METI
Ministry of Economy, Trade and Industry

Summary of "(Draft)OT Security Guidelines for Semiconductor Device Factories"

Cybersecurity Division / Information Industry Division,
Commerce and Information Policy Bureau

OT Security Guidelines for Semiconductor Device Factories
~Overview~

Background and purpose of these guidelines

- In light of the economic and national security importance of the semiconductor industry and the growing cyber threats and risks at present, it is necessary to promote security measures, including responses to advanced cyberattacks.
- Internationally, the global semiconductor industry association SEMI has formulated E187/E188 as a standard for semiconductor manufacturing equipment, and the U.S. National Institute of Standards and Technology (NIST) is also formulating a semiconductor manufacturing profile for Cybersecurity Framework 2.0 (hereinafter referred to as NIST CSF 2.0).
→provides guidelines for factory security measures to maintain production goals, protect confidential information, and maintain the quality of semiconductors, while aligning with various security standards in the international semiconductor industry.

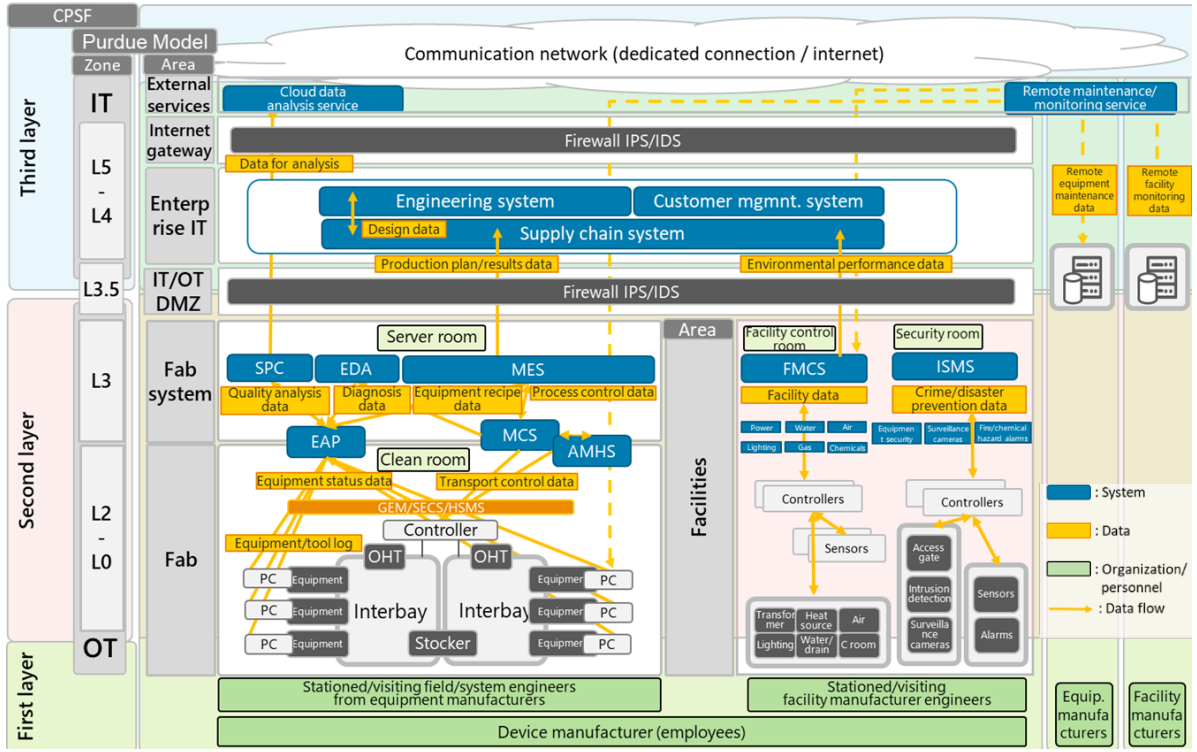
How to use these guidelines

- This guidelines are mainly aimed at **the manufacturing departments (at the working level) of semiconductor device manufacturers.** These guidelines provide fundamental principles and specific guidance for the integrative protection of cyberspace and physical space through **The Cyber/Physical Security Framework (hereinafter referred to as CPSF), as well as risk- based frameworks such as NIST Cybersecurity Framework 2.0 (NIST CSF 2.0).It can be utilized as a reference when conducting risk analysis and considering security measures.**

- **Creation of an organization profile**
With reference to the contents described in the features and considerations presented in Chapter 3 of this guideline, conduct an assessment of the current status and establish objectives for each subcategory
- **Formulate an action plan**
To develop an action plan based on the gap analysis of the current state and objectives outlined in the organizational profile, consult the CPSF measure requirement IDs and E187 manufacturing references detailed in Chapter 3 of this guideline, along with the measure examples specified in Chapter 4

Measures indicated in these guidelines

- Based on the reference architecture for semiconductor device factories, a risk mitigation framework (CPSF and NIST CSF 2.0) was utilized **to identify sources of risk (threats and vulnerabilities) specific to the characteristics of semiconductor device factories, and to compile the corresponding security control items**.
- **Measures were organized for fab areas, fab system areas, external services, IT/OT DMZ, and organizational and people aspects** classified by the Purdue model



Reference Architecture of Semiconductor Device Factory

Structure of the Guidelines 1. Background and Purpose of the Guidelines (1)

- In “Background and purpose of these guidelines“ outline the expected readers, the assets to be protected, the assumes attack actors, the utilization of these guidelines, and the structure of these guidelines.

Background and purpose of these guidelines

- 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. On the international stage, **global semiconductor industry association SEMI has developed the E187 and E188 Standards for semiconductor manufacturing equipment. Furthermore, 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).**

- 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.**

Expected readers

- Manufacturing divisions (practitioner level) of semiconductor device manufacturers (manufacturing divisions of equipment manufacturers and material manufacturers)

Assumed attack actors

- 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 (Nation-state cyber actors (APT)** (i.e., SL4 in IEC 62443).

