SEMI E169-0623
GUIDE FOR EQUIPMENT INFORMATION SYSTEM SECURITY

This Standard was technically approved by the Information & Control Global Technical Committee. This edition was approved for publication by the global Audits and Reviews Subcommittee on February 1, 2023. Available at www.semiviews.org and www.semi.org in June 2023; originally published April 2014; previously published June 2015.

NOTICE: Paragraphs entitled 'NOTE:' are not an official part of this Standard or Safety Guideline and are not intended to modify or supersede the official Standard or Safety Guideline. These have been supplied by the global technical committee to enhance the usage of the Standard or Safety Guideline.

NOTICE: The section symbol (§) is used to reference a numbered section, paragraph, or header and all subordinate paragraphs, headers, and embedded material (i.e., EXCEPTIONs, lists) therein. The paragraph symbol (¶) is used to reference a particular numbered paragraph and embedded material therein. When duplicated (i.e., §§ and ¶¶) the symbols are used to reference more than one section or paragraph, respectively.

1 Purpose

1.1 Incidents, such as the destruction of information by computer virus, confidentiality infringement due to leaked information, and limited information availability due to the denial of service (DOS), are reported daily throughout the world. Semiconductor manufacturing equipment information systems are also exposed to these threats.

1.2 Accordingly, security measures have become an inevitable requirement for semiconductor manufacturing equipment.

1.3 There are requirements for the security of semiconductor manufacturing equipment, such as:

- Malware (virus) protection that does not harm equipment performance.
- Confidentiality protection of recipes that does not degrade equipment operation efficiency.
- Availability of equipment operation log files for troubleshooting without compromising confidentiality security.
- Availability of equipment design information for the user without compromising confidentiality security.

1.4 Security measures are tailored to management plans for semiconductor manufacturing lines by individual equipment users. Negotiations of the security policies for equipment information system between equipment users and suppliers are inefficient because they vary by customer. Furthermore, the robustness and sustainability of these deals has not been substantiated. Guidelines for information security on semiconductor manufacturing equipment are required.

1.5 The purpose of this Standard is to establish a common basis for equipment information system security. This can be shared among users and suppliers of semiconductor manufacturing equipment, suggesting concepts, and measures of information security.

1.6 This Standard is expected to:

- Provide guidelines of applying appropriate security measures for equipment to optimize cost, delivery, and reliability.
- Make the design of user security systems easier and more robust by providing knowledge of the role and responsibility of equipment in the factory.
- Provide a common language to express the needs and evaluation methods of, and gain a consistent understanding within, the industry.
- Promote an open standard to provide a portable and interoperable implementation.

2 Scope

2.1 *Domain*

2.1.1 This Standard covers the domain of semiconductor manufacturing equipment operation.

Documents Document Sharing Hub

Full document details: SEMI E169-0623

2.1.2 The domain includes:

- Entities (person, process, system) that interact with the equipment,
- Data objects of the equipment operation, and
- Embedded information system components inside the equipment.

2.1.3 Entities external to the equipment domain (e.g., factory or company) will be addressed only when that entity is related to the equipment information security.

2.2 *Subjects*

2.2.1 This Standard addresses the following subjects in the creation of guidelines for information security related to equipment operation:

- The goal of information security (Confidentiality, Integrity, Availability)
- Assets to be secured (Equipment Information Asset)
- Roles to be supported by the equipment information system
- Significant security requirements (e.g., malware protection, illegal access protection on networks, local operation, hardware, disposing of components, etc.)

NOTICE: SEMI Standards and Safety Guidelines do not purport to address all safety issues associated with their use. It is the responsibility of the users of the Documents to establish appropriate safety and health practices, and determine the applicability of regulatory or other limitations prior to use.

3 Limitations

3.1 *Change in Time*

3.1.1 This Standard is written to cover security issues currently observed by the SEMI Standards committee. Threats, risks, and/or security technology continue to evolve over time. Therefore, this Standard shall be reviewed and updated regularly to keep pace with the evolving environment.

4 Referenced Standards and Documents

4.1 *SEMI Standards and Safety Guidelines*

SEMI E5 — Specification for SEMI Equipment Communication Standard 2 Message Content (SECS-II)

SEMI E30 — Specification for Generic Model for Communication and Control of Manufacturing Equipment (GEM)

SEMI E37 — Specification for High-Speed SECS Message Service (HSMS) Generic Services

SEMI E90 — Specification for Substrate Tracking

SEMI E116 — Specification for Equipment Performance Tracking

SEMI E132 — Specification for Equipment Client Authentication and Authorization

4.2 *NIST® Standards*[1]

NIST Special Publication 800-30 — Risk Management Guide for Information Technology Systems

NOTICE: Unless otherwise indicated, all documents cited shall be the latest published versions.

