Background Statement for SEMI Draft Document 6506

New Standard: Specification for Cybersecurity of Fab Equipment

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 ballot.

NOTICE: For each Reject Vote, the Voter shall provide text or other supportive material indicating the reason(s) for disapproval (i.e., Negative[s]), referenced to the applicable section(s) and/or paragraph(s), to accompany the vote.

NOTICE: Recipients of this ballot are invited to submit, with their Comments, notification of any relevant patented technology, copyrighted items, or trademarks 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.

Manufacturing automation and control systems operate within a complex environment. In recent years, more new intelligent solutions like full automation, big data analysis and artificial intelligence are adopted in organizations so that lots of Operational Technology (OT) Systems are connected to the network. Organizations are increasingly sharing information between business and industrial automation systems.

The OT Systems typically run critical infrastructure; however, they often run on aging software and obsolete hardware, which makes them difficult to patch and highly vulnerable to exploits by malicious actors. Cyber attacks related to these systems could be devastating to the supply chain of products and services.

The Computer Operating System (OS) of Fab equipment, such as Windows® and Unix-like OSes, usually face challenges from End of Support (EOS) or no update-to-date patch to fix vulnerabilities in software library packages. Malwares can use security exploits to attack the equipment, causing system crash and making operation interruption. Following instances explain the current status corresponding to above challenges of Fab/equipment operation system:

1. In a semiconductor Fab, 20+ versions of OSes have been EOS during 1995~2018. In average, it is expected that 1~2 OS versions will become EOS per year.
2. In semiconductor manufacturing, the production equipment life cycle is 20+ years in general. Making sure the equipment supplier providing complete technical support for security patch is important.
3. According to private survey, in recent 3 years, some delivered Fab equipment still use EOS OSes initially, like Windows XP.
4. In the near future (< 2 years), some OSes may meet the EOS issue, such as Windows 7 and Ubuntu 14.04.
5. Owing to the consideration on compliance issues, such as availability and interruption, making patch adoption is an extremely difficult task for Fab equipment.

These trends have combined to significantly increase organizations' risks associated with the design and operation of their manufacturing automation and control systems. As the threats to businesses increase, so does the need for security. Cybersecurity has become a more significant and widely acknowledged concern. This requires more structured standards to define cybersecurity applicable to computer systems of the Fab equipment. Therefore, we propose to define a standard for software and equipment manufacturers and suppliers to follow to properly manage and solve challenges of cybersecurity to protect the Fab equipment against various threats made by malwares.

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

Review and Adjudication Information

	TF review of the responses to the Letter Ballot	**Letter Ballot Review (including Adjudication) by the TC Chapter**
Group:	Fab and Equipment Information Security Task Force	TW Information & Control Taiwan TC Chapter
Date:	Friday, May 8, 2020	Friday, May 8, 2020
Time & Time zone:	11:00 AM – 13:00 AM Taipei Time	13:30 PM – 15:00 PM Taipei Time
Location:	SEMI Taiwan Office	SEMI Taiwan Office
City, State/Country:	Hsinchu County, Taiwan	Hsinchu County, Taiwan
Leader(s):	Leon Chang (TSMC) Ares Cho (ITRI)	Scott Yu (TSMC)
Standards Staff:	Cher Wu (SEMI) cherwu@semi.org	Cher Wu (SEMI) cherwu@semi.org

SEMI
673 S. Milpitas Blvd.
Milpitas, CA 95035-5446
Phone: 408.943.6900

DRAFT
Document Number: 6506
Date: 2020/3/18

LETTER BALLOT

SEMI Draft Document 6506

New Standard: Specification for Cybersecurity of Fab Equipment

1 Purpose

1.1 The audience for this standard includes system integrators, product suppliers and service providers of computer components of the Fab equipment.

1.2 The purpose of this standard is to define a common, minimum set of requirements to reach progressively more stringent security levels and properly manage and solve cybersecurity challenges to protect the Fab equipment against various threats made by malwares.

1.3 System integrators, product suppliers and service providers will use this standard to evaluate whether their products and services can provide the functional security capability to meet the target security level requirements of manufacturing Fab.

