), which is responsible for the IT zone's security, and the Product Security Incident Response Team (PSIRT), which is responsible for product security.

Semiconductor device factories handle an extremely large number of equipment/tools and facilities and are operated by a large number of maintenance personnel. Once an incident occurs, not only will the company suffer damage, but it will also greatly affect the company's responsibility to supply semiconductors to industries that use semiconductors. Therefore, FSIRT's operations, which include the following, are critical: taking proactive measures by detecting signs of an attack; making incident responses when an attack has been detected, which include preventing the damage from spreading and making an early recovery; and preparing for attacks during ordinary times.

As in the case of measures implemented against natural disasters, companies must, in advance, prepare a framework for making responses should an incident occur and must also establish procedures and provide education and training for carrying out those responses.

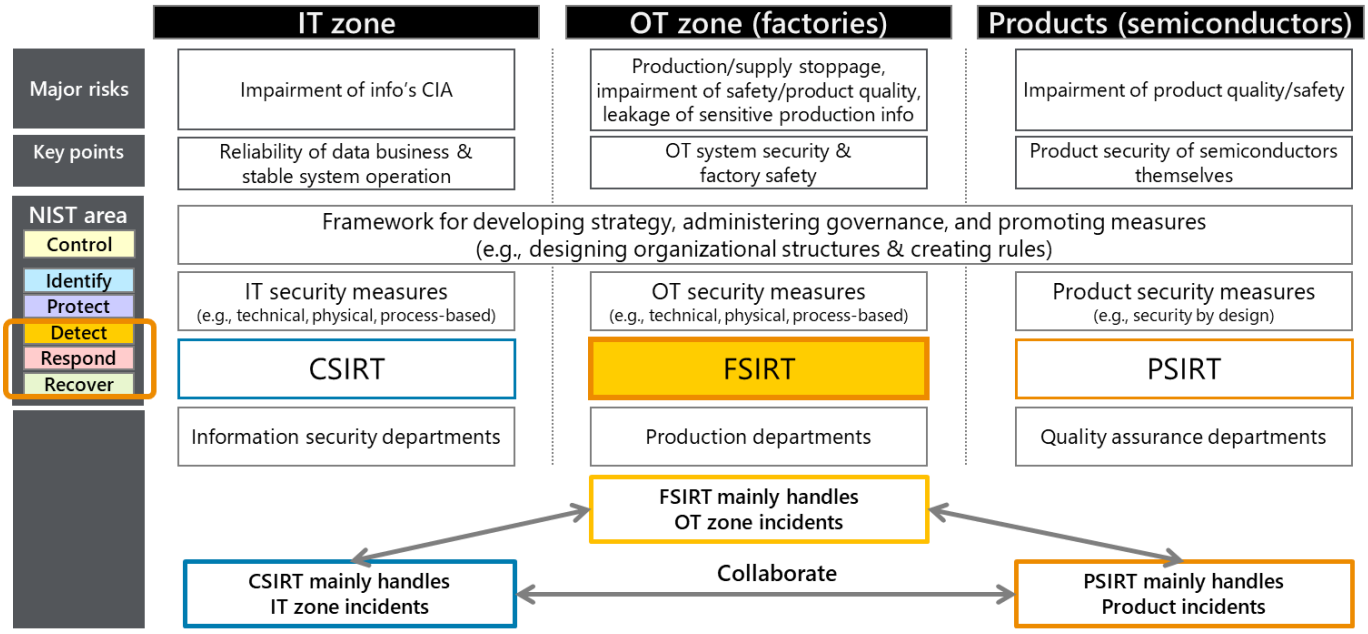


Figure 4-14. Roles of CSIRT, PSIRT, and FSIRT

FSIRT must establish a framework and prescribe operations for making incident responses when a cyberattack has been detected and must prepare for attacks during ordinary times. At an early stage, FSIRT shall implement measures to prevent an incident from spreading when one occurs at a factory. If damage is confirmed, it must escalate the matter as necessary and ensure early recovery so that normal production can be resumed (the incident response process to be taken in the event of an incident is described in "Figure 4-18. FSIRT's Incident Response Process").

During ordinary times, FSIRT is responsible for carrying out activities to prevent production stoppages, information leakages, etc. FSIRT ensures that safety measures are implemented for assets that are installed in the factory's OT zone and that operational rules for ensuring human and physical security are being followed correctly. During ordinary times, it shall also assess the factory's current level of security and analyze risks with the aim of developing an improvement plan.

	Incident response	Ordinary procedures
Example of actions	Quickly detect incidents that occur at the factory and work to prevent spread / achieve early recovery to regular production if damage is suffered	Ensure safety of the factory's important assets and observance of security rules to prevent production stoppage and information leaks
	Prevent spread of damage by detecting attacks at the initial stages. Work to contain damages and achieve early recovery if damages are suffered • Investigate cause/damage details (e.g., conduct interviews & check logs) • Contain damages (e.g., enable network restrictions & enhance authentication levels) • Eradicate the root of cause (apply patches) • Restore equipment/tools, systems, etc. (from backup data)	Ensure that security measures are not being compromised and ensure safety. Confirm security operations concerning human/physical security and make any necessary corrections • Policies & operational rules • Analyze & assess risks • Manage assets & monitor security (e.g., vulnerability management) • Improve awareness (e.g., education & training)

Figure 4-15. Details of FSIRT's Actions During Ordinary Times and When an Incident Occurs

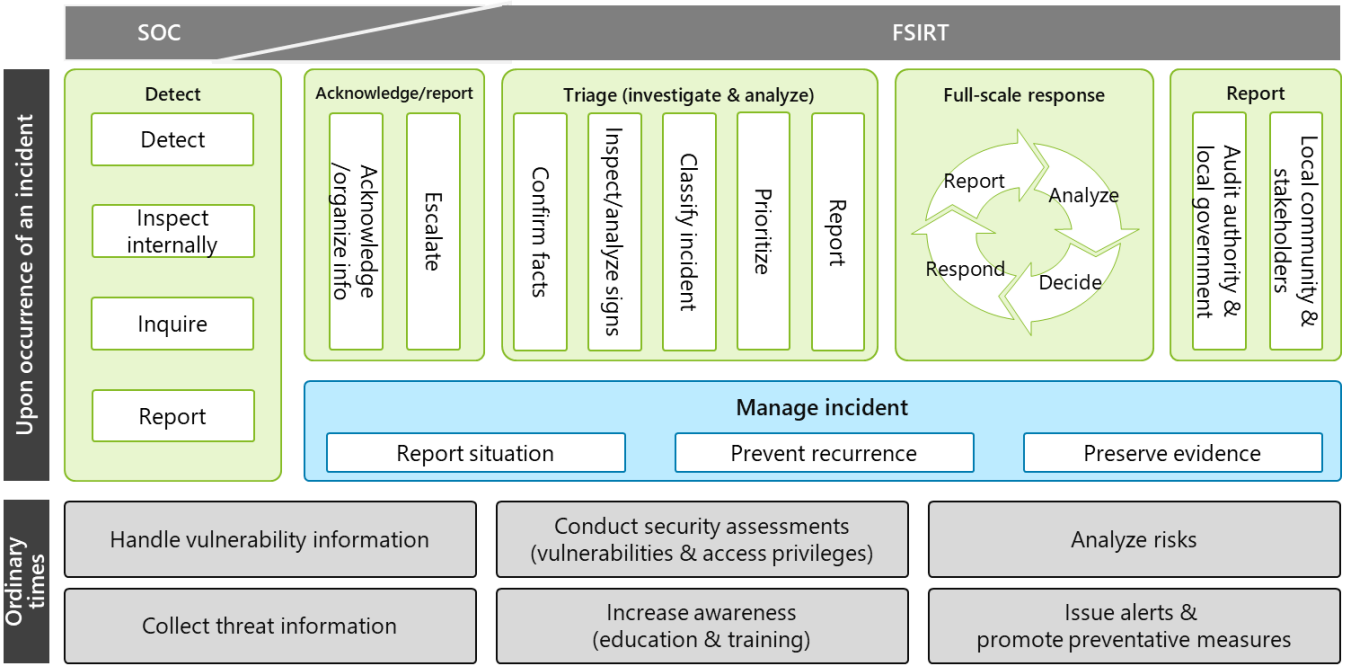


Figure 4-16. Details of FSIRT's Operations During Ordinary Times and When an Incident Occurs

Starting from its intrusion point, a cyberattack is carried out over several stages until its objective is achieved, followed by the exposure of damage. The example below shows the flow of an attack to a semiconductor device factory from network intrusion or physical intrusion to objective achievement using a cyber kill chain model.

