Background Statement for SEMI Draft Document 5422A

**New Standard: GUIDE FOR EQUIPMENT INFORMATION SYSTEM SECURITY**

**Notice**: This background statement is not part of the balloted item. It is provided solely to assist the recipient in reaching an informed decision based on the rationale of the activity that preceded the creation of this Document.

Incidents of information security violation via virus infection, security failure, or leakage of valuable information are reported daily throughout the world. Semiconductor manufacturing equipment is also exposed to security threats; viruses and data leakage/destruction have been reported in manufacturing facilities.

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.

Agreement on concepts and technology for semiconductor manufacturing equipment information security is required in the industry.

* Challenge 1 – Application of Anti-virus Software

The application of anti-virus software is inevitable for every information system today. Semiconductor manufacturing equipment information systems are no exception, but the need to install anti-virus software brings up the argument that anti-virus software degrades the performance of the equipment’s intended functions. Anti-virus software also requires equipment downtime for pattern file updates.

These requirements raise issues for the design and operation of semiconductor manufacturing equipment. Guidelines for the application of anti-virus software are required in order to provide common understanding of security measures and to optimize implementation throughout the industry.

* Challenge 2 – Process Information Protection

Process information includes process specification (including recipes and other settings on the equipment) and process data, and is regarded as the intellectual property of the IC device manufacturer. Equipment is required to support the ability to prevent the disclosure of intellectual property. For instance, recipes should not be viewed by unauthorized individuals or transferred to unknown clients.

Guidelines are required to secure intellectual property.

* Challenge 3 – Log Information Utilization

Log files of semiconductor manufacturing equipment operation record comprehensive information related to the processes, equipment activity/behaviors, and/or manufacturing of a product. Because the information recorded on log files is considered intellectual property, the log files should be secured and not disclosed.

On the other hand, log files contain valuable information for troubleshooting. While the information in log files must be kept from unauthorized individuals, the log files should be available, when required, to individuals who need the information for maintenance. The challenge is to provide availability of log information while maintaining confidentiality.

Guidelines are required to ensure the availability of the information required for troubleshooting.

* Framework for understanding and thinking of the best practice

Numerous aspects exist in information security, and these aspects are often interrelated. These aspects must be captured and characterized.

These guidelines will address the framework for information security on semiconductor manufacturing equipment and introduce challenges and ideas for the best practice of security measures. Sharing the concepts of security challenges and ideas regarding the required measures will help designers and users of information systems to efficiently optimize their systems.

**Notice**: Recipients of this Document are invited to submit, with their comments, notification of any relevant patented technology or copyrighted items of which they are aware and to provide supporting documentation. In this context, “patented technology” is defined as technology for which a patent has been issued or has been applied for. In the latter case, only publicly available information on the contents of the patent application is to be provided.

The ballot results will be reviewed and adjudicated at the meetings indicated in the table below. Check [www.semi.org/standards](http://www.semi.org/standards) under Calendar of Events for the latest update.

**Review and Adjudication Information**

|  |  |  |
| --- | --- | --- |
|  | **Task Force Review** | **Committee Adjudication** |
| **Group:** | Equipment Information System Security (EISS) TF | Japan Information and Control Committee |
| **Date:** | Thursday, December 5, 2013 | Friday, December 6, 2013 |
| **Time & Timezone:** | 13:00-17:00, Japan Time | 13:00-17:00, Japan Time |
| **Location:** | Makuhari Messe | Makuhari Messe |
| **City, State/Country:** | Chiba, Japan | Chiba, Japan |
| **Leader(s):** | Mitch Sakamoto (Tokyo Electron) | Takayuki Nishimura (Dainippon Screen Mfg.) Mitsuhiro Matsuda (Hitachi Kokusai Electric) |
| **Standards Staff:** | Chie Yanagisawa (SEMI Japan)+81.3.3222.5863 / cyanagisawa@semi.org | Chie Yanagisawa (SEMI Japan)+81.3.3222.5863 / cyanagisawa@semi.org |

This meeting’s details are subject to change, and additional review sessions may be scheduled if necessary. Contact Standards staff for confirmation.

Telephone and web information will be distributed to interested parties as the meeting date approaches. If you will not be able to attend these meetings in person but would like to participate by telephone/web, please contact Standards staff.

If you need a copy of the documents in order to cast a vote, please contact the following person within SEMI.

Chie Yanagisawa

SEMI Standards, SEMI Japan

Tel: 81.3.3222.5863

Email: cyanagisawa@semi.org

|  |  |  |  |
| --- | --- | --- | --- |
| ***Revision*** | ***Date Issued*** | ***Description*** | ***Remark*** |
| 1.0 | 2013/02/04 | First draft for the ballot cycle April 2, 2013 |  |
| 2.0 | 2013/06/17 | Draft for task force review for cycle 6 |  |
| 3.0 | 2013/08/12 | Ballot for cycle 6, 2013 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

SEMI Draft Document 5422A

New Standard: GUIDE FOR EQUIPMENT INFORMATION SYSTEM SECURITY

1. Purpose
	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, are reported daily throughout the world. Semiconductor manufacturing equipment information systems are also exposed to these threats.
	2. Accordingly, security measures have become an inevitable requirement for semiconductor manufacturing equipment.
	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. 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.
	2. 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.
	3. 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.
1. Scope
	1. Domain
		1. This standard covers the domain of semiconductor manufacturing equipment operation.
		2. The domain includes:
* Entities (person, process, system) that interact with the equipment
* Data objects of the equipment operation
* Embedded information system components inside the equipment
	+ 1. 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.
	1. Subjects
		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.