5 Terminology

5.1 *Abbreviations and Acronyms*

5.1.1 *DOS* — denial of service

[1] National Institute of Standards and Technology, 100 Bureau Drive, Stop 3460, Gaithersburg, MD 20899-3460, USA; Telephone: +1.301.975.2000, http://www.nist.gov. NIST trademark is owned by National Institute of Standards and Technology.

Documents
Document Sharing Hub
Full document details: SEMI E169-0623

5.1.2 *ECT* — equipment controller terminal

5.1.3 *EDA* — equipment data acquisition

5.1.4 *EIS* — equipment information system

5.1.5 *FTP* — File Transfer Protocol

5.1.6 *IP* — Internet Protocol

5.1.7 *MES* — manufacturing execution system

5.1.8 *OS* — operating system

5.1.9 *RBAC* — role-based access control

5.2 *Definitions*

5.2.1 *access control* — the restriction of access to an information asset via mechanisms used to verify authenticity and authority.

5.2.2 *application* — a software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

5.2.3 *attack* — an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

5.2.4 *audit* — an independent review and examination of records and activities to determine the adequacy of system controls and to ensure compliance with established policies and operational procedures.

5.2.5 *authenticity* — the property of being genuine, verifiable, and trusted; confidence in the validity of a transmission, a message, or a message's originator.

5.2.6 *authentication* — verifying the identity of an entity as a prerequisite to allowing access to resources in an information system.

5.2.7 *authority* — the property of being permitted access to specific information.

5.2.8 *authorization* — verifying the access privilege of an entity to ensure authority.

5.2.9 *denial of service (DOS)* — an attack that exhausts resources to prevent or impair the authorized use of networks, systems, or applications.

5.2.10 *entity* — an active element (person or computer process) that operates on information or the system state.

5.2.11 *firewall* — a hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

5.2.12 *hardening* — configuring a system to reduce the system's security weakness.

5.2.13 *incident* — the occurrence of a problem that harms an information asset and equipment operations.

5.2.14 *information asset* — the property of information on an information system.

5.2.15 *information port* — the interchange point of information between an equipment information system and a factory system.

5.2.16 *log* — a record of equipment operations or activities.

5.2.17 *malware* — a comprehensive term to represent malicious software, such as viruses or spyware, specifically designed to disrupt or damage a computer system or disclose secret information.

5.2.18 *masquerading* — claiming the authentication of another agent by an unauthorized agent.

5.2.19 *mission critical system* — a system that is not permitted to be interrupted for an incident, and is required to be available throughout a year.

5.2.20 *privilege* — a right granted to an individual, a program, or a process.

5.2.21 *proxy server* — a server that services the requests of its clients by forwarding those requests to other servers.

Documents Document Sharing Hub

Full document details: SEMI E169-0623

5.2.22 *risk* — the possibility of an incident that harms an information asset.

5.2.23 *spyware* — software that enables a user to obtain covert information about another computer's activities by transmitting data covertly from their hard drive/memory.

5.2.24 *third layer* — Layer 3 of the OSI model. IP Security (IPsec) that is a suite of protocols securing internet protocol (IP) communications by authenticating and encrypting each IP packet in a data stream can be applied to this layer.

5.2.25 *tampering* — an intentional event resulting in the modification of a system, its intended behavior, or its data.

5.2.26 *threat* — anything that has the potential to cause harm to an information asset.

5.2.27 *vulnerability* — a weakness that could be used to endanger or cause harm to an information asset.

5.2.28 *virus (computer virus)* — a piece of code capable of copying itself and, typically, having a detrimental effect, such as corrupting a system or destroying data.

5.2.29 *zero-day attack* — an attack taking advantage of a vulnerability (security hall) before the existence of the vulnerability is widely publicized.

6 EIS Security Policy

6.1 *Goal of Information Security*

6.1.1 The goal of information security is to assure the confidentiality, integrity, and availability of an information asset.

- Confidentiality is the protection of an information asset, by limiting access, so as not to leak confidential information.
- Integrity is the maintaining robustness of an information asset by protecting information against illegal modification or destruction.
- Availability is the ability to guarantee the timely use of information to a legitimate user.