An attacker improves the effectiveness of an attack by setting a clear objective. In the case of an attack made by a nation-state APT group, confidential production information is exploited for the purpose of ensuring the nation's competitive strength. In the case of an attack made by a cybercrime syndicate for financial purposes, production/supplies are suspended to cause a temporary plunge in stock prices for the purpose of acquiring trading profits. In this manner, preliminary investigations are conducted in order to carry out

effective attacks that are in line with their objectives, and multi-phased attacks are carried out targeting important assets in order to achieve those objectives.

In semiconductor device factories, since the impact on business in the event of damage is significant, defensive measures to detect signs of cyberattacks at an early stage and to prevent such attacks are implemented. In the case of intrusions via networks, there is a high risk that an attack will begin in the IT zone and then move into the OT zone. Therefore, it is effective to conduct cross-zone monitoring and analysis in both IT and OT zones and to respond to cyberattacks at their early stages.

At semiconductor device factories, due to the significant damage businesses would suffer if a cyberattack were to occur, defense measures are implemented to prevent attacks by detecting signs of cyberattacks at an earlier stage. Furthermore, many important assets related to confidential information and production stoppages are stored in the equipment/tools installed in the fab area (i.e., the clean room), and in addition to the company's employees who manage the equipment/tools, many maintenance personnel from various equipment manufacturers and facility manufacturers enter the fab area to perform maintenance work for those equipment/tools. Therefore, the maintenance work conducted for the equipment/tools installed in the fab area is highly likely to be exploited as a physical entry point for cyberattacks.

For this reason, rules for enforcing physical access controls—such as placing restrictions on individuals entering the fab area, bringing items into it, or establishing connections to it—are established and implemented. At the same time, detection at the initial stage is enhanced through security monitoring by implementing microsegmentation or defense in depth, which restricts intrusions and lateral movements via the network. FSIRT is required to determine the response to take when it becomes aware of a detection.

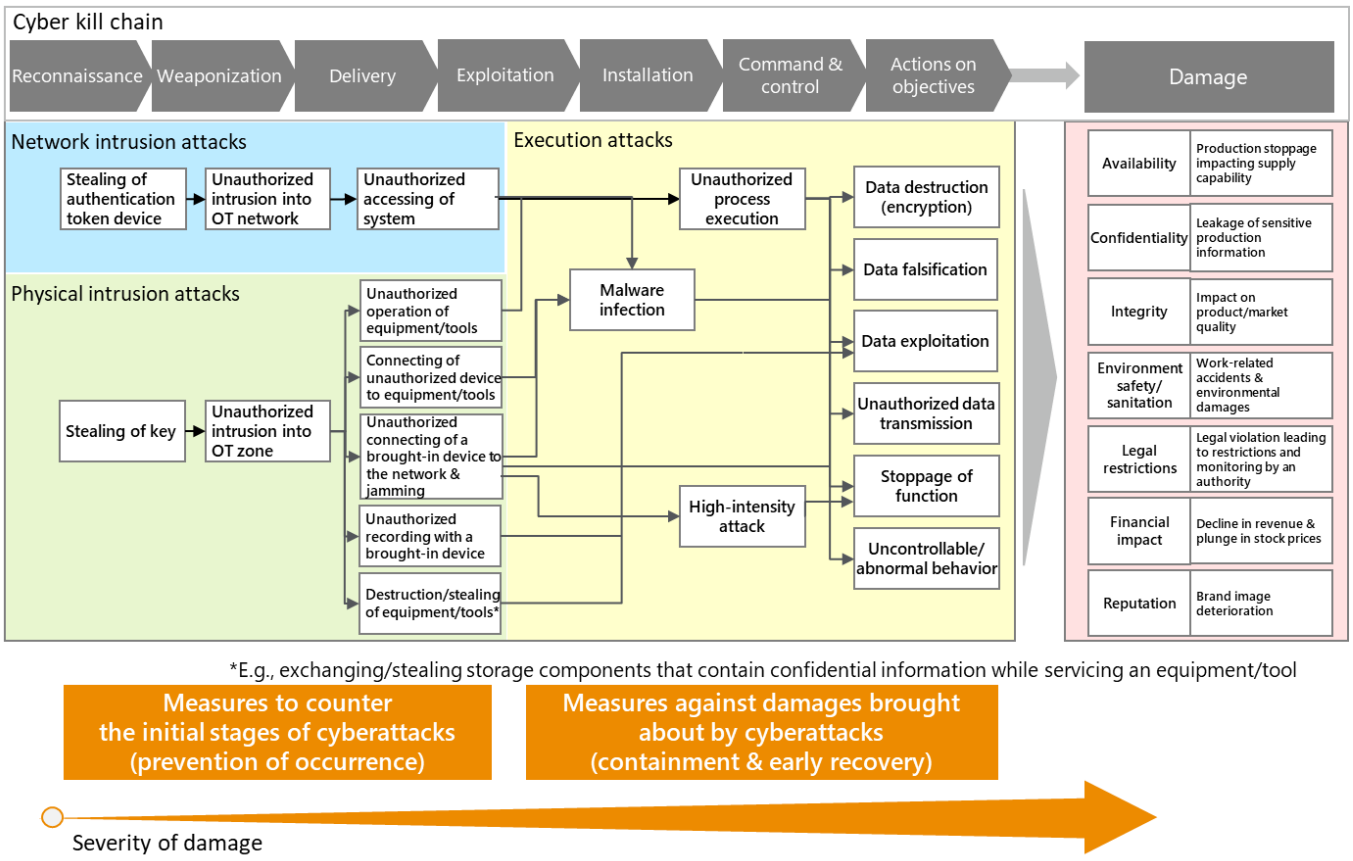


Figure 4-17. Cyber Kill Chain in Factories

Examples of FSIRT's incident response process and framework are shown below (see Figure 4-18 and Figure 4-19).

In semiconductor device factories, detection and registration, which are the first steps in the response process, occur extremely frequently, including false detection. This is because the number of cases detected is very large in proportion to the number of devices that detect and alert unauthorized accesses as a part of the network measures for preventing the occurrence/spread of cyberattacks by detecting their signs at an early stage, and proportional to the number of personnel who are monitored and restricted from entering restricted areas, bringing objects into, and connecting to restricted areas. Notices are issued for violations of these restrictions, further contributing to the high frequency of detections.

In order to efficiently register this large number of detections and implement emergency measures promptly, FSIRT shall prepare a procedure manual (e.g., a playbook) in advance, conduct training to enable personnel to respond appropriately, implement measures to prevent the occurrence of serious incidents, investigate and analyze the details and extent of the damage, and decide on a response policy according to the severity of the damage.

If the damage inflicted on the business is extremely severe, FSIRT shall decide to suspend production after consulting the matter with the factory manager and shall request the establishment of an emergency task force as a part of crisis management responses aimed at continuing business. If an

incident large enough to suspend production occurs, FSIRT must investigate the cause of the incident, contain it, eradicate it, and make an early recovery in cooperation with each relevant internal department so that production can be resumed, while regularly reporting to management concerning the current situation. Simultaneously, the FSIRT must report to external stakeholders, including customers and business partners that form part of the supply chain.

It is necessary to provide the tabletop exercises and education by specifically assuming that a large-scale cyber damage accompanying a production stoppage may be inflicted, just as evacuation drills and education are periodically conducted/provided by assuming that a natural disaster such as a large-scale earthquake may occur.

This series of incident response processes begins at the point when it is recognized that a "cyberattack" has occurred. However, in actual factories, it is also conceivable that when some equipment failure or malfunction occurs, the cause needs to be initially distinguished—whether it is merely a device failure or the result of a cyberattack. Therefore, it is desirable not only to conduct training specifically targeting cyberattacks but also to integrate cyberattack scenarios into general BCP training.