What to protect

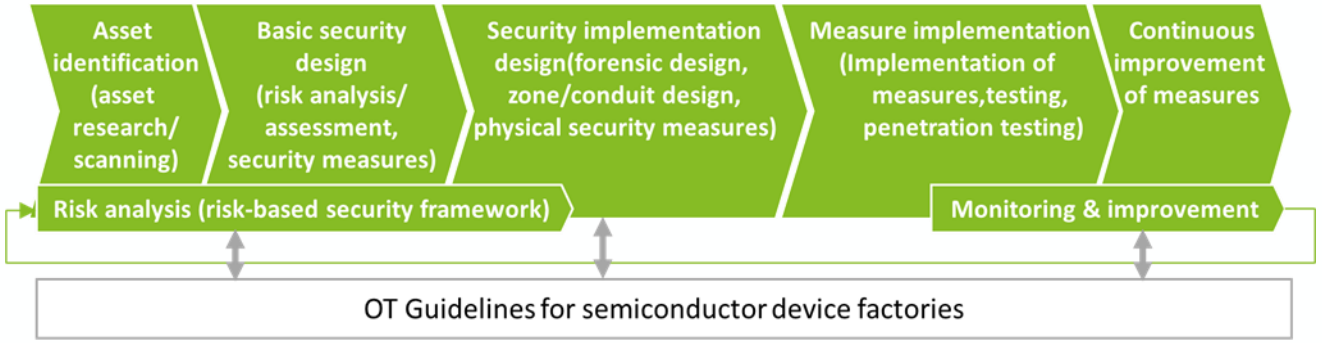
- The NIST CSF 2.0 Semiconductor Manufacturing Profile identifies the following five key areas as priorities to be safeguarded: Maintain Production Goals (supply responsibilities), Protect Confidential Information, Maintain the Quality of Semiconductors, Maintain Environmental Safety, and Maintain Human Safety.

- In particular, these guidelines focus on **"Maintain Production Goals (supply responsibilities)," "Protect Confidential Information," and "Maintain the Quality of Semiconductors."**

Structure of the Guidelines 1. Background and Purpose of the Guidelines (2)

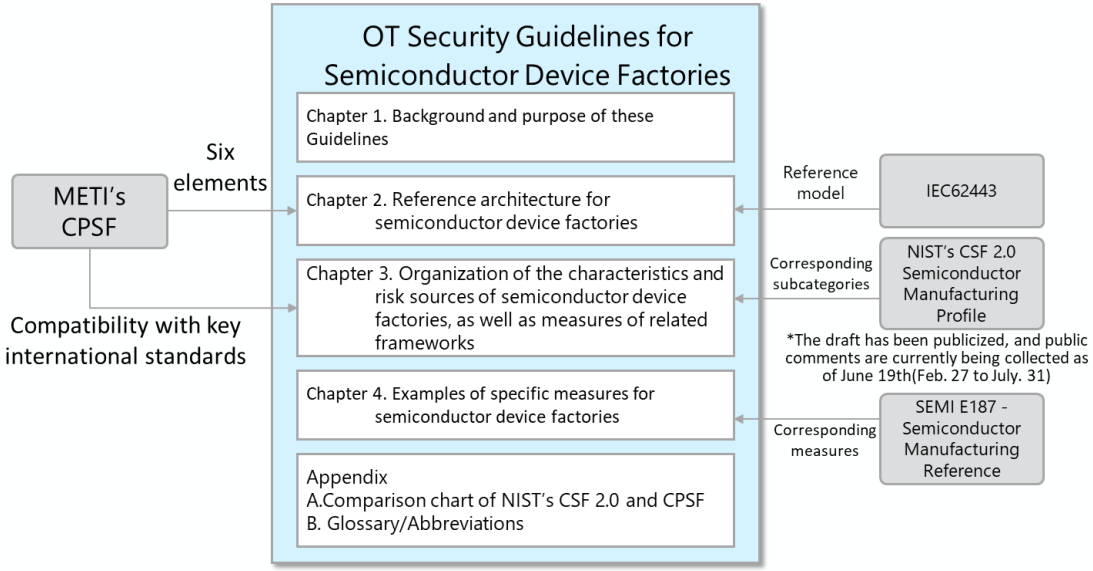
Utilization of these guidelines

- 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 (hereinafter referred to as CPSF [*1]), as well as risk-based frameworks such as NIST Cybersecurity Framework 2.0 [*2] (NIST CSF 2.0).** In addition, 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[*3].



Structure of the guidelines

- Chapter 2: Utilizing IEC 62443's 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 3: 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 4: More detailed examples of measures/methods are introduced for initiatives that are particularly important for semiconductor device factories, such as microsegmentation.



*1：https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
framework that establishes fundamental principles and specific guidelines for the integrated protection of cyber and physical spaces
*2：https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
*3：https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

Structure of the Guidelines 2. Reference Architectures for Semiconductor Device Factories (1)

- In "2. Reference Architecture for Semiconductor Device Factories", a reference architecture for semiconductor device factories is described that is organized with the aim of making it easier to consider security measures for "Maintain production Goals (supply responsibilities)"protection of confidential information", and "maintenance of semiconductor quality" to be protected from cyber attacks

Characteristics of the reference architecture of the semiconductor device factory

- **Applying the Purdue Model, an architecture for Industrial Control Systems (ICS), to generic semiconductor device factories**
  The factory's key areas are divided into "IT zone," "OT zone," and "IT/OT DMZ," and each area is associated with levels (L) 0 to 4/5.
- **To identify risks specific to semiconductor device factories and organize corresponding security measures, CPSF is applied**

  The semiconductor device factory is divided into CPSF's three-layer structure, and the six components of CPSF (Organization, People, Systems, Procedures, Physical Objects, and Data) are extracted

