SEMI E187-0122
SPECIFICATION FOR CYBERSECURITY OF FAB EQUIPMENT

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 October 6, 2021. Available at www.semiviews.org and www.semi.org in January 2022.

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.

1 Purpose

1.1 This Standard defines overarching and fundamental cybersecurity requirements as a baseline to secure semiconductor fab equipment by design and support security protection in operation and maintenance.

1.2 This Standard intends to be applied by entities who provide equipment or services to semiconductor fabrication plants such as equipment suppliers and system integrators.

2 Scope

2.1 This Standard addresses required measures for cybersecurity in the design, operation, and maintenance of semiconductor production equipment and automated material handling system.

2.2 This Standard provides fundamental requirements in the following aspects:

- Operating system (OS) support,
- Network security,
- Endpoint protection, and
- Security monitoring.

2.3 This Standard applies to computing devices of fab equipment, which are installed with Microsoft Windows®[1] or Linux®[2] operating system.

2.4 This Standard does not apply to computing devices of programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), and devices connected to them via sensor-actuator networks.

NOTE 1: Since this Standard is a fundamental standard, supplementary standards can be further developed to provide enhanced requirements to improve security of fab equipment.

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 This Standard does not define any security requirement for factory-provided IT system/servers (e.g., manufacturing execution system [MES]) in the fab.

4 Referenced Standards and Documents

4.1 *SEMI Standards and Safety Guidelines*

SEMI E169 — Guide for Equipment Information System Security

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

[1] Trademark is owned by Microsoft Corporation.

[2] Trademark is owned by Linus Torvalds.

5 Terminology

5.1 *Abbreviations and Acronyms*

5.1.1 *CVSS* — Common Vulnerability Scoring System

5.2 *Definitions*

5.2.1 *access control* — the restriction of access to an information asset via mechanisms used to authenticate and authorize the entity. [SEMI E169]

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. [SEMI E169]

5.2.3 *automated material handling system (AMHS)* — a factory system used to transport and store carriers. AMHS has two major types of components: an automated transport system and one or more storage systems (stockers). [SEMI E98]

5.2.4 *authentication* — verifying the identity of an entity as a prerequisite to allowing access to resources in an information system. [SEMI E169]

5.2.5 *authorization* — the process of granting the privilege to perform a specific action to a user or process.

5.2.6 *computing device* — an electronic device controlled by a central processing unit. It can accept software modifications or execute software to perform an operation.

5.2.7 *endpoint* — a computing device implemented on fab equipment that interacts with external entities via the fab network.

5.2.8 *end of life* — a product at the end of the product lifecycle, indicating that the product is at the end of its useful life (from the vendor's point of view). At this stage, a vendor stops the marketing, selling, or provision of parts, services or software updates for the product.

5.2.9 *end user* — party that uses the production equipment for the purposes of manufacturing semiconductors.

5.2.10 *fab* — a fabrication plant for semiconductor devices.

5.2.11 *fab equipment* — a major manufacturing facility located in the semiconductor fab. It means two types of components in this Standard: semiconductor production equipment and automated material handling system.

5.2.12 *production equipment* — equipment used to manufacture, measure, assemble, or test semiconductor products but not including AMHS.

5.2.13 *privilege* — a right granted to an individual, a program, or a process. [SEMI E169]

5.2.14 *timestamp* — the notation of the date and time of the occurrence of an event. [SEMI E58]

5.2.15 *vulnerability* — a weakness that could be used to endanger or cause harm to an information asset. [SEMI E169]

6 Conventions

6.1 *Requirements Identification*

6.1.1 The following notation specifies the structure of requirement identifiers.

6.1.1.1 The following requirements prefix format is used at the beginning of requirement text. See Table 1 for the format notation of the requirements prefix: [Esss.ss-RQ-nnnnn-nn]

6.1.1.2 To mark the end of the requirement text, the following suffix format is used: [/RQ]

6.1.1.3 Requirements in the body text are highlighted with a light green background (may appear gray in black and white printouts) as shown below.

[Esss.ss-RQ-nnnnn-nn] Requirement text. [/RQ]

Table 1 Requirement Identifiers

Format Notation	*Purpose*
Esss.ss	SEMI Standards Specification identifier. Examples: E87.00, E87.01, E134.00.
RQ	Indicates this is a requirement identifier.
Nnnnn	Unique five-digit number within this Specification.
Nn	Two-digit number that indicates version level of the requirement. A value of .00 is used for the first version of a requirement.
/RQ	Indicates the end of a requirement.

6.1.2 Only text marked with the RequirementID is a requirement of this Specification.

7 Computer Operation System Security Requirement

7.1 *Overview*

7.1.1 The computer operating system of fab equipment usually face challenges from end of life or no update-to-date patch to fix vulnerabilities. Malwares may exploit vulnerabilities to attack the equipment, causing system crash and interrupting operation.