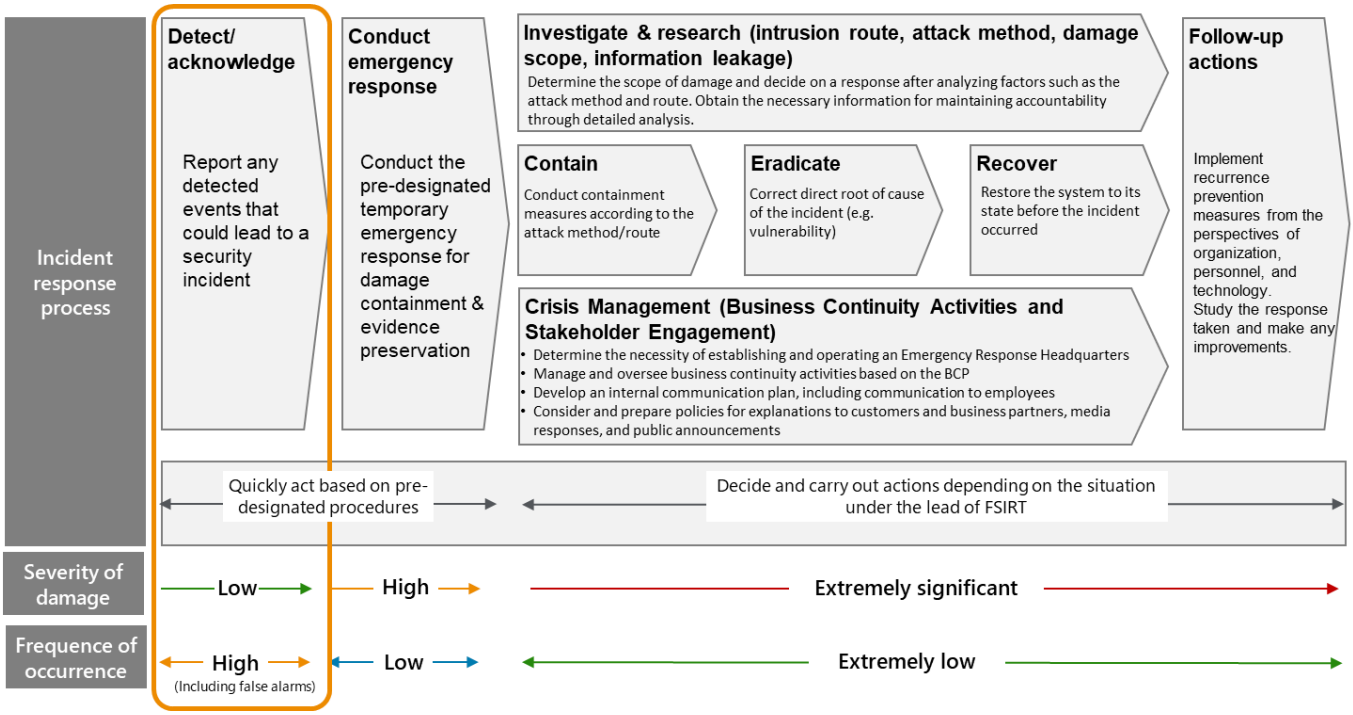


Figure 4-18. FSIRT's Incident Response Process

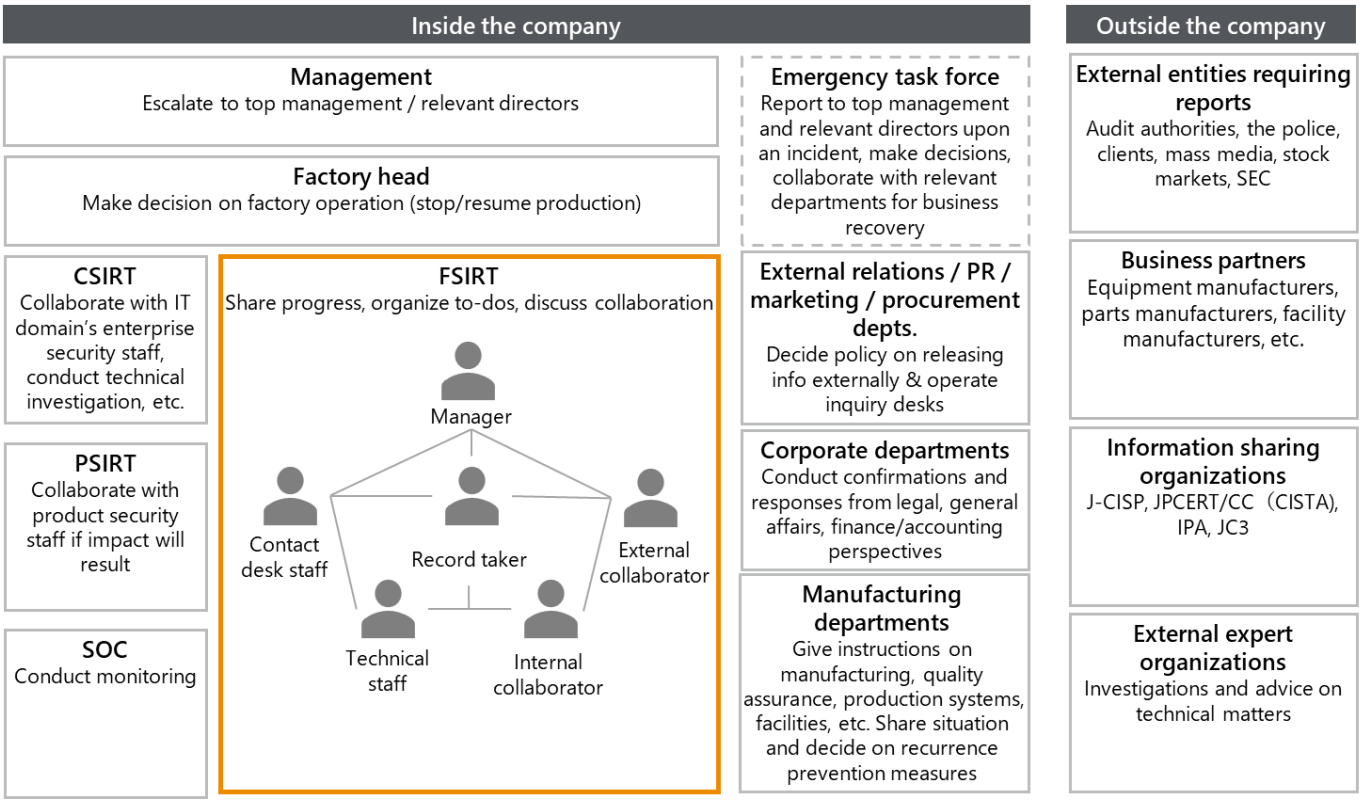


Figure 4-19. FSIRT's Organizational Structure and Internal/External Relationship Diagram

IPA's "Core Human Resources Development Program"[18] may be used to train personnel responsible for implementing security measures and conducting operations in the OT zone, such as FSIRT leaders and technical personnel.

This program enables trainees to learn in a comprehensive manner and deepen their knowledge about security and businesses with a bird's eye view of organizations, supply chains, and industries from a wide range of perspectives spanning from the field site to the management layer. Simultaneously, hands-on exercises using simulation systems are conducted for trainees to gain a deeper understanding of cybersecurity risks present at manufacturing sites, and training in collaboration with related overseas organizations is provided so that they can form top-level networks in Japan and overseas, and across industries.

As indicated in the reference architecture described in Chapter 2, semiconductor device factories produce semiconductors by employing a fully automated and continuously operating process that is combined an extremely large number of equipment/tools. Daily production activities are carried out by employees of the device factory and simultaneously, maintenance/support is provided by on-site field support engineers sent by the manufacturers of all equipment, which form the main components of production (i.e., this constitutes the first layer of the reference architecture for semiconductor device factories).

In order to protect semiconductor device factories from cyberattacks, which are increasing in number and maliciousness year by year, security measures

[18] https://www.ipa.go.jp/jinzai/ics/core_human_resource/2025.html

must steadily be implemented on a daily basis for equipment/tools, which are important assets that support semiconductor production.

For the large number of equipment/tools whose operation cannot be stopped, companies such as device manufacturers (i.e., FSIRT) and equipment manufacturers (i.e., PSIRT) must collaborate with each other to enhance security measures, such as by rapidly assessing and responding to threat and vulnerability information, managing signs of cyberattacks by monitoring equipment, activities, etc., and addressing incidents that are accompanied by cyber damage.