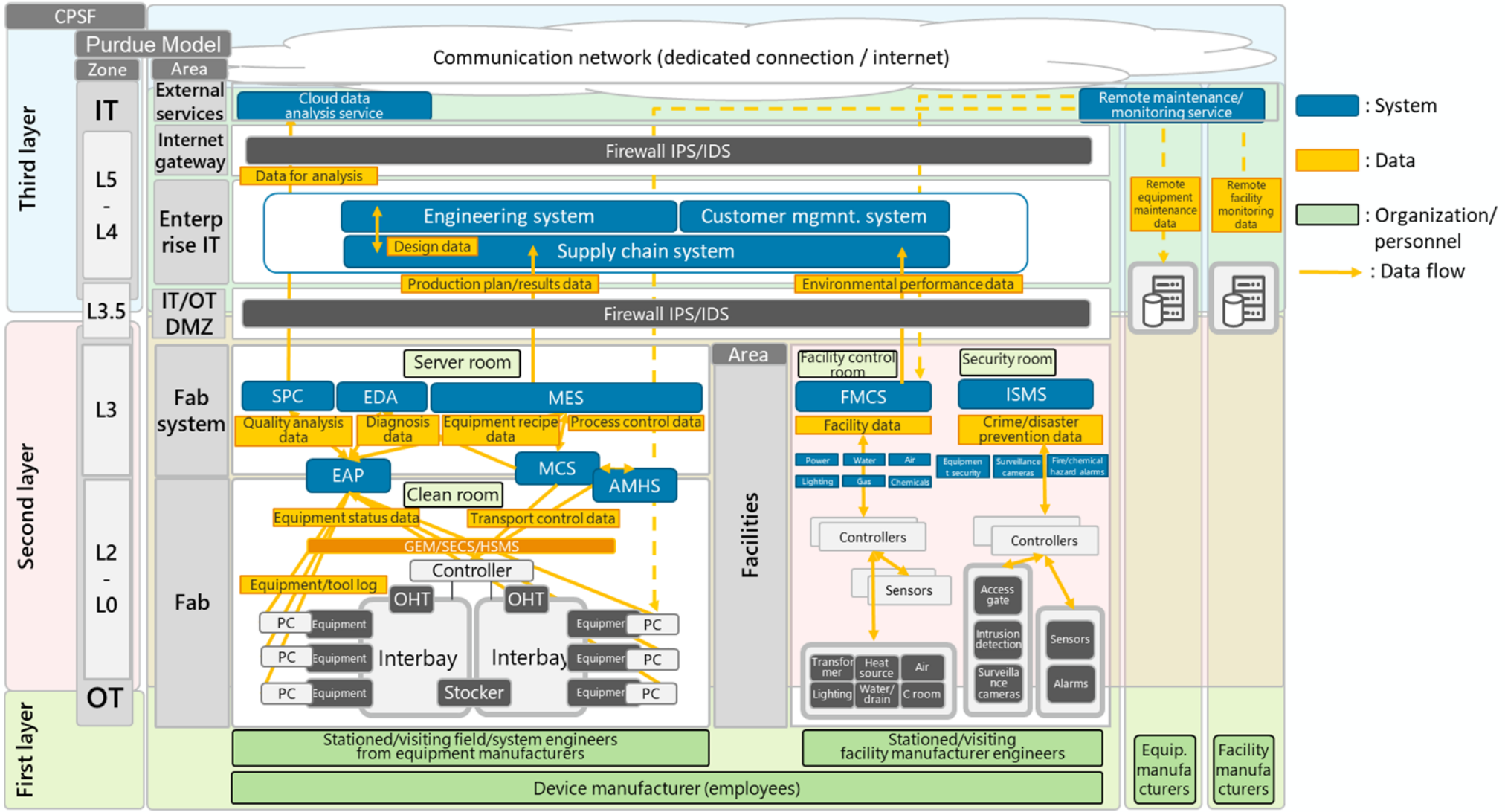
The purdue model

- IT zone (Levels 4-5)
  - Internet gateway (Level 5)
  - Enterprise IT area（Levels 4-5)
- OT zone（Levels 0-3)
  - Fab system area（Level 3)
  - Fab area（Levels 0-2)
  - Facility area（Levels 0-3)
- IT/OT DMZ（Level 3.5)

CPSF Three-Layer Structure

- First layer
  Indicates connections between companies (organizations/people), primarily focusing on semiconductor device factories.
- Second layer
  Indicates connections between physical space and cyberspace within a semiconductor device factory
- Third layer
  Indicates connections that take place within cyberspace when a semiconductor device factory uses external services

Structure of the Guidelines 2. Reference Architectures for Semiconductor Device Factories (2)



Reference Architecture of Semiconductor Device Factory

Structure of the Guidelines 2. Reference Architectures for Semiconductor Device Factories (3)

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				

The Purdue Model and the CPSF's Six Elements

Structure of the Guidelines

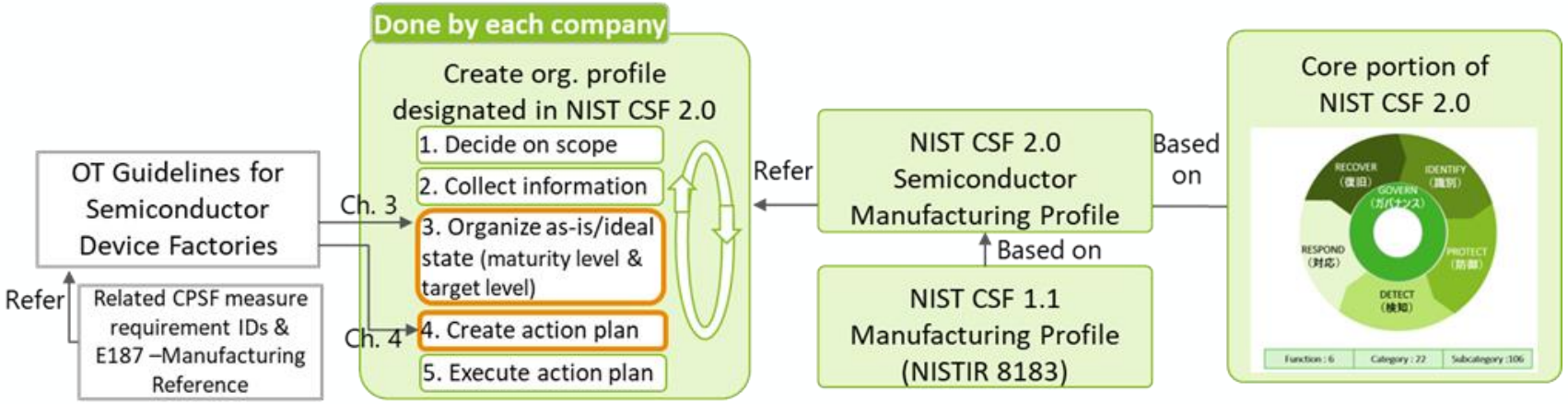
3. Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories(1)

Conducting Risk Analysis for an Organization Utilizing NIST CSF 2.0 and the NIST CSF 2.0 Semiconductor Manufacturing Profile

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.