2 Scope

2.1 Cybersecurity which is the particular focus of this specification, includes computers, computer networks, operating systems, applications and other programmable configurable components of the system.

2.2 This standard can be applied to system integrators, product suppliers and service providers of computer components of the Fab equipment.

2.3 This standard defines cybersecurity requirements for Fab equipment development, deployment, operation and maintenance.

2.4 There are a total of four major requirements for computer components of the Fab equipment.

2.4.1 Computer operating system security (e.g., Windows, Unix-like OSes) for the Fab equipment.

2.4.2 Network security (e.g., restricted TCP/UDP ports, avoid using high-risk vulnerable ports, security configuration, user authentication and authorization, vulnerability scanning)

2.4.3 Endpoint protection (e.g., anti-virus, application whitelisting)

2.4.4 Security monitor (e.g., audit logs, protection)

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 only provides commonly required specifications to cover the cybersecurity issues of Fab equipment currently observed by the SEMI Standard committee.

3.2 Threats, risks, and/or security technology continue to evolve over time. Therefore, this standard will 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 E169 — Guide for Equipment Information System Security

4.2 *IEC Standards*[1]

IEC 62443-1-1 — Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models

[1] International Electrotechnical Commission, 3, rue de Varembé, 1st floor, P.O. Box 131, CH - 1211 Geneva 20 – Switzerland. Telephone: +41.22.919.02.11; Fax: +41.22.913.03.00; https://www.iec.ch/index.htm

LETTER BALLOT

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

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

5 Terminology

5.1 *Abbreviations and Acronyms*

5.1.1 *EOS* — End of Support

5.1.2 *OEM* — Original Equipment Manufacturer

5.1.3 *OS* — Operating System

5.1.4 *OT* — Operational Technology

5.2 *Definitions*

5.2.1 *Access* — a means of approaching or touching.

5.2.2 *Access Control* — the restriction of access to an information asset via mechanism used to verify authenticity and authority.

5.2.3 *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.

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

5.2.6 *Authorization* — verifying the access privilege of an entity to ensure authority.

5.2.7 *Endpoint* — a computing device among the Fab equipment that connect to a network and communicates back and forth with the network.

5.2.8 *Endpoint Protection* — a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

5.2.9 *Mainstream Support* — operating system provides security updates for any vulnerability that emerge, adding new features, releasing design changes and warranty claims. It is also called full support.

5.2.10 *Extended Support* — operating system stops adding new features and terminating complimentary support, but OS system still provides vulnerability fixes and patches. It is also called maintenance support.

5.2.11 Privilege — a right granted to an individual, a program, or a process.

5.2.12 *Security Gateway* — relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other.

5.2.13 *Timestamp* — the notation of the date and time of the occurrence of and event.

5.2.14 *Vulnerability* — a weakness that could be used to endanger or cause harm to and information asset.

6 Resource, Organizations, and Standards

6.1 Important resources and organizations used in the generation and definition of this Document are found in:

6.1.1 The operating system provider will commonly offer mainstream/full support for 3-5 years from the date of a product's general availability and 3-5 years extended support/maintenance support from mainstream support end date.

LETTER BALLOT

6.1.1.1 Windows lifecycle policy — https://support.microsoft.com/en-us/help/14085/fixed-lifecycle-policy

6.1.1.2 Red Hat Enterprise Linux Life Cycle — https://access.redhat.com/support/policy/updates/errata/

6.1.2 Commonly accepted anti-malware solution

6.1.2.1 AV-Comparatives — https://www.av-comparatives.org/enterprise/test-results/

6.1.2.2 AV-Test.Org — https://www.av-test.org/en/antivirus/business-users/

6.1.2.3 NSS Labs — https://www.nsslabs.com/tested-technologies/advanced-endpoint-protection/

6.1.3 Commonly accepted system hardening recommendation

6.1.3.1 National Checklist Program Repository (part of the National Vulnerability Database) — https://nvd.nist.gov/ncp/repository?scap

6.1.3.2 National Cyber Security Centre UK — https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?&start=0&rows=20

7 Conventions

7.1 Requirements Identification

7.1.1 The following notation specifies the structure of requirement identifiers.

7.1.1.1 The following requirements prefix format is used at the beginning of requirement text. See 0 for the format notation of the requirements prefix: [Esss.ss-RQ-nnnnn-nn]

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

7.1.1.3 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. 90000–99999 are reserved for use by SEMI.
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.