1. Limitations
	1. Change in Time
		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.
2. Referenced Standards and Documents
	1. *SEMI Standards and Safety Guidelines*

SEMI E5 – SEMI Equipment Communication Standard 2 Message Content (SECS-II)

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

SEMI E37 – High-Speed SECS Message Service (HSMS)

SEMI E40 – Standard for Processing Management

SEMI E87 – Specification for Carrier Management

SEMI E90 – Specification for Substrate Tracking

SEMI E94 – Specification for Control Job Management

SEMI E116 – Specification for Equipment Performance Tracking

SEMI E120 – Specification for the Common Equipment Model (CEM)

SEMI E125 – Specification for Equipment Self Description (EQSD)

SEMI E132 – Specification for Equipment Client Authentication and Authorization

SEMI E134 – Specification for Data Collection Management

SEMI E139 – Specification for Recipe and Parameter Management (RaP)

SEMI E147 – Guide for Equipment Data Acquisition (EDA)

SEMI E148 – Specification for Time Synchronization and Definition of the TS-Clock Object

SEMI E157 – Specification for Module Process Tracking

* 1. *ISMI* *Documents*

ISMI Technology Transfer #04104567C-ENG: Semiconductor Equipment Security Guidelines - Virus Protection

ISMI Technology Transfer #07114888A-ENG: Semiconductor Equipment Security Guidelines - Intellectual Property Protection

* 1. *NIST* *Documents*[[1]](#footnote-1)

NIST IR 7298 Revision 1, Glossary of Key Information Security Terms

NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security

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

* 1. *Other Documents*

Equipment Engineering Capabilities (EEC) Guidelines (Phase 2.5), ISMI & JEITA/Selete

CIM Joint Guidance for 300 mm Semiconductor Factories, Release Five, ISMT and J300E

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

1. Terminology
	1. *Abbreviations and Acronyms*
		1. *DOS* – Denial Of Service
		2. *ECT* – Equipment Controller Terminal
		3. *EDA* – Equipment Data Acquisition
		4. *EES* – Equipment Engineering System
		5. *EIS* – Equipment Information System
		6. *EP-ITS* – Engineering Principles for Information Technology Security (NIST document)
		7. *FTP* – File Transfer Protocol
		8. *IP* – Intellectual Property. Example: IP Protection.
		9. *IP* – Internet Protocol. Example: IP address.
		10. *ISMI* — International SEMATECH Manufacturing Initiative
		11. *MES* – Manufacturing Execution System
		12. *NIST* — National Institute of Standards and Technology
		13. *OS* – Operating System
		14. *SQL* – Structured Query Language
	2. *Definitions*
		1. *access control –* The restriction of access to an information asset via mechanisms used to verify authenticity and authority.
		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.
		3. *attack* – An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
		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. *authenticity* – The property of being genuine, verifiable, and trusted; confidence in the validity of a transmission, a message, or a message’s originator.
		6. *authentication –* Verifying the identity of an entity as a prerequisite to allowing access to resources in an information system.
		7. *authority –* The property of being permitted access to specific information.
		8. *authorization* – Verifying the access privilege of an entity to ensure authority.
		9. *denial of service (DOS)* – An attack that exhausts resources to prevent or impair the authorized use of networks, systems, or applications.
		10. *entity* – An active element (person or computer process) that operates on information or the system state.
		11. *firewall* – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.
		12. *hardening* – configuring a system to reduce the system’s security weakness.
		13. *incident* — The occurrence of a problem that harms an information asset and equipment operations.
		14. *information asset* – The property of information on an information system.
		15. *information port* – The interchange point of information between an equipment information system and a factory system.
		16. log – A record of equipment operations or activities.
		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.
		18. *masquerading* – Claiming the authentication of another agent by an unauthorized agent.
		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.
		20. *privilege* – A right granted to an individual, a program, or a process.
		21. *proxy server* – A server that services the requests of its clients by forwarding those requests to other servers.
		22. *risk* – The possibility of an incident that harms an information asset.
		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.
		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.
		25. *tampering* – An intentional event resulting in the modification of a system, its intended behavior, or its data.
		26. *threat* – Anything that has the potential to cause harm to an information asset.
		27. *vulnerability* – A weakness that could be used to endanger or cause harm to an information asset.
		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.
		29. *zero-day attack* – An attack taking advantage of a vulnerability (security hall) before the existence of the vulnerability is widely publicized.
2. EIS Security Policy
	1. Goal of Information Security
		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.
	1. Purpose of the Security System
		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.

Classification of Attack

|  |  |
| --- | --- |
| *Class of Attack* | *Examples of Attack* |
| Passive Monitoring | Monitoring of information flowing on networkObservation of operation on ECT (Equipment Controller Terminal) |
| Active Network Attack | Invasion or malware injection through networkDOS (Denial of Service) |
| Exploitation by Insiders | Intentional security violation by legitimate user |
| Attack by Physical Access or Proximity | Virus infection or information disclosure through external device connectionInvasion through ECTWalking off with information storage device stripped off |
| Malicious Code | Computer virus activation |

* + 1. 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.
		2. 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.
	1. Management Aspect of Information Security
		1. Tradeoffs to the Cost and/or Performance
			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.
		2. Ease of Use
			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.
		3. Layered Security
			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.
		4. Compound Security
			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.
		5. Resilience
			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.
			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. Reliability Obsolescence over Time
			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.
			2. The information system should be designed so as that security measures can be updated easily.
		7. Improvement Process Implementation
			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.
	2. Technical Aspects of Information Security
		1. Scheme of Risk
			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.
			2. Known threats to information security include illegal access, masquerading, tampering, illegal execution, illegal use, malware execution, and denial-of-service (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.