- **Creation of an organization profile referring**
  Based on the content described in Chapter 3 of these guidelines, characteristics and viewpoints that must be considered, understand the current status and set goals for each subcategory.
- **Formulate an action plan**
  Formulating an action plan based on a gap analysis of the current state of the organization's profile and the targets, refer to the CPSF Requirement IDs and the E187 Manufacturing Reference in Chapter 3 of the Guidelines, as well as the examples of measures described in Chapter 4.



Structure of the Guidelines

3. Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories(2)

Organizing Security Measures Using Reference Architectures

These guidelines are designed to be utilized in general processes for advancing factory security measures, particularly for conducting risk-based analysis using cybersecurity frameworks such as CPSF and the NIST CSF 2.0 Semiconductor Manufacturing Profile, as well as for considering specific countermeasures. The following **outlines the process for analyzing the current state of an organizational profile and setting goals by leveraging this guideline (Chapters 3 and 4), the NIST CSF 2.0 Semiconductor Manufacturing Profile, CPSF, and other related frameworks.**

How to Utilize "Information for Risk Analysis" (Pages 12 and 13 of this document)

Creation of current state and goals

Understanding characteristics and confirming relevant sections

In Chapter 3, after reviewing the "characteristics" of each zone and area, confirm the contents of the subcategories and measure requirement IDs described in the “Relevant parts in NIST CSF 2.0 Semiconductor Manufacturing Profile and CPSF

Setting goals for the organizational profile

When conducting a current state analysis or setting goals for the organizational profile using resources such as the NIST CSF 2.0 Semiconductor Manufacturing Profile and CPSF, refer to the “Characteristics and viewpoints that must be considered when implementing security measures"

Development of an action plan

Utilization of specific measure examples

Refer to Chapter 4, “Examples of Specific Measures for Semiconductor Device Factories," as well as the E187 Manufacturing Reference and proceed with the consideration of measures