7.1.2 Only text marked with the RequirementID is a requirement of this specification.

8 Computer Operation System Security Requirement

8.1 Overview

8.1.1 The computer OS of Fab equipment with an expected lifetime of more than 20 years usually face challenges from end of support or no update-to-date patch to fix vulnerabilities in software library packages. The OEM supplier will no longer provide maintenance, troubleshooting or other support. Malwares can use system vulnerabilities to attack the equipment, causing system crash and making operation interruption. As such, the end user requires that the OS in all delivered computers is pre end of support and patched to the most recent level.

8.2 Long-term support for OS

[E<6506> RQ-00001-00] OEM Suppliers shall adopt mainstream support for OS at first production of its Fab equipment to ensure system updates and security patches which are made available for the end user.[/RQ]

LETTER BALLOT

8.3 Alternative countermeasures to address end of extended support

[E<6506> RQ-00002-00] Once Fab equipment OS reaches the end of its extended support, OEM Suppliers shall have alternative countermeasures to mitigate vulnerabilities. Fab equipment shall provide interfaces to connect with firewall, security gateway or alternative security appliances.[/RQ]

8.4 Full documentation with respect to availability of alternative proposal

[E<6506> RQ-00003-00] For system updating, security patching and alternative countermeasures, the equipment supplier shall provide documentation to describe the availability impact and operating procedures. [/RQ]

9 Network Security Requirement

9.1 Overview

9.1.1 There are many different approaches to harden system and its network to reduce the attack surfaces for malware. This can include, but is not limited to, configuring the system and its network to avoid common pitfalls, turn off unnecessary functionality and ensure issues identified by the equipment supplier have been addressed with patches. The end user needs more detailed instructions for the installation, configuration, operation, and termination of the Fab equipment to control and harden the system and its network security.

9.2 Documentation and the control mechanism about equipment configuration management

[E<6506> RQ-00004-00] Equipment supplier shall harden the system and its network with documentation for security control, at least including security policy for installed software, services, network protocols and ports, USB ports. [/RQ]

[E<6506> RQ-00005-00] Equipment supplier shall provide mechanisms to manage hardening options such as enabling of configuration and management of security policy. [/RQ]

9.3 The required policy of identification and authentication management on Fab equipment

[E<6506> RQ-00006-00] For Fab equipment access control, the user authentication and authorization mechanism shall be implemented to verify user identities and to enforce the principles of least privilege. [/RQ]

9.4 Vulnerability scans before shipment to minimize system vulnerabilities

[E<6506> RQ-00007-00] Equipment supplier shall provide vulnerability scanning report to prove no critical or high-risk issues at equipment shipment. The vulnerability scan shall follow commonly accepted security industry practices and recommendations. [/RQ]

10 Endpoint Protection Requirement

10.1 Overview

10.1.1 Malware scanning is commonly used to ensure that the Fab equipment is protected from malicious software. Thus, pre-shipment malware scanning of manufacturing equipment provide a proven method to prevent the transmission of malicious code. Meanwhile the Fab equipment suppliers can provide end users with the ability to install, manage, and maintain endpoint protection software which can reduce the risk of malware infection in their operations. This includes having proper operational configuration, anti-malware software with its latest definition files, and software updates running on all relevant hardware platforms in Fab equipment.

10.2 Virus-Free Evidence

[E<6506> RQ-00008-00] Equipment supplier shall deliver malware-free evidence at equipment shipment. The documentation of evidence shall include information of scanning time, software, scope and version, and the scan method is based on commonly accepted security industry practices and recommendations. [/RQ]

10.3 Certified endpoint protection

[E<6506> RQ-00009-00] Fab equipment shall be compatible with commonly accepted anti-malware solution or application whitelisting control for endpoint protection. [/RQ]

11 Security Monitor Requirement

11.1 Overview

11.1.1 Security monitor can aid in troubleshooting when an issue occurs by providing information about which users were working within the system during the time period. This capability also helps show if there are misconfigurations or other potential threats introduced in the Fab equipment.