1. Scheme of the Risk
	* 1. Access Control with Authentication and Authorization
			1. Access control of the information asset by means of authentication and authorization is required to prevent attacks such as invasion and unauthorized use.
			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.
			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.
			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.
		2. Assigning Minimum Privilege
			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.
		3. Isolation from Public Access
			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 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.
		4. Information Flow Control on Network Boundaries
			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
* Specifications for information exchange
	+ - 1. 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.
		1. Requirement of Audit Mechanism
			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.
	1. Security Across the Entire EIS Life-cycle
		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.
		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.

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. |

1. Equipment Information Asset
	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.
	2. Note: Figures and descriptions in this section are not intended to specify implementation of the information asset but to introduce the concept of information asset.



1. Example of Equipment Information Asset
	1. Equipment Information
		1. Equipment Information is all of the information managed by the EIS. Equipment Information is classified into manufacturing information and equipment design information.
		2. Manufacturing Information
			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.
			2. Manufacturing information contains product information, process information, equipment performance information, and equipment maintenance information.
			3. Product Information
				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.
			4. Process Information
				1. Process information represents how a product is going to be processed by the equipment and contains process specifications and process data.
				2. Process specifications define procedures and settings for the process (or manipulation) of the target product object. Process specifications may include such information as product design data (e.g. mask patterns), process flow, recipes, and recipe parameters.
				3. Process data represents equipment behavior in response to the process specifications. That is, the data represents processes or manipulations that are applied to the target product object.
			5. Equipment Performance Information
				1. Equipment performance information represents the performance of the equipment, such as reliability, availability, maintainability, and throughput of the equipment. For example, data collected on equipment based on the SEMI standard E116 (Equipment Performance Tracking) or E90 (Substrate Tracking) may be included in equipment performance information.
			6. Equipment Maintenance Information
				1. Equipment maintenance information is used to conduct maintenance activities in order to maintain performance of intended functions. Equipment maintenance information includes recipes for maintenance and scheduled time intervals for maintenance.
			7. Equipment Design Information
				1. Equipment design information represents the information related to the design of the equipment. Equipment design information includes equipment structure, lists of components, setting of components, component behaviors (such as control sequence), recipe structures, and recipe element names and settings.
				2. If equipment design information is disclosed to a competitive equipment supplier, the design could be copied, damaging the equipment supplier’s business. Equipment design information is owned by the equipment supplier and is considered confidential.
		3. Instances of Equipment Information
			1. Instances of equipment information are contained in the information system’s transactions, storage, and running processes. An example of the relation between the equipment information asset and the equipment information instance is shown in Figure 3.
			2. If the instances of equipment information correspond exactly to the classification of the equipment information, then access to the equipment information can be controlled by controlling access to the instances. However, on typical equipment implementation, equipment information class does not correspond to the class of instance. The equipment information instance contains a mix of the equipment information classes. For example, the equipment operation log may contain process information and equipment design information.
			3. Studying how the equipment information has been separated or mixed within the instance is required to design access control.



1. Example of Equipment Information Instance
	1. Equipment Information System (EIS)
		1. The EIS itself is a part of the information asset to be secured. The EIS includes hardware, platforms, and applications.
		2. Hardware
			1. Hardware represents components of the EIS that are used to transfer or store information, or to execute software programs. Hardware includes communication network interfaces, embedded computers, memory, hard discs, or any devices to control/manage the equipment functions.
		3. Platform
			1. A platform is basic software that is implemented with an operating system to support the management of information and the execution of application programs.
		4. Application
			1. An application is a software program that executes a specific function directly for the user, such as equipment control or equipment engineering.
		5. Ports and Components of the EIS
			1. Figure 4 shows information ports and components of an EIS. The EIS interacts with the factory system through the information port. With the information port being the point of incursion to the equipment information asset, there exists the likelihood of vulnerabilities.
			2. The equipment information port, network port, equipment controller terminal (ECT) port, and external device port are identified in this standard. Access control should be implemented on these ports to protect the information asset from illegal access.



1. Ports and Components of the EIS
	* + 1. Another point of vulnerability exists within the components of the EIS. The vulnerability of the operating system (OS) often poses problems. Data storage is a distinctive target of attacks. Embedded communication networks can be used to attack EIS components.
			2. Network Port
				1. Network ports connect the EIS to an MES host, EDA client, or other applications. Examples of communication service through the network port are listed in table 3. Security measures should be implemented corresponding to the characteristics of the individual communication service. Security of the individual service will be discussed in section 9- Security Practice.