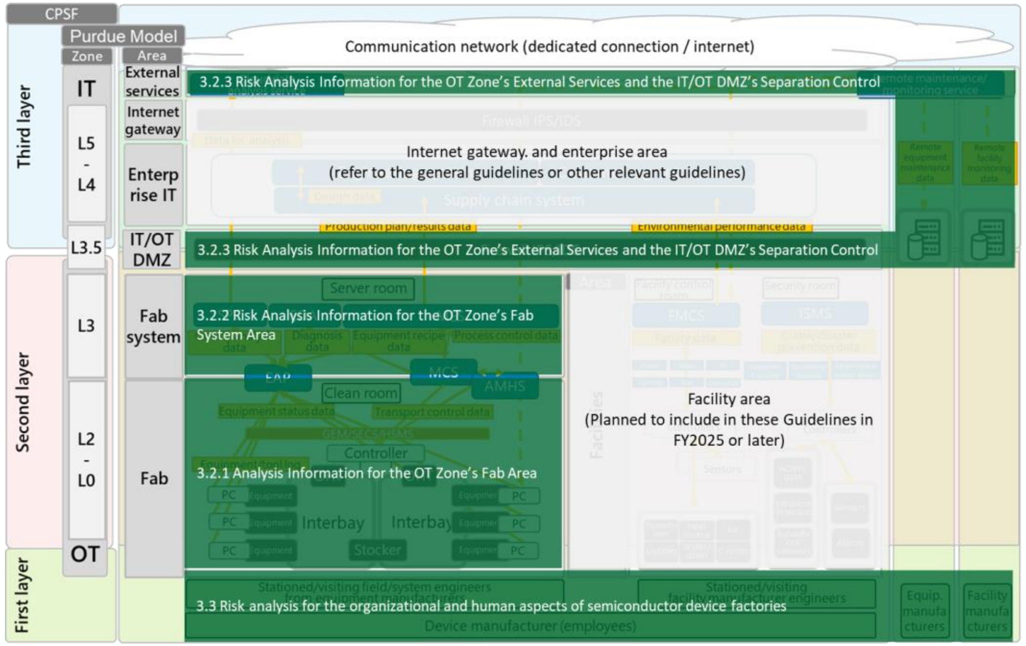
Structure of the Guidelines

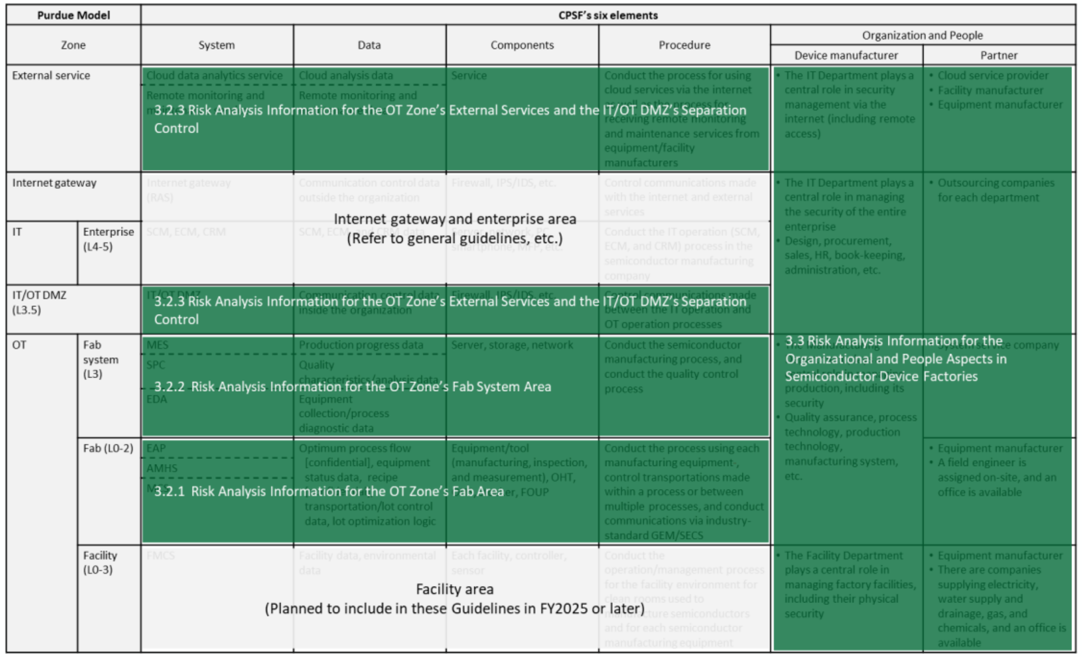
3. Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories(3)

Organizing Security Countermeasure Items Utilizing a Reference Architecture

By utilizing the reference architecture, risks (threats and vulnerabilities) are identified based on the characteristics of semiconductor device factories, and the corresponding security countermeasure items from the risk management frameworks (CPSF and NIST CSF 2.0) are consolidated.

The scope of organizing 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.





Structure of the Guidelines

3. Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories(4)

Information for Risk Analysis

Based on the Purdue model organized reference architecture, **the characteristics and viewpoints to be considered from technical and physical aspects are searched for and identified, and threats and vulnerabilities are summarized from a risk source perspective 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.**

Technical and physical aspects

3.2 Risk Analysis Information for Each Area of the OT Zone from the Technical and Physical Aspects of Semiconductor Device Factories
3.2.1 Risk Analysis Information for the OT Zone's Fab Area
① Asset management and vulnerability assessment of equipment/tools
② Additional defense measures to minimize equipment/tool damages and to prepare for early recovery
③ Procurement and introduction of safe equipment/tools
④ Identification and data management of confidential production information
⑤ Physical access restrictions (people entering/bringing in devices/making connections)
⑥ Logical access restrictions (ID management, authentication, and access control)
3.2.2 Risk Analysis Information for the OT Zone's Fab System Area
①System availability
②Data preservation
③Physical measures for server rooms
3.2.3 Risk Analysis Information for the OT Zone's External Services and the IT/OT DMZ's Separation Control
① Utilization of external services (cloud services)
② Utilization of external services (use of remote diagnosis services)
③ IT/OT DMZ

Organizational and people aspects

3.3 Risk Analysis Information for the Organizational and People Aspects in 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

Structure of the Guidelines

3. Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories(5)

Information for Risk Analysis（e.g., : Asset management and vulnerability assessment of equipment/tools①）

<table>
<tr><th colspan="2">Zone/area</th><th>Characteristics and viewpoints that must be considered when implementing security measures</th></tr>
<tr><td>OT</td><td>Fab area</td><td>
①Asset 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="4">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 this number is expected to increase in the future due to digital twinning occurring at sites</td><td>6</td><td>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</td></tr>
<tr><td>2</td><td>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</td><td>7</td><td>Software cannot be added to some equipment/tools due to their design (i.e., EPP/EDR)</td></tr>
<tr><td>3</td><td>A single equipment/tool is connected to multiple networks for different purposes</td><td>8</td><td>Patch applications cannot be implemented on some equipment/tools due to their design</td></tr>
<tr><td>4</td><td>A generic OS is used for the pre-process PC installed inside the equipment (i.e., Windows/Linux)</td><td>9</td><td>Some equipment/tools use legacy OS, preventing the implementation of patch applications</td></tr>
<tr><td>5</td><td>Industry standard protocols (i.e., unencrypted/unauthenticated protocols) are used (i.e., GEM/SECS/HSMS) to communicate between equipment systems and between equipment</td><td>10</td><td>Patch application time is limited (i.e., line downtime is limited)</td></tr>
</table>
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 mplemented 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
</td></tr>
</table>

Structure of the Guidelines

3. Organization of the Characteristics and Risk Sources, and Measures in Related Frameworks for Semiconductor Device Factories(6)

Information for Risk Analysis（e.g., : Asset management and vulnerability assessment of equipment/tools②）

CPSF's risk sources (threats / vulnerabilities /vulnerability IDs)	Relevant parts in NIST's CSF 2.0 Semiconductor Manufacturing Profile /CPSF
Threats : Malware infection exploiting security vulnerabilities **Vulnerabilities** : • The security status of components and how they are connected to the network are not properly managed • Knowledge on devices that are connected to the information systems and industrial control systems of one's own organization is lacking • Vulnerability information and threat information have not been collected and analyzed, and appropriate measures have not been implemented • The status of security measures (e.g., software configuration information and patch application status) for the organization's IoT devices that are connected to information systems and industrial control systems has not been ascertained • Vulnerabilities that need to be addressed in the organization's systems are left unaddressed • Vulnerabilities that should be addressed in the system are not being addressed properly **Targeted elements** Components: equipment/tools **【CPSF's vulnerabilityIDs】** • 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	**【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 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 outlines how to reduce security threats to assets connected to the fab network, such as real-time detection of unauthorized movements and patch application

Structure of the Guidelines 4. Examples of Specific Measures for Semiconductor Device Factories

Examples of Specific Measures for Semiconductor Device Factories

The following four specific countermeasure examples are provided as references for advancing countermeasure considerations in semiconductor device factories

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))

Structure of the Guidelines 4-1. Asset Management and Vulnerability Assessment of Equipment/Tools(1)