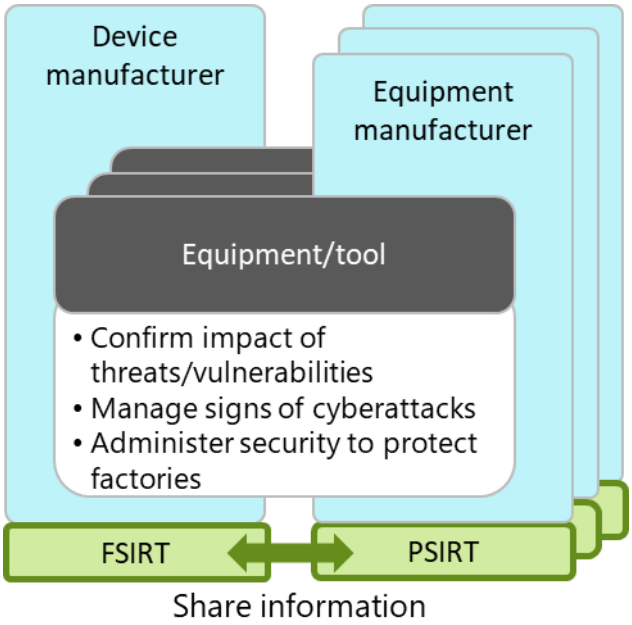


Figure 4-20. Inter-business Collaboration Between Device Manufacturers and Equipment Manufacturers

With regard to the details of the security collaboration conducted between device manufacturers and equipment manufacturers, it is important to add security requirements (e.g., the Capability Requirements of SEMI E187 and 188) to procurement specifications prepared during the process of procuring equipment/tools and to field support support/maintenance agreements concluded while running the equipment/tools, since collaboration between companies can only be conducted after the conclusion of an agreement.

Building a collaboration framework is also important. At present, equipment/tool/process management technicians from the device manufacturer and field support engineers from the equipment manufacturer serve as the primary points of collaboration between the companies. However, it is desirable for the security managers from both sides to work together and engage in regular communication to discuss security requirements, operational methods, and incident response measures.

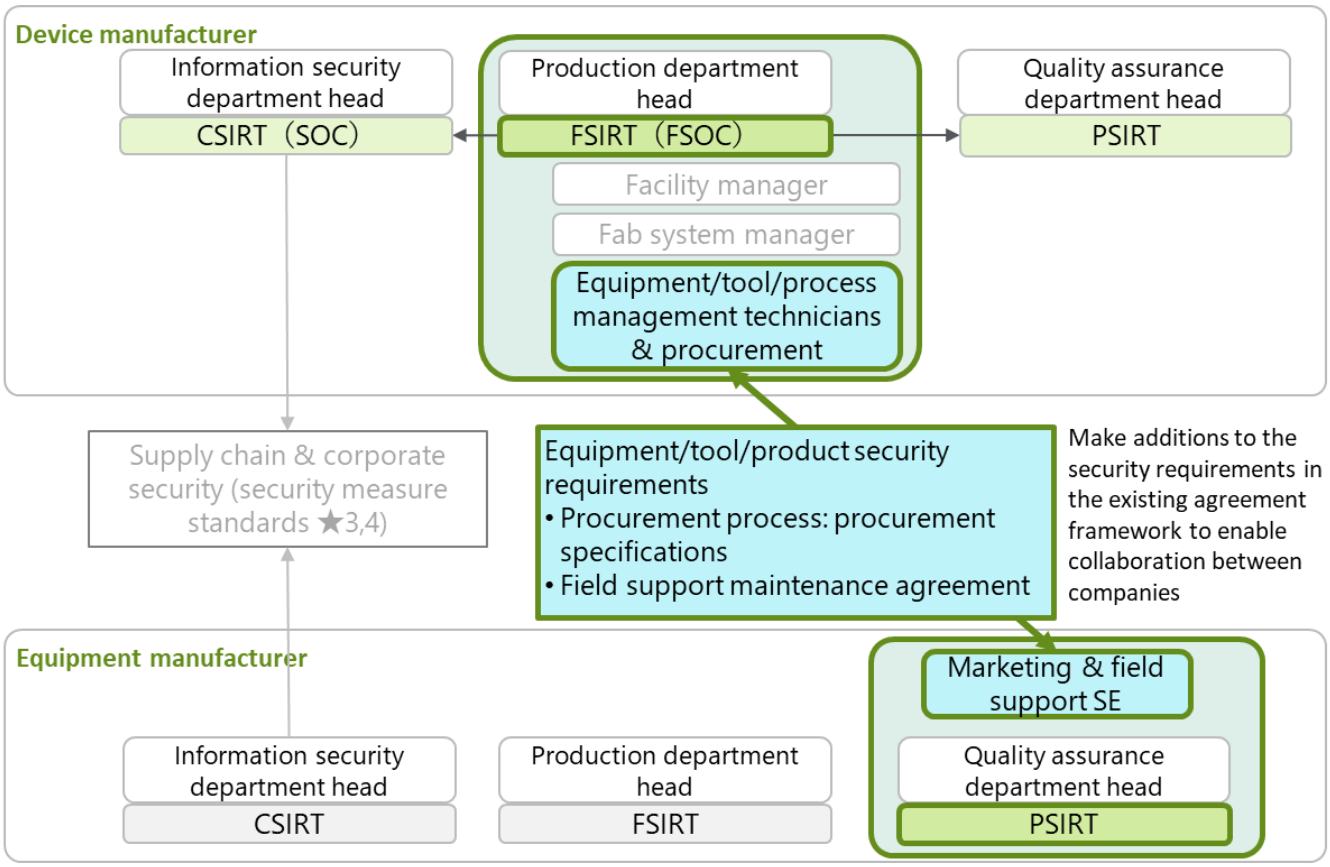


Figure 4-21. Detailed Illustration of the Security Collaboration Conducted Between Device Manufacturers and Equipment Manufacturers

To enhance the security measures of equipment and tools, the collaboration points between device manufacturers and equipment manufacturers are classified into two categories: during procurement (from procurement specifications to delivery) and during operation (routine and emergency responses under maintenance contracts). The seven specific security collaboration events at each collaboration point are shown in Table 4-5.

For each collaboration event, both the device manufacturer and the equipment manufacturer shall make operational arrangements by prescribing security requirements and the details of what will be provided.

Since the confidential production information of the device manufacturer, including its additional security measures, is provided and the confidential information of the equipment manufacturer, including the security configuration information of its product, is provided, a non-disclosure agreement (NDA) must be concluded in advance by having the security-related personnel of both companies participate in the process.

Reference information on how to handle relevant confidential information is included in Section 9.3.3 titled “Confidentiality Requirements of Equipment Design Information” and Section 9.3.4 titled “Requirement for Information Availability” of SEMI E169[19].

[19] https://store-us.semi.org/products/e16900-semi-e169-guide-for-equipment-information-system-security

Table 4-5. Security Cooperation Events that Occur Between Device Manufacturers and Equipment Manufacturers

Security cooperation events		Device manufacturers	Equipment manufacturers
Procurement (procurement specifications)	**Quoting/ordering (Confirm spec.)** 1. Quoting	Describe security requirements in the procurement specifications of the equipment/tool and request a quote (E.g., SEMI E187/188 Capability Requirements)	Prepare/submit quotation specifications that include the designated security requirements (SEMI E187/188 Capability Requirements: - Response: C – complies; NC – does not comply; WC: will comply; NA – not applicable)
	Decision/purchasing	Order → Build	
	Before delivery 2. Design	Confirm the security requirements of the purchased equipment/tool and design additional defense measures based on the installation environment (defense in depth/microsegmentation, settings for security monitoring, inquiry from the device manufacturer to the equipment manufacturer)	Confirm the additional defense measures needed for the installation environment make a response
	Delivery 3. Delivery	Confirm evidence of compliance with the equipment/tool's security requirements	Submit evidence of compliance with the equipment/tool's security requirements (asset configuration info, malware/vulnerability inspection, whether hardening was done, etc.)
	Installation 4. Connection	Confirm the results of the security settings of the equipment/tool, carry out additional measures for the network, register the equipment/tool on the asset management ledger, and start operation	Perform security settings that are required before connecting to the Fab network (Introduce security tools designated by the device manufacturer, perform necessary settings concerning networks/logs)
		Start testing for the implementation of the equipment/tool (conventional)	
Operation (field support)	**Ordinary procedures** Vulnerability assessment 5. Evaluation	Collect vulnerability/threat information for the equipment/tool Confirm the impact of the vulnerabilities Conduct and share the vulnerability assessment (Decide how to respond: respond immediately; respond at the timing of performing routine operations; tolerate vulnerability and maintain current measures)	Collect vulnerability/threat information for the equipment/tool Provide information on the impact of the vulnerabilities Share the results of the vulnerability assessment
	Vulnerability response 6. Modification	Decide how to respond to the equipment/tool's vulnerabilities Confirm the plan for responding to the vulnerabilities Announce information on the response plan (including suspension/adjustments) Confirm the results after the response is complete Conduct change management	Prepare a plan for responding to the vulnerabilities (including measures to decrease/mitigate risks) Conduct security measures for the equipment/tool
	Incident response 7. Abnormality	Conduct incident response (investigation & analysis) and share/report the situation	Conduct measures to minimize (contain) the impact on the equipment/tool Work to achieve early recovery

4.4 Physical Access Restrictions (People Entering/Bringing Objects in/Making Connections): Physical Measures in the Fab Area

The fab area, which is the manufacturing site of a semiconductor device factory, is isolated as a clean room, but is easily targeted by attackers as a physical entry point. The characteristics of the fab area are described once again and organized, and simultaneously, examples of physical security measures are shown below.