6.2 *Purpose of the Security System*

6.2.1 The purpose of the security system is to protect the property of the information asset against 'attack' in order to achieve the goal of information security. Attacks can be classified into the classes listed in Table 1. To examine a security measure, the 'the class of attack' should be referred.

Table 1 Classification of Attack

Class of Attack	*Examples of Attack*
Passive Monitoring	Monitoring of information flowing on network Observation of operation on equipment controller terminal (ECT)
Active Network Attack	Invasion or malware injection through network DOS
Exploitation by Insiders	Intentional security violation by legitimate user
Attack by Physical Access or Proximity	Virus infection or information disclosure through external device connection Invasion through ECT Walking off with information storage device stripped off
Malicious Code	Computer virus activation

6.2.2 Specific types of attacks are not always known. Though protection against known types of attacks is a minimum requirement, protection against attacks that aren't known, but can be anticipated due to previous patterns, is also required.

Documents
Document Sharing Hub
Full document details: SEMI E169-0623

6.2.3 EIS should be prepared to protect information against attacks, always considering the possibility of security gaps within the system. For example, systems should be updated in a timely fashion to protect against unexpected attacks, such as zero-day attacks.

6.3 *Management Aspect of Information Security*

6.3.1 *Tradeoffs to the Cost and/or Performance*

6.3.1.1 Measures of reducing risk are applied to maintain security, but the process of lowering risk tends to have adverse effects, such as increasing costs and decreasing system performance for the intended function. The tradeoffs between security performance increase, cost increase, and system performance decrease must be considered and optimally balanced. Cost includes the initial costs plus the running costs of the security system.

6.3.2 *Ease of Use*

6.3.2.1 If the maintenance and operation of the security function is not easy, the effectiveness of the security measure declines. Security measures should be designed to be easy to maintain and operate. Additionally, investment in continued education and training of system administrators and users is required.

6.3.3 *Layered Security*

6.3.3.1 It is important for the security designer to integrate the equipment into the system hierarchy of the user (the company, the factory, etc.). Stacking the user's system onto the equipment increases the effort necessary to attack the equipment. The security system will be more robust due to the layered hierarchy. For example, application gateways, intrusion detection systems, packet filtering, password control, user training, and other measures may be applied in either hierarchy. Determining the optimum distribution of roles and responsibilities between the layers, balancing security performance, security cost, and manufacturing performance, is a requirement.

6.3.4 *Compound Security*

6.3.4.1 Compounding security measures is essential, in addition to layered security. For example, in the case that only one type of security measure is applied to each layer, an invasion may easily penetrate deep inside the system because the protection only needs to be broken once. It is important to compound security measures across those layers.

6.3.5 *Resilience*

6.3.5.1 When an incident has occurred, the information system should limit damage and be resilient to the problem. To fulfill this requirement, the system is required to have a clearly defined strategy to deal with the incident. For example, removing the system in trouble from the line in order to eliminate risk may be part of the strategy. Defining a procedure to recover from incidents is also required, emphasizing the speed of the recovery.

6.3.5.2 The security status of an information system should be managed to indicate incidents. For example, the system may change its status to 'emergency-response', 'recovery', or 'normal-operation.'

6.3.6 *Reliability Obsolescence over Time*

6.3.6.1 The reliability of information security measures decreases over time as technology evolves and environments change. Information security measures should be evaluated and reconsidered regularly. Updating the technologies used and/or introducing new technology are required when new risks are identified.

6.3.6.2 The information system should be designed so as that security measures can be updated easily.

6.3.7 *Improvement Process Implementation*

6.3.7.1 Problems that the design of the system did not anticipate can occur repeatedly and adversely affect information security. It is necessary to learn from the past and continuously implement security improvements, utilizing the experience of non-anticipated problems and exposed vulnerabilities of the system to prevent the recurrence of the problem.

6.4 *Technical Aspects of Information Security*

6.4.1 *Scheme of Risk*

6.4.1.1 Risk is the likelihood that an information asset is damaged by an incident caused by a threat attacking a vulnerability of the information security.

Documents Document Sharing Hub

Full document details: SEMI E169-0623

6.4.1.2 Known threats to information security include illegal access, masquerading, tampering, illegal execution, illegal use, malware execution, and DOS. Malfunctions, performance degradation, failure, or damage/destruction of the information asset can be caused by these attacks. To lower risk, it is necessary to understand the threats, vulnerabilities, attacks, and the potential damage of an incident. Figure 1 illustrates the relations among threat, attack, risk and incident.