- 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

Asset management	How to search for and identify all assets (equipment/tools) and manage their configurations	Classifying assets by giving weights based on their degree of importance, as automated, continuous, process-based production results in a large number of assets and complexity in configuration
	How to determine the degree of importance of assets (equipment/tools)	
Vulnerability assessment	Methods for identifying the vulnerabilities of equipment/tools	Conducting assessment based on an understanding of the vulnerability of a vast number of assets. These sections indicate methods for conducting assessments effectively and deciding on the priority for addressing each vulnerability, given the increasing number of vulnerabilities detected each year.
	Methods for collecting information on threats to equipment/tools	
	Vulnerability assessment of equipment/tools and methods for determining response priority levels	

Structure of the Guidelines 4-1. Asset Management and Vulnerability Assessment of Equipment/Tools(2)

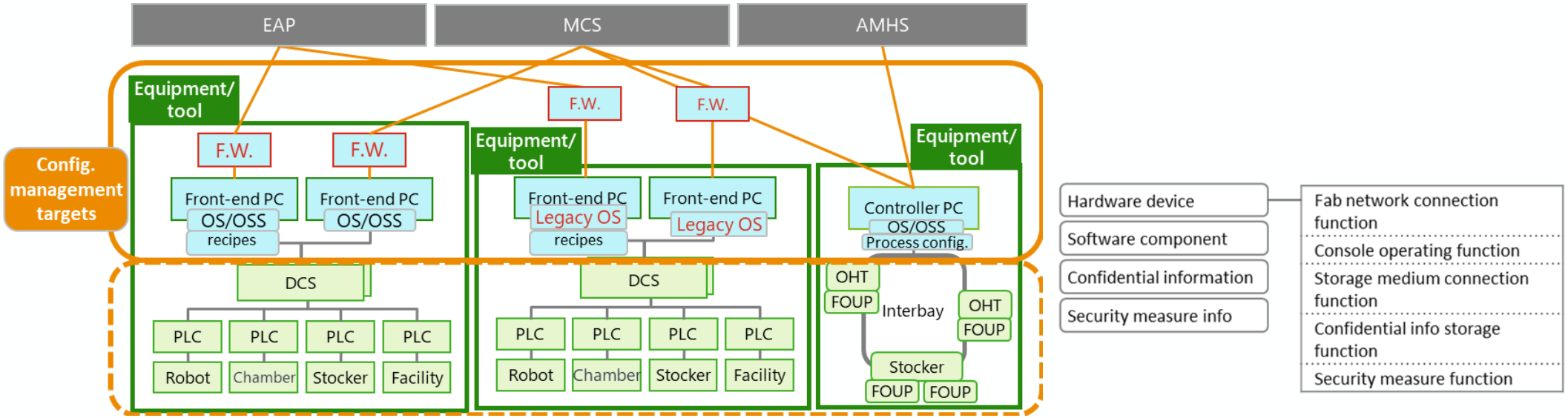
Determining the Identification and Configuration Management of Assets (Equipment/Tools)

- 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, access control network management, and security monitoring.



Structure of the Guidelines 4-1. Asset Management and Vulnerability Assessment of Equipment/Tools(3)

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

- 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.**

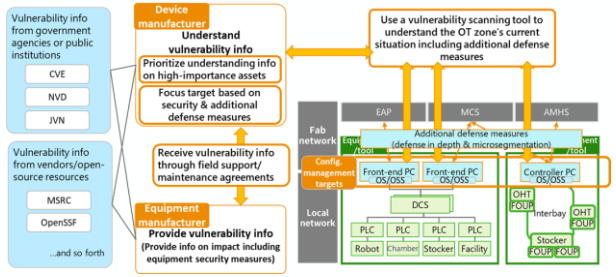
Risk area	Expected business damage and impact on business continuity in the event an asset receives a cyberattack							Value as a system asset	
	Business continuity (availability)		Semiconductor quality (integrity)		Safety of industrial activities (HES)		Compliance with laws, regulations, etc.	Information leakage (confidentiality)	Financial impact
Degree of importance	Production stoppage	Impact on supplies	Impact on yield	Impact on market qualityy	Work-related accident	Environmental damage		Leakage of confidential production information	Damage to an equipment/ tool
High	1day or more	7days 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	2days 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	

Structure of the Guidelines 4-1. Asset Management and Vulnerability Assessment of Equipment/Tools(4)

Methods for Identifying the Vulnerabilities of Equipment/Tools

Sources of vulnerability information

- 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)