Services on the EIS Network Port

| *Category* | *Service* | *Comment* |
| --- | --- | --- |
| SEMI Standard (Factory-Equipment) Communication Service | GEM/SECS | HSMS Connection |
| EDA  | SOAP/XML based |
| Generic Service | File Transfer | e.g. FTP, File Share |
| Remote Login | e.g. TELNET |
| User Communication | e.g. Web Browser, E-mail, Chat |
| Other | Application Specific | e.g. SQL, Remote Equipment Control Terminal Connection |

* + - 1. Equipment Control Terminal (ECT) Port
				1. The equipment controller terminal (ECT) port connects the EIS to the terminal that has implemented a display and a keyboard or touch panel and is used by humans to operate the EIS. In general, at least one ECT is placed within the equipment proximity. ECT ports may be implemented with multiple hardware connectors to support multiple terminals, or the terminal may be extended to the remote location (Remote ECT).
			2. External Device Port
				1. External device ports connect devices such as USB memory, hard disc drives, CD drives, FD drives, or smart phones to the EIS. In some cases, computer systems for diagnostics may require connections to the external device port.
			3. Embedded Components
				1. The EIS has various embedded components such as data storage, internal communication networks, computer systems, operating systems, and/or sensors/actuators that are used to the control equipment functions (process or manipulation). Appropriate security measures should be applied for these components.
			4. Integrated Computer System
				1. If an EIS component implements an embedded computer system on itself (such case as integrated metrology), security measures should be applied recursively to the component.
1. Roles of the EIS
	1. In this section, roles of the EIS are identified as a part to be integrated into the security measures of the factory.
	2. Position of the EIS in the Factory System
		1. The EIS is a computer system used exclusively for equipment operation, such as equipment controllers or equipment engineering systems. The EIS is typically implemented by the equipment supplier.
		2. EIS security should be designed to be integrated as a component of the operations of the factory system, as shown in figure 5.



1. Position of the EIS
	1. Security by Factory System
		1. The factory system is the environment that entirely envelopes EIS security. Ideally, the factory system implements a robust security system with state-of-the-art technologies. A layered security plan by a factory system is shown in figure 6. The security of the factory system may include:
* The isolation of factory networks from the internet or IC maker’s office networks
* The application of network security technologies such as firewalls, proxy servers, and third layer access controls
* The practice of access control by assigning authentication and authorization to individual entities
* The application of state-of-the-art protection measures against malware



1. Factory System
	1. Security by the EIS
		1. As part of the entire security system, the EIS is required to implement measures to protect information asset against attacks that get past the factory system layer of security. Threats that cause attacks may exist even in the factory system. At a minimum, the EIS should implement the following security measures:
* Malware protection
* Disabling unused services and programs
* Access control
* Classification and separation of information
* Providing security audit information
	+ 1. Malware Protection
			1. The EIS should implement the capability to protect the information assets against malware. Required capabilities include malware incursion protection, malware eradication, and malware execution denial. Off-the-shelf software such as “anti-virus” programs is commonly applied for this purpose.
		2. Deactivating Unused Services and Programs
			1. The EIS should deactivate unnecessary services and programs that are not used for the intended function of the equipment, including programs running in the background such as system services or daemons. Risk is decreased by limiting services and programs to only those required for equipment operation. For example, a web browser may be a distinct program that is not required for equipment control.
		3. Access Control
			1. The EIS should implement the capability of controlling access to equipment information assets from humans, programs, and processes, via authentication and authorization. The EIS should control access so that only legitimate users are allowed to access and operate the equipment information asset.
			2. The user should be given the privilege for individual operations. In general, the operation is classified as:
* Read information
* Write information
* Edit information
* Delete information
* Execute/control function/program
	+ - 1. Figure 7 shows an image of access control in which the user is a person accessing the information asset. The access proxy is a system providing the user a means of accessing the information asset. It includes an external device, equipment control terminal, or program (on a network).
			2. Authentication provides the ability to deny illegal access and authenticate legitimate access via account and password verification. Authorization is the ability to specify and limit access to a specific information asset.



1. Image of Access Control
	* 1. Classification and Separation of Information
			1. Equipment information should be classified and separated to protect intellectual property. Access permission for the subject should be controlled by the separated subset of equipment information.
		2. Providing Security Audit Information
			1. The EIS should support the ability to provide information for security audits. Access to the equipment information asset should be recorded in order to provide information for the audit’s security review. For the access control audit, it is important to record operations (who, what, when, where, how) to the information asset in order to identify illegal activities.
	1. Coordination of the Compound Security
		1. As described in the section 6.3.4, security measures on equipment should be implemented as to fit into the compound security of the factory level. Security of equipment layer should be configured so that it can coordinate with the factory layer. Suppliers and IC Makers need to coordinate design of the configuration.
2. EIS Security Practice
	1. In this section, practices of the EIS for semiconductor manufacturing are discussed.
	2. Malware Protection Software Implementation
		1. In an EIS environment where the factory system has implemented information security, one might believe that there is only a small chance for the EIS to be infected with malware. Despite this, the EIS is also required to implement protection measures against malware (i.e. the implementation of malware protection software), since external systems do not always assure stability.
		2. Malware Protection with Black List
			1. Malware protection software based on the black list method uses malware patterns to detect malware. For example, some malware protection software scans the information on the EIS to compare it to the malware patterns.
			2. Risk of Black List: Performance Degradation
				1. In general, applications on the EIS (such as equipment controllers or equipment engineering capabilities) require system performances that enable a response to any event in real-time. The performance of the equipment’s intended function will be degraded when the malware protection software scans the system because the software consumes a certain amount of computer power.
			3. Risk of Black List: Pattern Update Requirement
				1. Malware protection software with the blacklist needs a pattern file. The pattern file must be updated frequently to maintain protection against constantly evolving malware. Since updates need a file download and deployment, the operation and performance of equipment will be hindered by every update applied to the pattern file on the EIS.
			4. Risk of Black List: Operating System Lifecycle
				1. Support of operating systems embedded on the EIS must be provided. This is to prevent the case where support of the operating system is terminated while the equipment is still used in the life-cycle. Support of the malware protection software can be terminated along with termination of the operating system support, leading to the system not having protection against newly emerging malware.
			5. Malware Protection with White List
				1. Malware protection software with white list has a list of programs that are permitted to run on the system and only allows the programs registered on that list to be activated. Programs not registered on the list, including malware, are not allowed to be activated.
				2. Malware protection software with white list is known as software that poses less equipment performance degradation because it consumes less computer power. Therefore malware protection with white list is a suitable malware protection method for real-time applications such as equipment controllers.
			6. Risk of White List: Malware Activation in Maintenance
				1. It should be noted that malware protection with white list does not provide the ability to detect or eradicate malware. Malware will be given the chance to activate itself while the white list malware protection is suspended, such as during maintenance.
				2. In the case of white list malware protection is suspended, use of black list malware protection may be required to check lurking threats prior to the suspension.
			7. Risk of White List: Setup Labor
				1. Setup to register the programs and services that are allowed to run on the EIS is required for the function of malware protection with white list. The operation of the setup should be as easy as possible. Semiconductor manufacturing equipment is often required to implement a user’s requirement for special capabilities. As a result, it may have a number of versions. Setup of the white list will be required for each equipment version change. Moreover, the setup may be required at the site where the equipment is installed. Time and cost should be planned with consideration of the setup work.
		3. Summary of the Black List and the White List
			1. Table 4 summarizes the malware protection software.