11.2 Audit logs integrity

[E<6506> RQ-00010-00] Fab equipment shall have the capability to preserve and export audit logs relevant to security. An audit log includes at least synchronized timestamp, originating device, application/process name, human user account, event type and description. [/RQ]

11.3 Audit logs protection

[E<6506> RQ-00011-00] Fab equipment shall provide protection mechanism to prevent audit logs from tampering or erasing. [/RQ]

LETTER BALLOT

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 Statement of Compliance

[E<6506>-RQ-90001-00] Each implementer of the capabilities defined in this specification shall complete a Capability Requirements compliance table per Table A1-1 when reporting on compliance to E<6506>. [/RQ]

A1-2 Compliance Table: Capability Requirements

[E<6506>-RQ-90002-00] Each implementer of the capabilities defined in this specification shall document compliance to E<6506> capability requirements per with Table A1-1 the following compliance codes: C – comply, NC – not comply, WC – will comply, NA – not applicable. [/RQ]

[E<6506>-RQ-90003-00] 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]

A1-2.1 Child requirements inherit the conditional status of the parent requirement. Where a parent requirement is marked NA, the child requirements should also be marked NA.

[E<6506>-RQ-90004-00] An explanation for NC shall be provided by the implementer. [/RQ]

A1-2.2 If WC is assigned, the implementer should provide a date for implementation.

A1-2.3 Items included in the Condition/Selection Criteria column of Table A1-1 are defined in Table A1-2.

[E<6506>-RQ-90005-00] Each implementer of this specification shall include in the completed capability Requirements compliance table a value as specified in Table A1-2 for all defined conditions or selection criteria included in Table A1-1. [/RQ]

Table A1-1 E<6506>- Capability Requirements

Section	*RequirementID*	*Parent RequirementID*	*Condition/Selection Criteria*	*Compliance Codes (C/NC/WC/NA)*
Capability: A1-1 Statement of Compliance				
A1-1	E<6506>.<BB>-RQ-90001-00	Esss.00-RQ-00002-00	<none>	
A1-2	E<6506>.<BB>-RQ-90002-00	Esss.00-RQ-90001-00	<none>	
A1-2	E<6506>.<BB>-RQ-90003-00	Esss.00-RQ-90002-00	<none>	
A1-2	E<6506>.<BB>-RQ-90004-00	Esss.00-RQ-90002-00	<none>	
A1-2	E<6506>.<BB>-RQ-90005-00	Esss.00-RQ-90002-00	<none>	
A1-3	E<6506>.<BB>-RQ-90006-00	Esss.00-RQ-90002-00	<none>	

Capability: 8 – Computer Operating System				
8.2	E<6506>.<BB>-RQ-00001-00		<none>	
8.3	E<6506>.<BB>-RQ-00002-00		<none>	
8.4	E<6506>.<BB>-RQ-00003-00		<none>	
Capability: 9 - Network Security				
9.2	E<6506>.<BB>-RQ-00004-00		<none>	
9.2	E<6506>.<BB>-RQ-00005-00		<none>	
9.3	E<6506>.<BB>-RQ-00006-00		<none>	
9.4	E<6506>.<BB>-RQ-00007-00		<none>	
Capability: 10 - Endpoint Protection				
10.2	E<6506>.<BB>-RQ-00008-00		<none>	
10.3	E<6506>.<BB>-RQ-00009-00		<none>	
Capability: 11 - Security Monitor				
11.2	E<6506>.<BB>-RQ-00010-00		<none>	
11.3	E<6506>.<BB>-RQ-00011-00		<none>	

A1-3 Compliance Table: Equipment Conditional Criteria

[E<6506>.<BB>-RQ-90006-00] Each implementer shall document E<6506>.<BB>-specific conditional criteria per Table A1-2. [/RQ]

A1-3.1 Conditional criteria are used to identify when conditional requirements are to be implemented.

Table A1-2 Conditional Criteria

Name	*Values*	*Description*	*Section*
<none>		There are no conditional criteria related to the requirements in this specification.	

LETTER BALLOT

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.

<end of ballot>