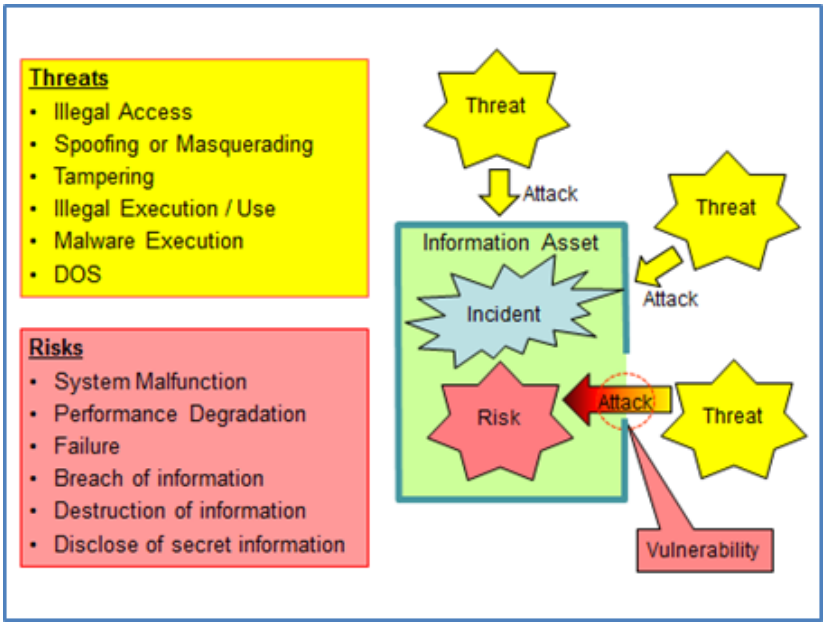

Figure 1
Scheme of the Risk

6.4.2 *Access Control with Authentication and Authorization*

6.4.2.1 Access control of the information asset by means of authentication and authorization is required to prevent attacks such as invasion and unauthorized use.

6.4.2.2 Authentication is a verification process of the authenticity of the entity attempting to access the system. The entity accessing the system should prove its authenticity. Often, user identification (user ID) and password are used to prove authenticity.

6.4.2.3 Authorization is an access control process for an entity based on access privileges for specific parts of the information asset. The entity should be permitted access to the information asset within its specified privileges but should not be permitted access to information that is outside of that privilege.

6.4.2.4 The security system should support access control capability across the entire information system. In order to establish integrated authentication operations, the security system may implement an authentication server that supports authentication of all entities within the domain.

6.4.3 *Assigning Minimum Privilege*

6.4.3.1 The privilege given to an entity should be limited to the minimum privilege required by that entity to perform its role. Assignment of an unnecessarily wide privilege range increases the risk of illegal access. Users and administrators of the system should be given separate access privileges corresponding to their roles. Allowing users privileges that are so-called 'Super-user' increases the risk of illegal access.

6.4.4 *Isolation from Public Access*

6.4.4.1 EIS is characterized as a mission critical system used exclusively for control of the equipment. EIS should be isolated from public access. The environmental domain of the EIS (the factory) should implement measures to isolate

Documents
Document Sharing Hub
Full document details: SEMI E169-0623

public access to the EIS. Additionally, the EIS should apply measures to limit external domain interaction in order to isolate access from the public domain.

6.4.5 *Information Flow Control on Network Boundaries*

6.4.5.1 Control of access and information flow on the network boundary is an essential security requirement. For access and information flow control, the following attributes should be considered:

- External interfaces,
- Information flow mechanisms (push or pull),
- Required ports, protocols, network services, and
- Specifications for information exchange.

6.4.5.2 It should be noted that information flowing out from the EIS should be controlled as well as information flowing into the EIS. The EIS may be used as a step to harm other systems within the factory.

6.4.6 *Requirement of Audit Mechanism*

6.4.6.1 Support for audit mechanisms is required to identify illegal access and to investigate incidents. The EIS should provide the capability to support a regular review of logs for audit activities.

6.5 *Security Across the Entire EIS Life-Cycle*

6.5.1 Security involves different aspects depending on the phase of the information system's life cycle. Phases in the system life cycle should be identified to provide a framework for risk management.

6.5.2 NIST, in its document (NIST Special Publication 800-30), has provided definitions of these phases and can be applied to the EIS. Table 2 shows phase definitions quoted from the NIST document.