The fab area of a semiconductor device factory is deemed as a high-security area which manages many important assets that significantly impact business. It is difficult to identify individuals in the clean room as many personnel, including factory employees and maintenance personnel, enter and exit the area. Since individuals wear clean suits inside the clean room, making visual identification difficult, it is necessary to manage access using authentication devices and systems, such as ID cards and biometric authentication systems. Additionally, physical intrusion points must be identified, and corresponding physical security measures must be implemented with continuous security posture monitoring.

Examples of physical security measures have been developed with reference to IEC62443 and the Ministry of Economy, Trade, and Industry's “The Cyber/Physical Security Guidelines for Factory Systems 1.1,” specifically Section 3.2, Step 2: Planning Security Measures (2) Physical Measures.

Table 4-6. Physical Measures in the Fab Area

Points of Physical intrusion attack points	Characteristics of the fab area	Example of measures
• Unauthorized intrusion into the OT zone	• Many personnel who are unfamiliar with each other enter and exit the clean room, which is a fab area, it is difficult to identify individuals • Contract maintenance personnel assigned from various equipment manufacturers enter the room aside from factory employees who manage equipment/tools • Since production continues 24/7, factory employees (including shift workers) and contract maintenance personnel are subject to these measures • Contract maintenance personnel assigned from equipment manufacturers consist of both on-site workers and visitors • Since personnel working in the clean room wear full-body clean suits, it is difficult to identify individuals based on visual information (i.e., via visual inspection and video recordings)	• Management of people entering and visiting the factory • Placing limits on the permissions granted (to factory employees, on-site workers, and visitors) for entering the fab area • Constantly escorting visitors
• Unauthorized operations on equipment/tools	• Within the fab area, there is a large floor with a uniform layout where numerous equipment tools, classified as critical assets are intermingled, making access to consoles relatively easy	• Strengthen console login authentication for equipment tools • Ensure constant supervision of visitors
• Connection of unauthorized device to equipment/tools	• Devices are brought into the fab area during maintenance work to repair malfunctions or improve faulty equipment/tools • External storage media/devices are connected to equipment/tools for maintenance purposes, maintenance PCs are connected to equipment/tools, and maintenance/replacements are implemented by replacing software components in equipment/tools including the replacement storage parts	• Restrictions on bringing in computer devices • Restrictions on bringing in devices with storage capabilities • Physical and logical protection (i.e., port locks) of interface ports in equipment/tools
• Unauthorized network connections by brought-in devices	• The network communication protocols used within the fab area rely on plaintext/unauthenticated protocols as defined by industry standards	• Restrictions on bringing in devices with recording functions • Physical and logical protection of network cables, network device connection ports, and wireless access connections
• Jamming signals transmitted by brought-in devices	• Automatic transport equipment is controlled via wireless communication, and the radio frequency used is managed	• Restrictions on bringing in devices that transmit radio waves

• Unauthorized recordings made by brought-in devices	• Visual information of the fab area's layout (e.g., configurations of processes, as well as model information and the number of units of equipment/tools in the fab area) is also considered confidential production information	• Restrictions on bringing in devices with recording functions
• Destruction or theft of equipment tools	• The storage of equipment/tools contains production confidential information, such as recipe data	• Ensure the secure erasure and verification of production confidential information during the maintenance, replacement, or removal of equipment tools

For the points of attacks, see "Figure 4-22. Physical intrusions/attacks made into factories within the context of a cyber kill chain"

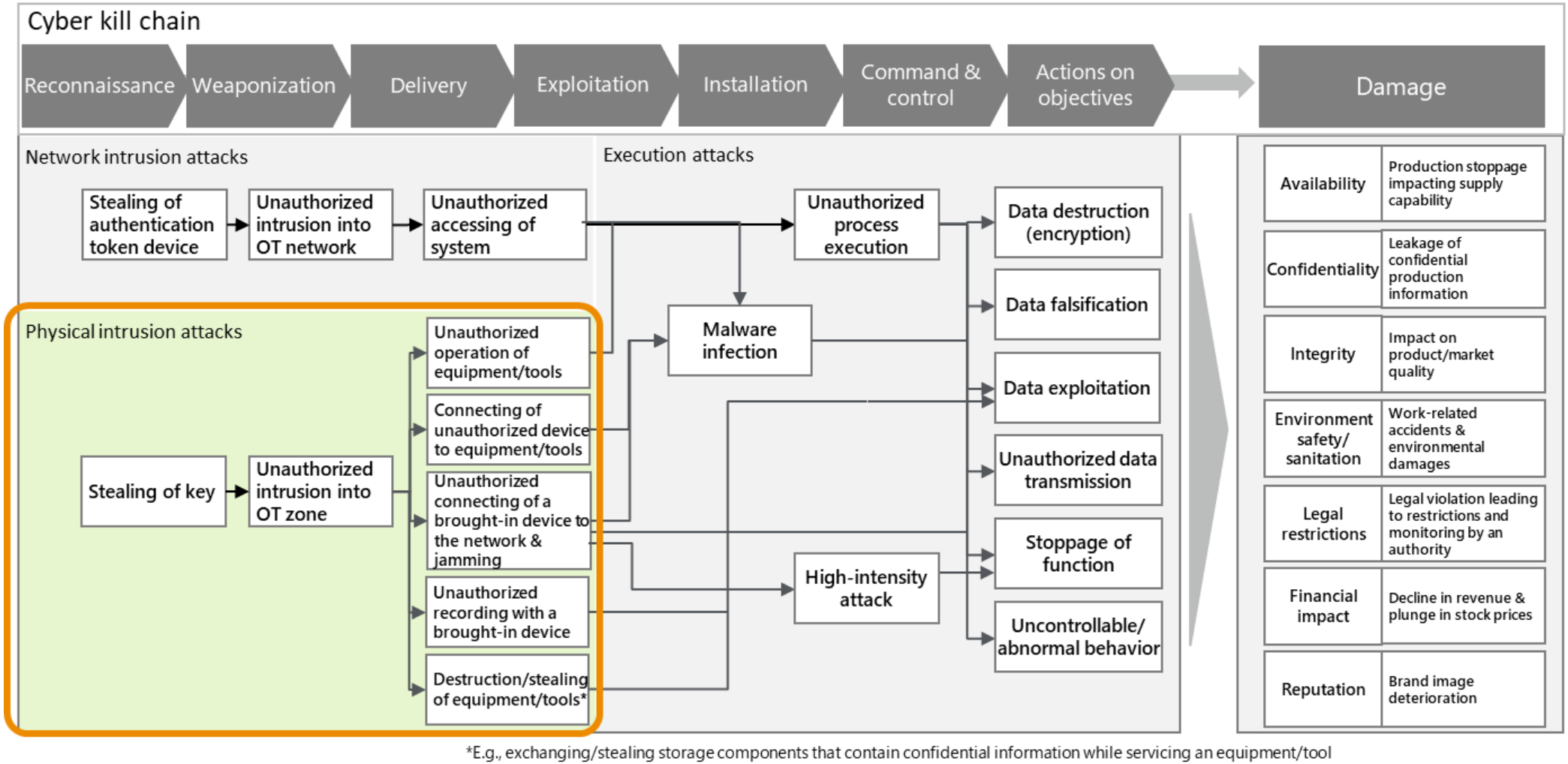


Figure 4-22. Physical intrusions/attacks Made into Factories within the Context of a Cyber Kill Chain