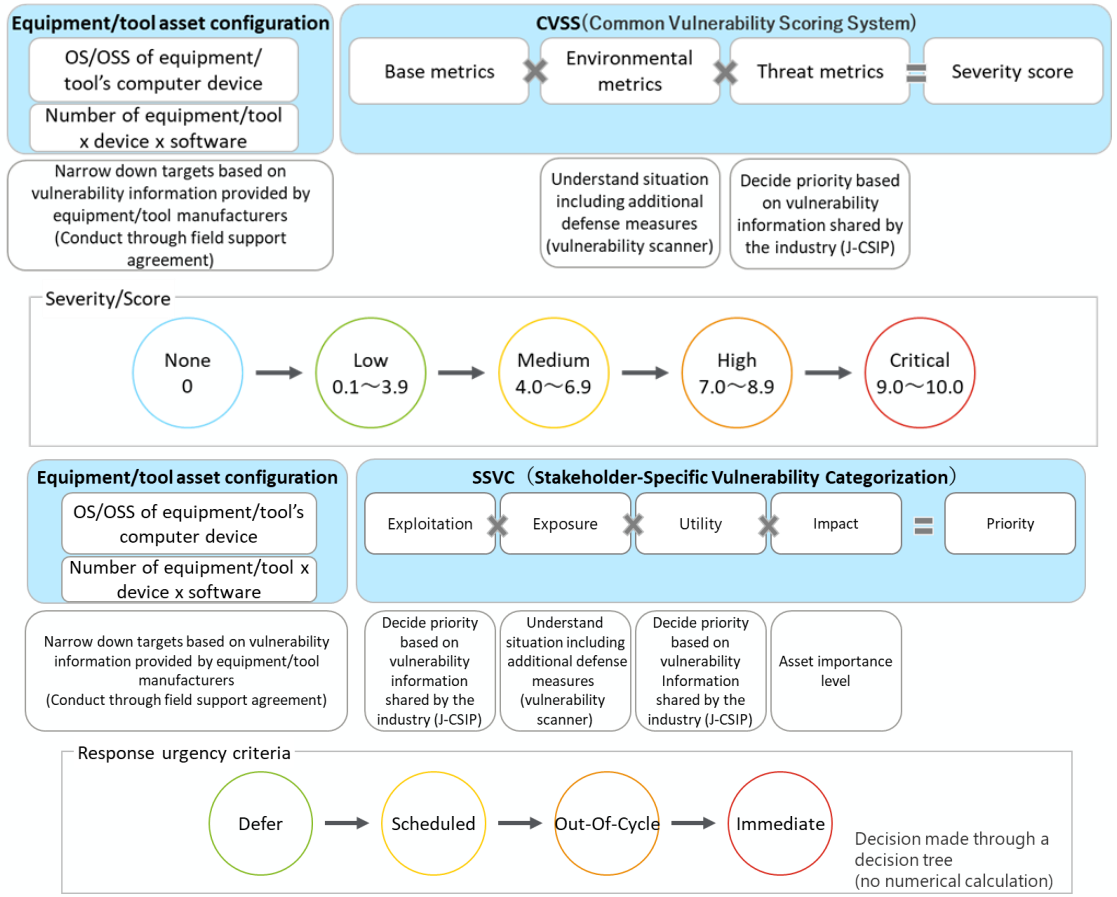
Methods for Collecting Information on Threats to Equipment/Tools

Methods for collecting threat information

- Collecting information from government agencies or public institutions such as NISC, JPCERT/CC, IPA, CISA, US-CERT, ENISA, and CERTEU
- Collecting information from CISA's KEV list and FIRST's 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 SEMI-SMCC-WG5, IT-ISAC Semiconductor Industry SIG, and J-CSIP Semiconductor Industry SIG
- Collecting information obtained from the results of analyses conducted on the company's attack/incident information

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

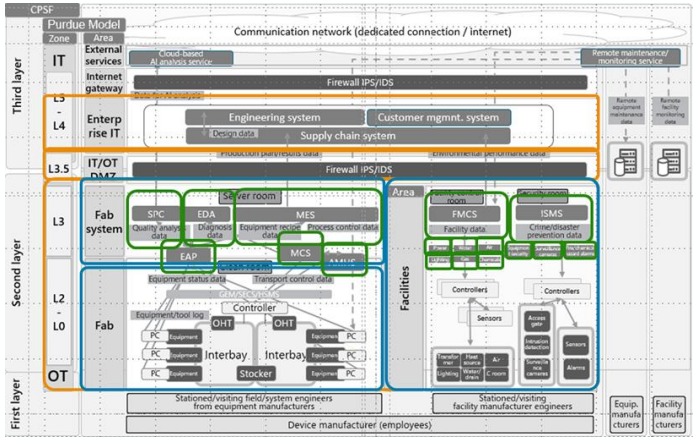
When vulnerability information for equipment/tools is obtained, it is necessary to identify the vulnerabilities of equipment/tools, assess their severity in the context of potential threats from attackers, and determine the appropriate response strategy (e.g., mitigate, avoid, or accept the vulnerabilities) as well as the timing of such actions.

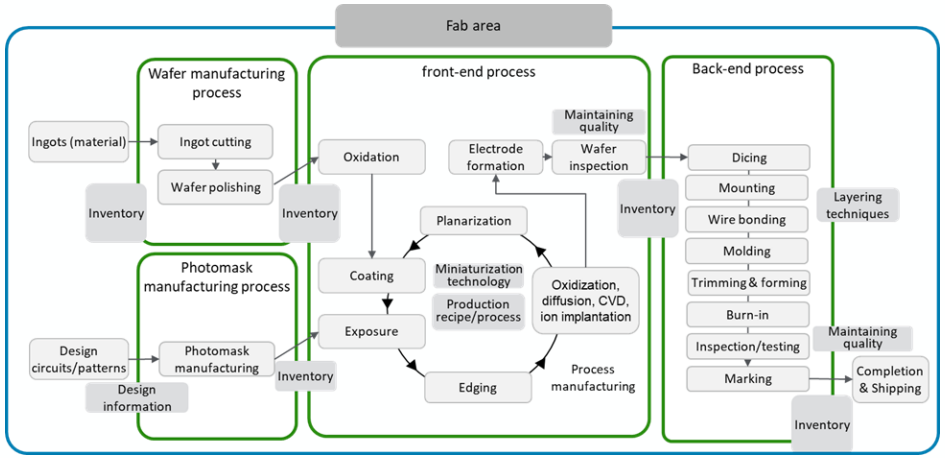


Structure of the Guidelines 4-2. Additional Defense Measures to Minimize Equipment/Tool Damage and to Prepare for Early Recover(1)

- **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.

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)
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)
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) For the fab area, communications are restricted after dividing the network by process for which a production plan is created and executed. (Green frameworks)