Summary of Black List/White List Comparison

|  |  |  |
| --- | --- | --- |
|  | ***Black List*** | ***White List*** |
| Function | Detect and eradicate malwares | Suppress unauthorized program activation |
| Method | Scan storage | Control program activation |
| Specification  | Pattern File  | Selection of executable programs |
| Update | Frequently required | Required when adding programs to the list |
| Real-time application | Not recommended | Recommended |
| Comment |  | Need to scan with Black List before the white list malware protection is suspended |

* + 1. Operating System Security Patch
			- 1. Security patches are often required to eliminate the vulnerability of an operating system. Downloading and deployment of a patched program is required.
			1. Equipment Downtime Requirement
				1. In general, the manufacturing capability of the equipment should be halted while a patch operation is in progress. The equipment should be in a scheduled downtime state so that the availability of the equipment will not be affected.
			2. Risk of Patch Application Delay
				1. In general, patches should be applied to a system as soon as possible after the patch has been released. However, in the practice of the EIS, patches are not always applied to the system at the time of their release. Due to the requirement of maximizing equipment uptime, halting equipment operations to apply a patch may not be allowed, even when the patch application is required. This delays the application of the security measure until the next operational breakpoint for the equipment. Factory-level security will be required to cover the vulnerability of the equipment until the patch is applied.
			3. Performance Verification Requirement after Patch
				1. In general, when an operating system has been updated, application programs that run on that operating system should have their performance verified before the application is released for the production. The verification process requires a certain amount of time to complete.
	1. Access Control
		1. Access control is the basic capability applied to the protections against a wide range of threats.
		2. Factory Confidentiality Requirements
			1. Manufacturing information is the intellectual property of the IC maker or foundry. The IC maker or foundry would suffer damage if the intellectual property is leaked or if any manufacturing information was disclosed to a competitor’s IC maker or foundry. Access to the manufacturing information should be strictly limited to people identified as legitimate users.
			2. There are a variety of situations where the classification and separation of manufacturing information is required. For example, where processes are developed by multiple IC makers in a shared consortium factory environment, process information should be classified and separated among those IC makers.
			3. As another example, when a foundry is manufacturing products ordered by an IC maker, the manufacturing information should be separated from other customers’ manufacturing information. Detailed consideration of manufacturing information is required before classifying and separating it.
			4. Example of Factory Information Security: Recipe Security
				1. Recipes must be securely managed in all three aspects (confidentiality, integrity, availability). Security measures will be required for the recipe in the following forms:
* On storage: in general, recipe information is recorded on a recipe file and the file is stored in a folder. In this situation, security of the recipe is practiced via access control to the file or folder.
* On equipment control terminals: in general, recipes can be read from the recipe file, and displayed and edited on the equipment control terminal. Access control should be practiced with respect to recipe operations at the equipment control terminal to avoid any illegal operations.
* On communication: in general, recipe information is downloaded or uploaded from/to the factory system through communication networks. Procedures of authentication and authorization should be practiced by the factory systems communicated with.
	+ - 1. Example of Recipe File Management
				1. Requirements for the security of recipe file management include:
* Identification of the owners and users of the recipe
* Separation of recipe files by the owners and users
* Access Control by the owners and users
* Restriction of recipe transfers
	+ - * 1. One of the easiest recipe file-transfers uses USB memory. But this method of file transfer poses higher risk. Using well defined method of information transfer that allows inspections and audits is recommended. SEMI communication standard SECS (SEMI E5) has defined the recipe transfer method that can be applied for this purpose.
				2. For inspections and audits, traceability of recipe operations will be required. This requires recording such information as who operated the recipe, what recipe was operated, and when, where, and how it was operated.
		1. Confidentiality Requirements of Equipment Design Information
			1. Hardening against Cyber-attacks
				1. Cyber-attacks are easier if the equipment design information (such as configurations or specifications) of the EIS is publicly known. For example, knowledge of the specifications of the communication bus used in the EIS provides a significant clue for cyber-attackers. To protect against cyber-attacks, equipment design information should be secured.
			2. Equipment Suppliers’ Intellectual Property Protection
				1. Equipment design information (such as equipment configurations, control sequences, or component condition settings) should not be disclosed to other equipment suppliers. Equipment design information should be hidden as much as possible by the equipment supplier.
				2. Equipment design information is often required to be provided to the equipment user in order to improve equipment performance. In this case, appropriate access control should be applied based on a non-disclosure contract between the equipment user and supplier. It is desirable for the equipment design information to be classified and separated in the equipment information asset.
		2. Requirement for Information Availability
			1. In the practice of equipment operation on the factory floor, there is a significant need to share confidential information both ways between the equipment user and the supplier. For example, the equipment user may tweak factory operation by referring to the equipment design information within the supplier’s confidential information in order to run the equipment stably. Conversely, the equipment supplier may refer to the manufacturing information of the equipment user’s confidential information in order to provide troubleshooting.
			2. Thus, information should be available when use of the information is required to achieve higher factory performance. Security measures should be designed to provide required information, maintaining mutual confidentiality between the user and the supplier. For this purpose, classification and separation of information should be applied.
			3. Example of Availability Requirement: Log File Security
				1. Log files record various information regarding equipment operations. Log files are reviewed for analysis and consideration of improvement.
				2. In general, log files contain a mix of manufacturing information and equipment design information. In that situation, a user’s intellectual property is not separated within the file. Because of this, log file transfers for review are often denied by the equipment user to protect confidentiality.