Appendix A: Comparison chart of NIST's CSF2.0 and CPSF

TableA-1. Mapping Table between CPSF and NIST CSF 2.0, with CPSF as the Base

CPSF		NIST's CSF2.0	
Measure ID	Measure requirement	Subcategory	
CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	ID.AM-01	Inventories of hardware managed by the organization are maintained
		ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained
CPS.AM-2	Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.		
CPS.AM-3	Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to store components for a certain period of time.		
CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.	ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained
		ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained
CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	ID.AM-04	Inventories of services provided by suppliers are maintained
CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business	ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission
CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.	GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
		GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
CPS.BE-1	Identify and share the role of the organizations in the supply chain.	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management
		GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated
CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management
CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
		GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated
CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
		GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
		GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission
		GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are

			understood and considered
		GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.		
CPS.GV-4	Develop a strategy and secure resources to implement risk management regarding security.	GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes
CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded
CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources
		ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established
CPS.RA-3	Identify and document the assumed security incidents, those impacts on the organization's assets, and the causes of those.	ID.RA-03	Internal and external threats to the organization are identified and recorded
CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
		ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated
CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization
CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated
CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders
		GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
		GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.	GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained
		GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated
CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
		GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by

			organizational stakeholders
		GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
		GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
		GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement
CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
		GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
		GV.SC-04	Suppliers are known and prioritized by criticality
		GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
		ID.RA-10	Critical suppliers are assessed prior to acquisition
CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.		
CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.		
CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
		ID.RA-10	Critical suppliers are assessed prior to acquisition
CPS.SC-7	Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.		
CPS.SC-8	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.		
CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activity to ensure action for incident response in the supply chain.	GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
		ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties
CPS.SC-10	Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)		
CPS.SC-11	Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.		
CPS.AC-1	Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization
		PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed,

			enforced, and reviewed, and incorporate the principles of least privilege and separation of duties。
CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk
CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	PR.AA-03	Users, services, and hardware are authenticated
		PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
		PR.IR-01	Networks and environments are protected from unauthorized logical access and usage
CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect login attempts and providing a time interval until safety is ensured		
CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions).	PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	PR.AA-03	Users, services, and hardware are authenticated
		PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	PR.IR-01	Identities and credentials for authorized users, services, and hardware are managed by the organization。
		PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk
CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures	PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions
CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	PR.AA-03	Users, services, and hardware are authenticated
CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
		PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
		PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind
CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
		ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved
		PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
		PR.AT-02	Individuals in specialized roles are provided with

			awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind
CPS.AT-3	Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.		
CPS.DS-1	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.		
CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected
CPS.DS-4	Encrypt information itself when sending/receiving information.	PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected
CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.		
CPS.DS-6	Secure sufficient resources (e.g., People, Components, System) for components and systems, and protect assets property to minimize bad effects of cyberattack (e.g., DoS attack).	PR.IR-04	Adequate resource capacity to ensure availability is maintained
CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	PR.IR-04	Adequate resource capacity to ensure availability is maintained
CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, select IoT devices and servers equipped with anti-tampering devices.	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
		PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected
		PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected
CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
		PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected
		PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected
CPS.DS-10	Conduct integrity checks of software running on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.	ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
CPS.DS-13	Confirm that IoT devices and software are genuine products during the booting-up process		
CPS.DS-14	Maintain, update, and manage information such as the origination of data, and data processing history, throughout the entire data life cycle.		
CPS.DS-15	Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.		
CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked
		PR.PS-01	Configuration management practices are established and applied
CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	PR.PS-01	Configuration management practices are established and applied
CPS.IP-3	Introduce the system development life cycle to manage the systems.	PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle
		ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles
CPS.IP-4	Perform a periodic system backups and testing of	PR.DS-11	Backups of data are created, protected,

	components (e.g., IoT devices, communication devices, and circuits).		maintained, and tested
		RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration
CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
		PR.IR-02	The organization's technology assets are protected from environmental threats
CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles
		PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk
CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities
CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities
CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	GV.RR-04	Cybersecurity is included in human resources practices
CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded
		PR.PS-02	Software is maintained, replaced, and removed commensurate with risk
CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands.	ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles
		PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk
CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles
		PR.PS-02	Software is maintained, replaced, and removed commensurate with risk
CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	PR.PS-04	Log records are generated and made available for continuous monitoring
CPS.PT-2	Minimize functions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
		PR.PS-01	Configuration management practices are established and applied
CPS.PT-3	Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.	PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations
CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained
CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	DE.AE-02	Potentially adverse events are analyzed to better understand associated activities
CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security incidents and comparative analysis with the threat information obtained from outside the organization.	DE.AE-03	Information is correlated from multiple sources
		DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis
		RS.MA-02	Incident reports are triaged and validated
CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.	DE.AE-04	The estimated impact and scope of adverse events are understood
CPS.AE-5	Specify the criteria to determine the risk degree of security events.	DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria
CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	DE.CM-01	Networks and network services are monitored to find potentially adverse events
CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT	DE.CM-02	The physical environment is monitored to find potentially adverse events

	devices and servers.		
CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	DE.CM-01	Networks and network services are monitored to find potentially adverse events
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	DE.CM-01	Networks and network services are monitored to find potentially adverse events
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
CPS.CM-5	Monitor communication with external service providers so that security events can be detected properly.	DE.CM-06	External service provider activities and services are monitored to find potentially adverse events
CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	DE.CM-01	Networks and network services are monitored to find potentially adverse events
		DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events
		DE.CM-06	External service provider activities and services are monitored to find potentially adverse events
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
		PR.PS-05	Installation and execution of unauthorized software are prevented
CPS.CM-7	Confirm the existence of vulnerabilities that require are regular check-up in IoT devices and servers managed within the organization.	ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded
CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.	GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
CPS.DP-2	Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.		
CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.	ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties
CPS.DP-4	Continuously improve the process of detecting security events.	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities
CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved
		DE.AE-06	Information on adverse events is provided to authorized staff and tools
		RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared
		RS.CO-02	Internal and external stakeholders are notified of incidents
		RS.CO-03	Information is shared with designated internal and external stakeholders
		RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging
CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved
		RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared
		RS.MA-04	Incidents are escalated or elevated as needed
		RS.CO-03	Information is shared with designated internal and external stakeholders
CPS.RP-3	Include security incidents in the business continuity plan or	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from

	emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.		the organization are understood and communicated
		RS.MA-05	The criteria for initiating incident recovery are applied
		RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process
		RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed
CPS.RP-4	Take appropriate measures on goods (products) whose quality may be affected by security incidents, especially regrading production facilities damaged by the security incident.		
CPS.CO-1	Develop and manage rules regarding publishing information after the occurrence of the security incident.	RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging
CPS.CO-2	Include the item in the business continuity plan or contingency plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.	RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging
CPS.CO-3	Include the item in the business continuity plan or contingency plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.	RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	RS.MA-02	Incident reports are triaged and validated
		RS.MA-03	Incidents are categorized and prioritized
		RS.MA-04	Incidents are escalated or elevated as needed
		RS.AN-08	An incident's magnitude is estimated and validated
CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.	RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident
		RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security related impact, penetration vector, and other factors.	RS.MA-03	Incidents are categorized and prioritized
CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.	RS.MI-01	Incidents are contained
		RS.MI-02	Incidents are eradicated
CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved
CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved

Table A-2. Mapping Table between CPSF and NIST CSF 2.0, with NIST CSF 2.0 as the Base

NIST CSF2.0		CPSF	
Subcategory	Measure requirements	Measure ID	
GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	CPS.BE-1	Identify and share the role of the organizations in the supply chain.
		CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).
GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
		CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	CPS.GV-2-	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.
GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
		CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
		CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.
		CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
		CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
		CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
		CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.
GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	CPS.BE-1	Identify and share the role of the organizations in the supply chain.
		CPS.BE-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders	CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish

			and implement the process to confirm the implementation status of security risk management of relevant parties.
GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.
GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	CPS.GV-4	Develop a strategy and secure resources to implement risk management regarding security.
GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.
GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.
GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.
GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions		
GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving		
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
		CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.
		CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.
GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.
GV.RR-04	Cybersecurity is included in human resources practices	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction		
GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks		
GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed		
GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the

			responsibilities.
GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.
		CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.
GV.SC-04	Suppliers are known and prioritized by criticality	CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.
GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties。	CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.
GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.
GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.
		CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.
GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activity to ensure action for incident response in the supply chain.
GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.
GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.
ID.AM-01	Inventories of hardware managed by the organization are maintained	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.
		CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.
ID.AM-04	Inventories of services provided by suppliers are maintained	CPS.AM-5	Specify the criteria to determine the risk degree of security events.
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.

ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	CPS.IP-3	Introduce the system development life cycle to manage the systems.
		CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.
		CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands.
		CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.
		CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.
		CPS.CM-7	Confirm the existence of vulnerabilities that require are regular check-up in IoT devices and servers managed within the organization.
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.
ID.RA-03	Internal and external threats to the organization are identified and recorded	CPS.RA-3	Identify and document the assumed security incidents, those impacts on the organization's assets, and the causes of those.
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices
		CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.),

			analyzes the information, and establishes a process to implement and use measures.
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.
ID.RA-10	Critical suppliers are assessed prior to acquisition	CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.
		CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.
ID.IM-01	Improvements are identified from evaluations		
ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
		CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activity to ensure action for incident response in the supply chain.
		CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.
ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.
		CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.
		CPS.DP-4	Continuously improve the process of detecting security events.
		CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.
		CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
		CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
		CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
		CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.
		CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	CPS.AC-1	Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures
PR.AA-03	Users, services, and hardware are authenticated	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).
		CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor

			authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.
		CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).
PR.AA-04	Identity assertions are protected, conveyed, and verified		
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	CPS.AC-1	Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
		CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).
		CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions).
		CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.
		CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
		CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
		CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.
		CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, select IoT devices and servers equipped with anti-tampering devices.
		CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.
		CPS.DS-10	Conduct integrity checks of software running on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.
		CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.
		CPS.PT-2	Minimize functions of IoT devices and servers by physically and logically blocking unnecessary network

			ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.
		CPS.DS-4	Encrypt information itself when sending/receiving information.
		CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, select IoT devices and servers equipped with anti-tampering devices.
		CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, select IoT devices and servers equipped with anti-tampering devices.
		CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.
PR.DS-11	Backups of data are created, protected, maintained, and tested	CPS.IP-4	Perform a periodic system backups and testing of components (e.g., IoT devices, communication devices, and circuits).
PR.PS-01	Configuration management practices are established and applied	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
		CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.
		CPS.PT-2	Minimize functions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.
		CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.
		CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands.
PR.PS-04	Log records are generated and made available for continuous monitoring	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.
PR.PS-05	Installation and execution of unauthorized software are prevented	CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	CPS.IP-3	Introduce the system development life cycle to manage the systems.
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).
		CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT

			devices vs. other environments within the organization).
PR.IR-02	The organization's technology assets are protected from environmental threats	CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	CPS.PT-3	Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.
PR.IR-04	Adequate resource capacity to ensure availability is maintained	CPS.DS-6	Secure sufficient resources (e.g., People, Components, System) for components and systems, and protect assets property to minimize bad effects of cyberattack (e.g., DoS attack).
		CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.
DE.CM-01	Networks and network services are monitored to find potentially adverse events	CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.
		CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.
		CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.
		CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.
DE.CM-02	The physical environment is monitored to find potentially adverse events	CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	CPS.CM-5	Monitor communication with external service providers so that security events can be detected properly.
		CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.
		CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.
		CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people,

			components, and systems.
		CPS.DS-10	Conduct integrity checks of software running on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.
		CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.
DE.AE-03	Information is correlated from multiple sources	CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security incidents and comparative analysis with the threat information obtained from outside the organization.
DE.AE-04	The estimated impact and scope of adverse events are understood	CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.
DE.AE-06	Information on adverse events is provided to authorized staff and tools	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security incidents and comparative analysis with the threat information obtained from outside the organization.
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	CPS.AE-5	Specify the criteria to determine the risk degree of security events.
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
		CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
RS.MA-02	Incident reports are triaged and validated	CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security incidents and comparative analysis with the threat information obtained from outside the organization.
		CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.
RS.MA-03	Incidents are categorized and prioritized	CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.
		CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security related impact, penetration vector, and other factors.
RS.MA-04	Incidents are escalated or elevated as needed	CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.
		CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
RS.MA-05	The criteria for initiating incident recovery are applied	CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and	CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.

	provenance are preserved		
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved		
RS.AN-08	An incident's magnitude is estimated and validated	CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.
RS.CO-02	Internal and external stakeholders are notified of incidents	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
RS.CO-03	Information is shared with designated internal and external stakeholders	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
		CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
RS.MI-01	Incidents are contained	CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.
RS.MI-02	Incidents are eradicated	CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.
RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	CPS.IP-4	Perform a periodic system backups and testing of components (e.g., IoT devices, communication devices, and circuits).
RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms		
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed		
RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed		
RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	CPS.CO-3	Include the item in the business continuity plan or contingency plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.
RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
		CPS.CO-1	Develop and manage rules regarding publishing information after the occurrence of the security incident.
		CPS.CO-2	Include the item in the business continuity plan or contingency plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.

Appendix B:Glossary/Abbreviations

AMHS ≪Automated Material Handling Systems≫

APT ≪Advanced Persistent Threat≫

CAD ≪Computer-Aided Design≫

CASB ≪Cloud Access Security Broker≫

CCD ≪Charge Coupled Devices≫

CSPM ≪Cloud Security Posture Management≫

CSIRT ≪Computer Security Incident Response Team≫

CVE ≪Common Vulnerabilities and Exposures≫

CVSS ≪Common Vulnerability Scoring System≫

CWPP ≪Cloud Workload Protection Platform≫

DCS ≪Distributed Control System≫

DMZ ≪DeMilitarized Zone≫

EAP ≪Extensible Authentication Protocol≫

EDA ≪Electronic Design Automation≫

EDR ≪Endpoint Detection and Response≫

EOSL ≪End of Service Life≫

EPP ≪Endpoint Protection Platform≫

FOUP ≪Front Opening Unified Pod≫

FSIRT ≪Factory Security Incident Response Team≫

GEM ≪Generic Equipment Model≫

HSMS ≪High Speed Message Service≫

IAM ≪Identity and Access Management≫

I/O≪Input/Output≫

IDS ≪Intrusion Detection System≫

IPS ≪Intrusion Prevention System≫

JVN ≪Japan Vulnerability Note≫

MCS ≪Material Control System≫

MES ≪Manufacturing Execution System≫

MSRC ≪Microsoft Security Response Center≫

NDR ≪Network Detection and Response≫

NVD ≪National Vulnerability Database≫

OEM≪Original Equipment Manufacturing≫

OHT ≪Overhead Hoist Transport≫

PLC ≪Programmable Logic Controller≫

PSIRT ≪Product Security Incident Response Team≫

SBOM ≪Software Bill of Materials≫

SECS ≪SEMI Equipment Communications Standard≫

SPC ≪Statistical Process Control≫

SSPM ≪SaaS Security Posture Management≫

SSVC ≪Stakeholder-Specific Vulnerability Categorization≫

VPN ≪Virtual Private Network≫

WORM ≪Write Once Read Many≫

Access control
The process of granting or denying specific requests for obtaining and using information and related information processing services; and to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). [NIST SP 800-53 Rev.4]

Active scanning
A security assessment technique that sends packets or probes to actively search for vulnerabilities in networks and systems. This includes port scanning, vulnerability scanning, and penetration testing, and assesses security risks by identifying system misconfigurations and known vulnerabilities.

Anomaly Detection
A mechanism providing a multifaceted approach to detecting cybersecurity attacks. [NISTIR 8219]

Authenticator
The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational

operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [NIST SP 800-53 Rev.4]

Cloud

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [NIST SP 800-53 Rev.4]

Configuration management

A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. [NIST SP 800-53 Rev.5]

Conduit

A communication channel used to transfer information between different zones within an Industrial Automation and Control System (IACS) environment. It allows secure communication between zones with different security levels.

Component

A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware. [NIST SP 800-53 Rev.5]

Console

A visually oriented input and output device used to interact with a computational resource.[NIST SP 1800-27B]

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.[NIST SP 800-53 Rev. 5]

Defense in depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [NIST SP 800-53 Rev.4]

Endpoints

Any device, such as computers, mobile devices, IoT devices, and other terminals, that connects to an organization's network and accesses the information system or transmits and receives data.

Enterprise

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. [NIST SP 800-53 Rev.4]

Firewall

A gateway that limits access between networks in accordance with local security policy. [NIST SP 800-53 Rev.4]

Firmware

Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. [NIST SP 800-53 Rev.4]

Front PC(Factory Facing Components)）

A PC attached to equipment tools for operating and controlling the equipment tools. It has the capability to connect to the fab network and provides functions such as console operation and storage media connection.