7.2 *Support for Operating System*

[E187.00-RQ-00001-00] Equipment supplier shall not ship equipment with OS that are not supported by the OS vendor (e.g., end of life). [/RQ]

[E187.00-RQ-00002-00] Equipment suppliers shall provide the procedure to apply the patches or the security updates. It includes items to evaluate software compatibility, software package dependency, performance impact, and side-effect of applying the patches or security updates. [/RQ]

8 Network Security Requirement

8.1 *Overview*

8.1.1 There are many different approaches to harden system and its network to reduce the attack surfaces for malware. This can include configuring the system and its network to avoid common pitfalls, turning off unnecessary functionality and ensuring that issues identified by the equipment supplier have been resolved with patches. The end user needs detailed instructions for the installation, configuration and operation of the fab equipment to control and harden the system and its network security.

8.2 *Network Transmission Security*

[E187.00-RQ-00003-00] Equipment that provides applications of web service, file transfer, and terminal service (telnet) shall support secure transmission protocols like HyperText Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) accordingly. [/RQ]

NOTE 2: E187.00-RQ-00003-00 applies to endpoints located in fab equipment and accessible over the fab network.

8.3 *Network Configuration Management*

[E187.00-RQ-00004-00] Equipment supplier shall provide documentation for network configurations including network protocols/ports usage and provide maintenance instructions for changing the network configuration if supported (such as changing the network port assignment). [/RQ]

9 Endpoint Protection Requirement

9.1 *Overview*

9.1.1 Vulnerability assessing is a way to determine if vulnerabilities affect the fab equipment, and malware scanning is commonly used to ensure that the fab equipment is protected from malicious software. Thus, pre-shipment vulnerability scan and malware scan of production equipment provide a proven method to prevent malware intrusion. Meanwhile equipment suppliers can provide end users with the ability to install, manage, or maintain endpoint protection mechanisms that can reduce the risk of malware infection in their operations. Moreover, access control with authentication and authorization is required to prevent invasion attacks and unauthorized use. See SEMI E169 for guidance on authentication and authorization for the information asset.

9.2 *Vulnerability Mitigation*

[E187.00-RQ-00005-00] Equipment suppliers shall perform vulnerability scan prior to equipment shipment and deliver a scanning report, including name and version of scanning tool, scanning scope of coverage, and scanning date, with evidence of no critical severity vulnerability according to common industrial vulnerability scoring standard. [/RQ]

NOTE 3: Regarding to vulnerability scoring, Common Vulnerability Scoring System (CVSS) is an example of a common industrial vulnerability scoring standard for assessing the severity of computer system security vulnerabilities. According to the CVSS score, critical vulnerability is defined as qualitative severity ratings at 9.0-10.0.

9.3 *Malware Scanning*

[E187.00-RQ-00006-00] Equipment suppliers shall perform malware scan prior to equipment shipment and deliver a scanning report, including name and version of scanning tool, scanning scope of coverage, and scanning date. [/RQ]

9.4 *Anti-Malware Protection*

[E187.00-RQ-00007-00] Equipment suppliers shall provide documentation that specifies the compatible anti-malware solutions for the fab equipment. [/RQ]

NOTE 4: Anti-malware is necessary for fab equipment protection to avoid malware attacks. Anti-malware solutions include but are not limited to antivirus software or application allow list control mechanisms.

[E187.00-RQ-00008-00] Equipment suppliers shall provide documents regarding security hardening including:

- Enable/disable input/output interfaces such as Universal Serial Bus (USB) or DVD Rewritable (DVD±RW).
- Disable unused operating system utilities and services.

[/RQ]

9.5 *Access Control Mechanism*

9.5.1 Authentication is a verification process of the authenticity of the entity attempting to access the system. On the other hand, authorization is an access control process for an entity based on access privileges for specific parts of the information asset.

[E187.00-RQ-00009-00] Authentication mechanism(s) shall be used for operating system and equipment access control. [/RQ]

NOTE 5: Authentication mechanism(s) include but not limited to account/password, pin-code or biometric identification.

NOTE 6: Strong authentication such as multi-factor authentication is an optional recommendation for authentication of important accounts. For more information about secure authentication technologies, please refer to Related Information 1, Authentication Technologies.

[E187.00-RQ-00010-00] Equipment suppliers shall provide access rights/privileges authorization solutions to support segregation of duties and least privilege policy. [/RQ]

NOTE 7: Based on least privilege policy, the administrative accounts and privileges should be separated from operator accounts.