For example, SECS communication logs record the communication history with the MES host and contain indispensable information for troubleshooting of the automation. The communication log contains various kinds of equipment operation information including such transactions as recipe downloads/uploads, process result data, and equipment performance data.

* + - * 1. Meanwhile, because log files provide significant information for troubleshooting, they are required to be available at certain occasions. Factory productivity is maintained by saving troubleshooting time via the review of log file information.
				2. Well-defined access control strategies for log file operations should be designed and practiced in order to secure the user’s confidentiality requirement and the supplier’s availability requirement. The strategy should be agreed upon by the user and the supplier in a contract.
		1. Account and Password
			1. Accounts and passwords are fundamental to access control and are applied to identify the authenticity of individual entities accessing to the operating system or applications such as equipment controllers or equipment engineering systems.
			2. Individual Authentication and Password Policy Requirements
				1. There are various ways to implement authentication on equipment. Legacy traditional equipment controllers may not have an account/password system, or may only have a simple authentication system without a well-designed authentication strategy. Authentication today requires that the account is assigned to an individual entity and that a robust password policy is applied.



1. Account/Password Policy
2. NR = Not Recommended
	* + 1. Examples of the password policy are:
* Require a minimum text length for the password.
* Require mixing character types (alphabet, number, special characters) for the password.
* Deny text that is conceivable with any context for the password (e.g. “password”).
* Invalidate expired account and/or password
* Any combination of these policies
	+ 1. Multi-Level, Multi-Entity Authentications
			1. In general, a modern EIS is required to authenticate multiple entities. For example, as shown in figure 9, an EIS has OS-level authentication and application-level authentication. Application-level authentication may be required for multiple applications including the ECT, EES client, and/or file transfer service.



1. Multiple Level, Multi-Entity Authentication
	* + 1. Authentication management for both the operating system and the application should be designed and implemented. Some believe that the user of the operating system be given a wide range of privileges to access and operate the EIS’s information asset, but restricted access and operations of the operating system user might be required.
			2. Discussion of OS-Level User
				1. This paragraph describes points to be discussed regarding how privileges of the operating system user (i.e. system manager) are restricted.
* How far is the system manager allowed to operate the information asset owned by an equipment user?
* Is it possible to separate access to the system completely between the system manager and a user? For instance, a system manager may be able to copy or browse files containing a user’s information. Should encryption be applied for security?
* The system manager may have been given the privilege of deleting files. Should access to folders be separated between the system manager and users?
* Backup and restoration of files should be secure.
	+ 1. Authorization
			1. Individual authenticated users (accounts) should be given privileges to access subsets of the equipment information asset and prohibited from accessing subsets of the asset not permitted with the privilege. The equipment information asset includes manufacturing information, equipment design information, and EIS components (i.e. hardware, platforms, and applications.) For example, to use an application the user should be given privilege to use the application. Or to access the process information, the user should be given privilege to access the process information file.
			2. Role-Based Access Control
				1. Assignment of authorization may sometimes be changed to deal with equipment operation scheme changes. Management of assigning authorizations to users creates complicated work for the user. To make management easier, Role-Based Access Control (RBAC) can be applied.



1. Image of Role-Based Access Control
* Role: a group of users (accounts). A member of a role can have the privilege assigned to that role.
* Privilege: definition of authorization to access a subset of the information asset.
* Access Control: access control based on the relation between the role and the privilege.
	+ - 1. RBAC Implementation
				1. For the implementation of RBAC, the following definitions are required:

Definition of role:

* The role should be defined along the operations of the organization.
* In general, roles are defined by the function groups in the organization (e.g. process engineers, equipment maintenance engineers, factory operation managers).
* For the purpose of the troubleshooting, equipment suppliers should be added as a role.
* Definition of role-to-account correspondence:
* Relations between roles and accounts (users) should be defined.
* Definition of privileges:
* Privileges should be defined by subsets of the information asset.
* To define the subset, the asset should be classified and separated.
* Definition of role-to-privilege correspondence:
* Relations between the roles and privileges should be defined.
* Relations may be altered by the situation of equipment operations such as production, process engineering, or maintenance.
* For example, the role of process engineers will be related to the privileges of editing engineering recipes and of running processes in the process engineering phase.
	+ - * 1. Management of the roles, privileges, and their relations must be secured against illegal operations. The procedure of the management of RBAC-related definitions should be permitted only to specially privileged persons.
	1. Network Security for the EIS
		1. Service Restriction
			1. Services through the network should be limited in order to reduce the possibility of getting attacked. Basically, services that have been defined by SEMI standards should be applied to communication between the semiconductor manufacturing equipment operations and the factory. Services that are not used for the equipment operation should be denied. For example, services for remote login, file sharing, or general purpose applications such as Web browsers should be disabled (since they are often the target of attacks). When a new service is going to be introduced, the security of the service should be assessed to assure security.
			2. Equipment Firewall
				1. As a means of limiting services on the network, equipment firewalls may be applied. An equipment firewall is a utility that monitors network activity and blocks unauthorized communications.
		2. HSMS/SECS/GEM Applications
			1. Nearly all semiconductor manufacturing equipment today applies SEMI standards HSMS (SEMI E37), SECS-II (SEMI E5), and GEM (SEMI E30) for communication with MES hosts. Specifications defined by these standards are specialized for the operation of semiconductor manufacturing equipment. For this reason, it may be posited that the communication of messages defined by these standards have less risk of attacks targeted to generic computer systems. However, there are some concerns to be considered.
		3. Risk of HSMS
			1. HSMS has no ability to authenticate entities attempting to access. The system cannot identify the entity behind the host, which poses the following risks:
* Impersonation of the host: If the HSMS on the EIS is configured in the passive connection mode, any host can connect to the equipment.
* Impersonation of the EIS: If the HSMS on the EIS is configured in the active connection mode and the IP address of the host is known, illegal entities can connect to the host.
* Increased risk by intermediate devices: Intermediate devices are often used to interchange SECS messages between the MES and equipment. If the security of the device is not appropriately managed, malicious clients may get the chance to intercept communications.
	+ 1. SECS Message Risks
			1. Some messages defined by the SECS provide the ability to transfer files. For instance, S13F5/F6 downloads “dataset”, or S19F17/F18 transfers “container”. Contents of data items such as “dataset” or “container” are opaque and the possibility of lurking threats in those contents cannot be denied. The entity communicating these data items with the EIS is not necessarily limited to the MES host. Such entities are often used to support efficient equipment operation, for example the equipment operation server. The user should verify the reliability of the security on the entity.
		2. EDA Risks
			1. EDA applies well-known communication technology, the Web Service, as its foundation. Therefore, EDA performs in an environment that can support communication with multiple clients. With that background, EDA has a greater chance of encountering threats compared to HSMS/SECS/GEM communication. For security, the EDA standard has defined its authentication and authorization specifications in SEMI E132.
			2. The risks of EDA are considered to depend upon the risks of the Web Service.
			3. A concern of the EDA operation risk is that semiconductor manufacturing equipment information containing confidential information is communicated on a Web Service intended to be used for public access. Role-Based Access Control should be strictly applied to communication on EDA to protect the system from threats.
			4. Discussion of Security for EDA
				1. The SEMI E132 standard defines authentication and authorization for EDA. The specifications for authorization have been defined based on the idea of role-based access control (RBAC). However, how to use RBAC has not been suggested, and usage has been dependent on individual system design. There may be risk that RBAC for EDA is not applied appropriately, creating vulnerability to illegal access. For secure application of EDA, access control should be implemented with classification and separation of equipment information.
		3. File Transfer Risk
			1. Occasionally, files may be transferred (uploaded or downloaded) by using FTP between the external entity and the EIS. The file transfer may pose the following risks:
* Threats lurking in the downloaded file.
* Disclosing confidential information in the uploaded file.
* Illegal file operations (edit, delete, etc.).
	+ - 1. The EIS should apply access control to limit FTP use. The factory system should manage of the use of FTP, also.
	1. Equipment Control Terminal (ECT) Security
		1. ECT Risks
			1. The risks of the ECT are:
* Read and Copy: information displayed on the ECT includes confidential information. For example, the person facing the ECT may be able to get knowledge of process information such as recipes from the displayed information.
* Edit and Delete: using the editing capability of the ECT, a person may be able to modify or delete information stored on the EIS.
	+ - 1. There are risks of confidentiality, integrity, and the availability of equipment information if the ECT has been illegally operated. Authentication and authorization on the ECT should be provided to implement access control, protecting the system against illegal operation.
		1. Protection of Unattended ECT
			1. To protect the ECT from illegal use, the operator (who has been authenticated and is working on the ECT) should log out soon after finishing his operation. A method of securing the ECT if the operator has left the ECT without logging out is required. The ECT should log users out automatically after a certain time that the ECT has not operated. It could involve a screen-saver with authentication.
		2. Remote ECT Risks
			1. Use of a remote ECT provides a more convenient way to monitor equipment performance or edit recipes. The use of a remote ECT is considered an effective way to operate equipment efficiently, achieving a high-level process. However, it should be noted that there are risks to information security.
* The risk of an improper operator: access to the system by a person without appropriate access permissions.
* Environmental risk: the remote operation environment may allow security infringements. For example, the environment may allow an unauthorized person to observe the operation from behind the operator.