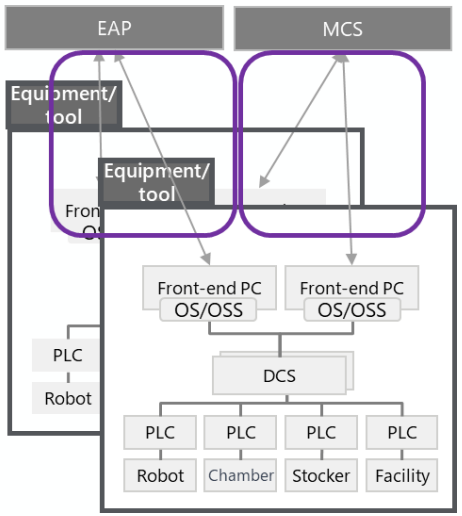


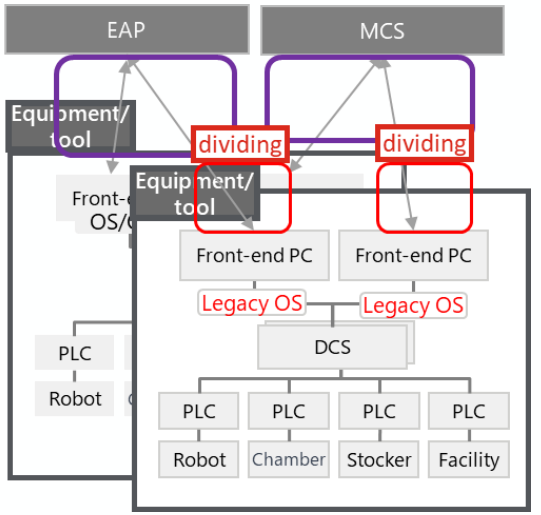


Structure of the Guidelines 4-2. Additional Defense Measures to Minimize Equipment/Tool Damage and to Prepare for Early Recover(2)

- **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.

Network-based defense in depth, microsegmentation, and security monitoring	
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)
5	**Microsegmentation protecting equipment/tools** 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) 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

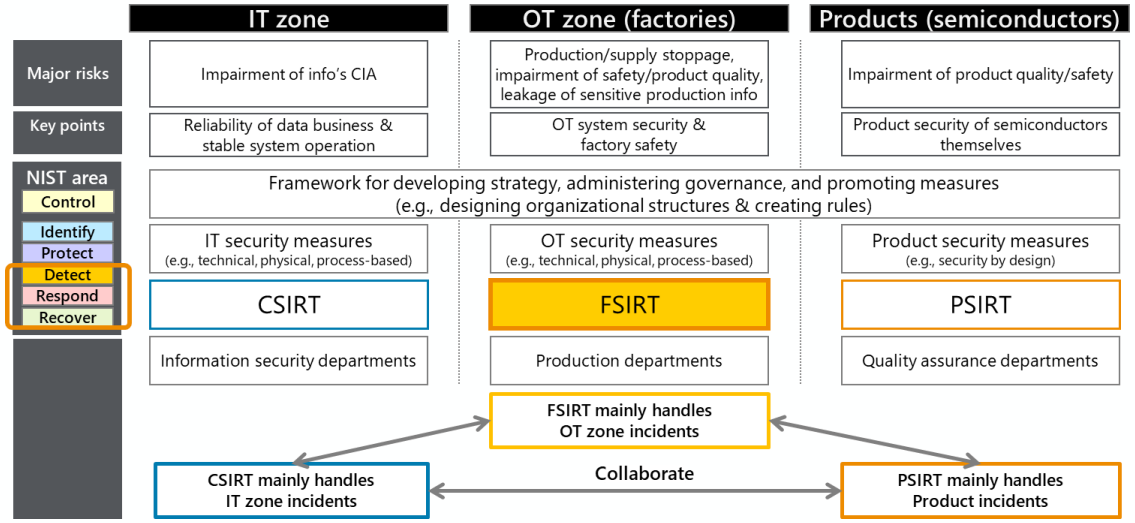




Structure of the Guidelines 4-3. Operations (Monitoring, Response, Recovery, and Improvement):FSIRT Operations(1)

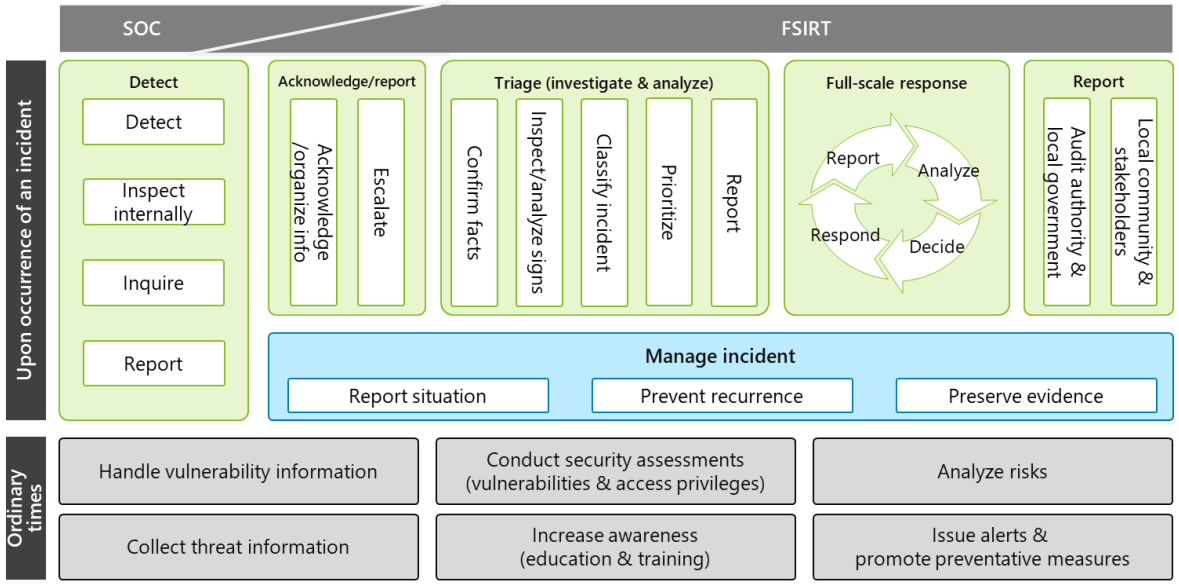
An Example of FSIRT in Semiconductor Device Factories

- **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.**
  Shows an example of FSIRT in semiconductor device factories, responsible for detecting, responding to, and recovering from cyberattacks in the factory OT zone.



FSIRT's Responses in Incident and Ordinary Situations

- **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.



Structure of the Guidelines

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.**

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, onsite 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 media 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


METI
Ministry of Economy, Trade and Industry