10 Security Monitor Requirement

10.1 *Overview*

10.1.1 End users require steady monitoring of vast events of operations on the equipment to find any security problem that causes risks. By providing the logs for security monitoring, faster response to any incident may be expected when it has been happening.

10.2 *Log Requirement*

[E187.00-RQ-00011-00] Fab equipment shall be capable of recording and exporting system and application security event logs. [/RQ]

[E187.00-RQ-00012-00] The types of event logs shall include access control, configuration changes and system errors, and the event log consists of event type, event description, user account and timestamp. [/RQ]

NOTE 8: Additional logs may be made available after alignment between end users and equipment suppliers.

NOTE 9: How long should logs be kept is to conform to the end users site rules.

11 Related Documents

11.1 *IEC® Standards*[3]

IEC 62443-1-1 — Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models

IEC 62443-2-4 — Industrial Communication Networks – Network and System Security – Part 2-4: Security Program Requirements for IACS Service Providers

IEC 62443-3-3 — Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels

[3] International Electrotechnical Commission, 3 rue de Varembé, Case Postale 131, CH-1211 Geneva 20, Switzerland; Telephone: +41.22.919.02.11, Fax: +41.22.919.03.00, http://www.iec.ch. Trademark is owned by International Electrotechnical Commission.

APPENDIX 1
STATEMENT OF COMPLIANCE

NOTICE: The material in this Appendix is an official part of SEMI [designation number] and was approved by full letter ballot procedures on [A&R approval date].

A1-1 Compliance Table: Capability Requirements

[E187.00-RQ-90001-00] Each party of the capabilities defined in this specification shall document compliance to E187.00 capability requirements per with Table A1-1 the following compliance codes: C – comply, NC – not comply, NA – not applicable. [/RQ

[E187.00-RQ-90002-00] The NA compliance code shall be used only in the case where a requirement is conditional and the condition evaluates to render the requirement not applicable for the current implementation. [/RQ]

[E187.00-RQ-90003-00] An explanation for NC shall be provided by the party. [/RQ]

Table A1-1 E187.00 – Capability Requirements

Section	*RequirementID*	*Condition/Selection Criteria*	*Compliance Codes (C/NC/NA)*
A1-1	E187.00-RQ-90001-00	<none>	
A1-1	E187.00-RQ-90002-00	<none>	
A1-1	E187.00-RQ-90003-00	<none>	
7.2	E187.00-RQ-00001-00	<none>	
7.2	E187.00-RQ-00002-00	<none>	
8.2	E187.00-RQ-00003-00	<none>	
8.3	E187.00-RQ-00004-00	<none>	
9.2	E187.00-RQ-00005-00	<none>	
9.3	E187.00-RQ-00006-00	<none>	
9.4	E187.00-RQ-00007-00	<none>	
9.4	E187.00-RQ-00008-00	<none>	
9.5	E187.00-RQ-00009-00	<none>	
9.5	E187.00-RQ-00010-00	<none>	
10.2	E187.00-RQ-00011-00	<none>	
10.2	E187.00-RQ-00012-00	<none>	

RELATED INFORMATION 1
AUTHENTICATION TECHNOLOGIES

NOTICE: This Related Information is not an official part of SEMI E187 and was derived from the work of the global Information & Control Technical Committee. This Related Information was approved for publication by full letter ballot procedures on October 6, 2021.

NOTE 10: During the past few years, people around the world are paying a lot of attention to data security. User authentication technologies are always changing. People need to know that passwords are not the only way to authenticate users. Instead, passwords are regarded as a weak point for a huge percentage of security breaches due to reuse, sharing etc. Although passwords are the most common methods of authentication, newer authentication technologies that are much more secure compared to password-based authentication are being developed. This kind of authentication does not require a memorized secret and usually uses just one highly secure factor to authenticate identity, making it faster and simpler. Some authentication technology examples are listed in this Related Information.

R1-1 Fast Identity Online (FIDO®[4])

R1-1.1 FIDO standard is one example of strong authentication mechanisms, and it is used for authenticating users to online services (by internet or intranet) that do not depend on passwords. That means FIDO can be deployed in factories without internet access or cloud, as a complementary or replacement mechanism for password-based authentication.

R1-1.2 FIDO authentication seeks to use the native security capabilities of the user device to enable strong user authentication and reduce the reliance on passwords.

R1-2 OAuth

R1-2.1 OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. Many companies permit the users to share information about their credentials with third party applications or websites by this mechanism.

R1-2.2 OAuth does not provide native security nor does it guarantee the privacy of data. It relies on the implementers of OAuth and other protocols such as TLS/SSL to protect data exchange.

R1-2.3 OpenID Connect can sit on OAuth as it provides a much stronger authorization mechanism.

[4] Trademark is owned by FIDO Alliance, Inc.