Table 2 Phase in the Information System Life Cycle

Phase	*Description*	*Remark for Risk Management*
Phase 1 – Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented.	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy).
Phase 2 – Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed.	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development.
Phase 3 – Implementation	The system security features should be configured, enabled, tested, and verified.	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation.
Phase 4 – Operation or Maintenance	The system performs its functions. Typically, the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces).
Phase 5 – Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software.	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

Documents Document Sharing Hub
Full document details: SEMI E169-0623

7 Equipment Information Asset

7.1 An equipment information asset is a representation of the objects that should be protected against threats. The information asset contains the equipment information system (EIS) and the equipment information it manages. An example of the equipment information assets is shown in Figure 2.

NOTE 1: Figures and descriptions in this section are not intended to specify implementation of the information asset but to introduce the concept of information asset.

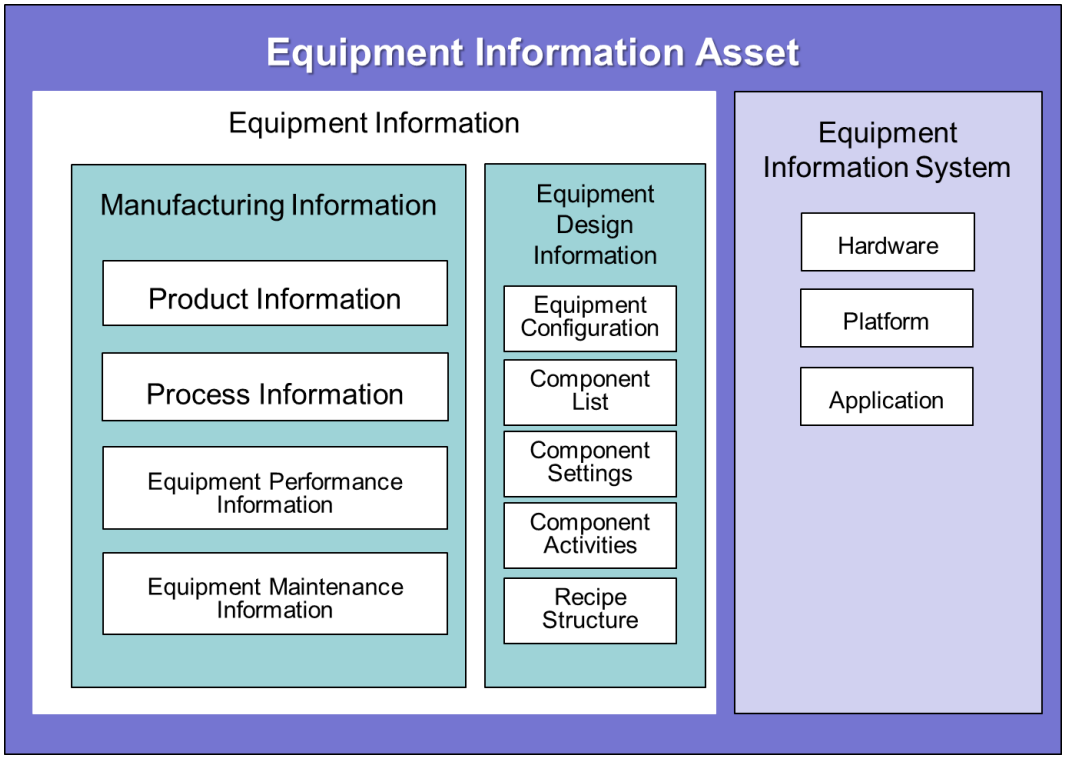

Figure 2
Example of Equipment Information Asset

7.2 *Equipment Information*

7.2.1 Equipment Information is all of the information managed by the EIS. Equipment Information is classified into manufacturing information and equipment design information.

7.2.2 *Manufacturing Information*

7.2.2.1 Manufacturing information contains information about the planning, execution, and results of the manufacturing activities on the equipment. If the manufacturing information has been disclosed, production techniques can be identified by competitors, damaging the user's business. Therefore, manufacturing information should be considered classified information.

7.2.2.2 Manufacturing information contains product information, process information, equipment performance information, and equipment maintenance information.

7.2.2.3 *Product Information*

7.2.2.3.1 Product information is related to the product to be processed (or manipulated) by the equipment. Product information may contain confidential contextual information such as the name, type, client, delivery, or quantity of the product. Product information may also involve process status, such as current process flow step, manufacturing yield, or product quality.

Documents
Document Sharing Hub
Full document details: SEMI E169-0623