Gateway

An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks. [NIST SP 800-53 Rev.4]

General-Purpose OS

An operating system that is not specialized for a specific purpose or hardware and can be used on a wide variety of computer systems and applications.

Hardware

The physical components of an information system. [NIST SP 800-53 Rev.4]

Hardening

A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[NIST SP 800-12 Rev. 1]

Industrial Control System (ICS)

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. [NIST SP 800-53 Rev.4]

Log

A record of the events occurring within an organization’s systems and networks. [NIST SP 800-92]

Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. [NIST SP 800-53 Rev.5]

Multifactor authentication (MFA)

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). [NIST SP 800-53 Rev.4]

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. [NIST SP 800-53 Rev.4]

Network management

The overall process of operating, monitoring, maintaining, and optimizing a network infrastructure.

Protocol

A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [NIST SP 800-53 Rev.4]

Port

The entry or exit point from a computer for connecting communications or peripheral devices. [NIST SP 800-82r3]

Reference Architecture

A template or framework that outlines best practices and standard components for building, operating, and managing systems or solutions within a specific domain or industry.

Resilience

The ability of an information system to continue to: (i) operate under adverse conditions

or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. [NIST SP 800-39]

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[NIST SP 800-30 Rev.1]

Risk analysis

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.[NIST SP 800-30 Rev.1]

Risk assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. [NIST SP 800-30 Rev.1]

Risk management

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [NIST SP 800-30 Rev.1]

Security logs

Records of events that occurred on a system. They contain information about security-related events, such as login attempts, file access, and system changes.

Segregation of duties

A security measure to restrict access to a system and apply the principle of least privilege to prevent a single user or process from having excessive privileges.

Server

A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).[NIST SP 800-175B Rev.1]

Supply chain

Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle. [NIST SP 800-53 Rev.5]

System

Discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST SP 800-30 Rev.1]

Software

Computer programs and associated data that may be dynamically written or modified during execution. [NIST SP 800-53 Rev.4]

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST SP 800-53 Rev.4]

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [NIST SP 800-53 Rev.5]

Zone

A collection of IACS system elements grouped into a logical group with a common security level. Restricting information flow between zones with different security levels

mitigates security risks.

Council of these Guidelines

Study Group for Industrial Cybersecurity WG1

(Strengthening Effectiveness and International Collaboration)

Semiconductor Industry SWG members

※Honorific titles omitted, in alphabetical order, as of October 24, 2025

	Hiroaki Akiyama	Director Micron Memory Japan, Inc.
|Chair|	Hiroshi Esaki	Professor Graduate School of Information Science and Technology The University of Tokyo
	Kensuke Higashi	Division Manager Legal, IP, and Compliance Division Advantest Corporation
	Kiyofumi Takahashi	Department Manager Information Security Department Group Governance & Administration NIKON CORPRATION
	Kiyoshi Watabe	Chief Executive Director Semiconductor Equipment Association of Japan
	Masahiko Hamajima	President SEMI Japan
	Masahiro Takahara	System Software Department, Production Operations, Cleanroom Division DAIFUKU CO.,LTD.
	Masanori Hamada	Chairperson of Semiconductor Steering Committee, Semiconductor Board, Japan Electronics and Information Technology Industries Association(*Sep.2025~)
	(Shoichi Nakagawa	Chairperson of Semiconductor Steering Committee, Semiconductor Board, Japan Electronics and Information Technology Industries Association(*~Sep.2025))
	Oriyuki Iijima	Product Security Strategy Dept.

	Tokyo Electron Limited
Shigeki Nagano	President
	SCREEN System Service Co., Ltd
Tetsuya Nikami	CIO
	Rapidus Corporation(*Sep.2025~)
(Toshio Fujii	Deputy Head of IT & Digital Division,
	Head of IT & Security Department, Senior Director
	Rapidus Corporation(*~Sep.2025))
Toyooki Mitsui	Vice Chairperson of Semiconductor Steering Committee/
	Chief of Policy Recommendation Task Force,
	Semiconductor Board,
	Japan Electronics and Information Technology Industries Association

Study Group for Industrial Cybersecurity WG1

(Strengthening Effectiveness and International Collaboration)

Semiconductor Industry SWG task force members

※Honorific titles omitted, in alphabetical order, as of October 24, 2025

Akira Tanaka	Information Security Dept. Tokyo Electron Limited
Eiichi Kadota	Chief Semiconductor & Device Group, Strategic Planning & Administration Dept. Information System Sect. Mitsubishi Electric Corporation
Eiji Hagio	Information Security Dept. Tokyo Electron Limited
Hanae Tobita	Senior Manager Information Security Division, Information Systems Renesas Electronics Corporation
Hidekatsu Matsuda	Product Security Strategy Dept. Tokyo Electron Limited
Hidemasa Ikeda	Manager Semiconductor & Device Group, Power Device Works, Manufacturing Control Dept. Mitsubishi Electric Corporation
Hiroichi Nakanishi	Planning & Control Division, Information System Department Sony Semiconductor Manufacturing Corporation
Hiroshi Nakamura	Senior Manager IT ＆ Security Department, IT ＆ Digital Division Rapidus Corporation.
Hitoshi Kobayashi	Information Security Committee Nuvoton Technology Corporation Japan
Junpei Horie	Information Security Unit, IT Department, Corporate Strategy Division SCREEN Holdings Co., Ltd.
Kiyofumi Takahashi	Department Manager Information Security Department Group Governance & Administration

	NIKON CORPRATION
Kiyoshi Watabe	Chief Executive Director
	Semiconductor Equipment Association of Japan
Koichi Imabayashi	Strategic Planning Div.
	Toshiba Electronic Devices & Storage Corporation
Masahiko Hamajima	President
	SEMI Japan
Masahiro Suzuki	4th Development Department Development Sector Semiconductor
	Lithography Business Unit Precision Equipment Group
	Nikon Corporation
Motoyasu Hayashi	Product Security Project, Engineering Management Department
	SCREEN Semiconductor Solutions Co., Ltd.
Oriyuki Iijima	Product Security Strategy Dept.
	Tokyo Electron Limited
Osamu Ono	System Development Section, Production Innovation
	Department, Manufacturing Development Center, Manufacturing
	Headquarters
	Sanken Electric Co. Ltd,
Osamu Tsubakida	Cyber Security Business Dept.
	VeriServe Corporation
Ryotaro Hayashi	Security Governance Planning Group, Cyber Security Center
	KIOXIA Corporation
Ryouji Fukuyama	Planning & Control Division, Information Security Department
	Sony Semiconductor Manufacturing Corporation
Satoshi Aoki	Product Security Project, Engineering Management Department
	SCREEN Semiconductor Solutions Co., Ltd.
Shigeki Nagano	President
	SCREEN System Service Co., Ltd
Shinsuke Sasaki	Cyber Security Center
	KIOXIA Corporation
Shoichi Nakagawa	Chairperson of Semiconductor Steering Committee,
	Semiconductor Board,
	Japan Electronics and Information Technology Industries Association
Shuji Yoshida	Planning & Control Division, Information Security Department
	Sony Semiconductor Manufacturing Corporation

Tadahioro Hayashi	Director Information Security Division, Information Systems Renesas Electronics Corporation
Taizo Matsuo	IT & Business Transformation Div. Toshiba Electronic Devices & Storage Corporation
Takahisa Mori	Planning & Control Division, Information Security Department Sony Semiconductor Solutions Corporation
Takanori Makioka	Business Promotion Headquarters, DX Promotion Management Division, IT Promotion Department, Business Applications Section Sanken Electric Co. Ltd,
Takayuki Nishimura	Engineering Management Department SCREEN Semiconductor Solutions Co., Ltd.
Tomoyuki Kobayashi	Information Security Unit, IT Department, Corporate Strategy Division SCREEN Holdings Co., Ltd.
Toyooki Mitsui	Vice Chairperson of Semiconductor Steering Committee/ Chief of Policy Recommendation Task Force, Semiconductor Board, Japan Electronics and Information Technology Industries Association
Yuichi Manabe	Planning & Control Division, Information Security Department Sony Semiconductor Manufacturing Corporation
Yumi Kaneko	Planning & Control Division, Information Security Department Sony Semiconductor Solutions Corporation
Yuuichi Kawakami	IT & Business Transformation Div. Toshiba Electronic Devices & Storage Corporation

DAIFUKU CO.,LTD.

Micron Memory Japan, Inc.

ROHM CO., Ltd.