* Risk of malware infection: The ECT is often implemented on a computer system and can be infected by malware. For example, if the ECT has been infected by spyware, authentication information can be learned by the threat.
	+ - 1. The system manager should consider that the use of a remote ECT will increase the risk to information security when implementing security measures.
	1. External Device Port Security
		1. Malware invasions and confidential information leaks tend to happen most easily at external device ports, leading to greater risk in an EIS. However, external device ports are required for equipment maintenance. For example, the use of external device ports is required to support capabilities that maintain equipment performance stability, such as software updates, diagnostic computer connections, and equipment information backups. Despite of this, limiting the use of external device ports is required for the security. The use of the external device ports should be monitored and inspected.
		2. External Device Port Hardening
			1. When the equipment is running for normal functions (other than maintenance purpose), external device ports will be required to be set to no use by applying “hardening”. For “hardening”, measures such as disabling the use of devices on the operating system, or covering the device port physically by a barrier, should be implemented. “Hardening” must be able to be deactivated when the device port is required for use. Procedures for hardening control should be premeditated and applied to the operation.
	2. Hardware Security
		1. Physical Locks
			1. Port Locks
				1. Connectors of ports (network ports, ECT ports, and external device ports) that are not in use should be physically sealed to prevent them from being used. A set of procedures for the sealing and unsealing of ports should be defined and the practice should be monitored and recorded for audits.
			2. EIS Locks
				1. In order to protect the EIS hardware from physical attacks, the EIS hardware should be locked.
			3. EIS Component Locks
				1. Removable components such as storage devices can be pulled out and carried away or returned into the EIS after being modified or infected with malware. To protect the EIS component against these risks, components of the EIS should be locked.
		2. Storage Device Disposal
			1. Storage devices will eventually be disposed of or replaced. Before disposing of a storage device, it is required that measures be taken to ensure that the storage device is not readable in order to protect confidential information. There are various ways to permanently destroy information on the storage device by means of software or hardware.
			2. It should be noted that destroying the information by electro-magnetic means may not be perfect because the memory remains on the magnetic field and can be revived using known technology. Stronger disposal methods such as physical destruction of the hardware or the application of special high-level electro-magnetic tools will be required to secure the confidentiality of the storage device being disposed of.
			3. In the case of transferring used semiconductor manufacturing equipment, security measures should be applied to the storage device.
			4. The defining the disposal procedure, monitoring the practice, and auditing the process are required.
	3. System Update
		1. Software update is required to the equipment information system occasionally in the equipment life-cycle. That includes security related update. Conceivable risks in the software update are malware embedded in the software code, and intrusion exploiting the update process. Assurance that the software has not been infected any malware should be verified before the update. Process of the update should be designed and practiced to make the update secure to prevent intrusion.
		2. Typically the software is updated via network or external device.
		3. Update via Network
			1. Software can be updated via internet from an equipment vendor site, or intranet from a server in the factory. For the update via internet, special permission will be required to go through firewalls. Negotiation with IT owner might be required to get the permission. In the technology, software can be updated via network, but in the security, obstacle is looming.
		4. Update via External Device
			1. External devices are typically well used for the software update of the EIS in practice. Meanwhile, use of external device should be prohibited in daily equipment operation to prevent intrusion. Temporary use of external devices is required to be specially permitted when the software is updated.
			2. Inspection of the update process should be practiced for the security, at the update. For example, supervision should be practiced to the update process to prevent intrusion via human intervention to the update. As well, the device should be inspected before it is used for the software update. For example, a standalone computer system certified for malware detection may be used for the inspection.
	4. Audits
		1. To maintain security and ensure sustainable security performance, periodical audits should be performed. To support this requirement, information for the audit should be recorded by the security system. The information for the audit can be recorded in an electrical format on the EIS or in another format; the information can also be recorded by a person. The information for the audit is confidential information.
		2. Audit information should be managed so as to be provided as soon as possible whenever required by people authorized for the audit.
		3. Point of Audits in the Equipment Life-cycle
			1. Audits should be performed regularly and at the significant points in the equipment life-cycle. There are specific points in the phase of the equipment life-cycle when inspections and audits should be performed, such as development, implementation, operation, maintenance, and disposal.
		4. Malware Protection Audits
			1. The following records may be required for malware protection audits:
* Malware protection software updates
* Operating system patches
* Malware scans
* Malware detection
* Malware incidents
* Emergency responses
	+ 1. Access Control Audits
			1. The following records may be required for access control audits:
* Account settings/modifications
* Authorization settings/modifications
* Operating system log-ins
* Network connections
* External device port use
* ECT operations
* Remote terminal use
	+ 1. Hardware Audits
			1. The following records may be required for hardware audits:
* The EIS lock status
* The EIS component lock status
* Unused port lock status
* Disposed storage devices

**NOTICE:** SEMI makes no warranties or representations as to the suitability of the Standards and Safety Guidelines set forth herein for any particular application. The determination of the suitability of the Standard or Safety Guideline is solely the responsibility of the user. Users are cautioned to refer to manufacturer’s instructions, product labels, product data sheets, and other relevant literature, respecting any materials or equipment mentioned herein. Standards and Safety Guidelines are subject to change without notice.

By publication of this Standard or Safety Guideline, SEMI takes no position respecting the validity of any patent rights or copyrights asserted in connection with any items mentioned in this Standard or Safety Guideline. Users of this Standard or Safety Guideline are expressly advised that determination of any such patent rights or copyrights, and the risk of infringement of such rights are entirely their own responsibility.

1. National Institute of Standards and Technology, 100 Bureau Drive, Stop 3460, Gaithersburg, MD 20899-3460, USA; Telephone: 301.975.6478, <http://www.nist.gov> [↑](#footnote-ref-1)