

SEMI E188-0222

SPECIFICATION FOR MALWARE FREE EQUIPMENT INTEGRATION

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 January 4, 2022. Available at www.semiviews.org and www.semi.org in February 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.

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

1 Purpose

1.1 The nature of semiconductor manufacturing supply chains requires standards for mitigating potential threats. By preventing the introduction of external threats into the manufacturing ecosystem, device manufacturers and equipment suppliers will benefit from clear mutual expectations and improved equipment reliability and uptime.

1.2 This Standard provides a framework for how to mitigate the propagation of malware to manufacturing facilities during capital equipment delivery and support activities.

2 Scope

2.1 This Standard addresses the required measures for information security in manufacturing equipment delivery, installation, and support activities over the course of the manufacturing equipment life cycle within semiconductor manufacturing facilities.

2.2 This Standard defines protection systems and processes that ensure the integrity of manufacturing equipment, specifically defining the requirements for:

- Controlling access to manufacturing equipment via networks, removable media, etc.
- Manufacturing equipment installation
- Manufacturing equipment upgrade and support tasks
- Manufacturing equipment restoration, such as hard disk drives (HDD) or computer component replacement

2.3 This Standard applies to equipment suppliers, equipment users, and hardware and software component suppliers. This Standard applies to any computing device (e.g., computers, controllers, programmable logic controllers [PLCs], etc.).

2.4 This Standard applies to any computing devices and systems located in a manufacturing facility used in the production of semiconductors. This includes process, metrology, and material handling equipment. Computing devices provided by the factory, such as manufacturing execution system (MES), material control system MCS, Host Systems etc., are excluded from this Standard.

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 specify who is responsible for providing the software and applications outlined in this Specification.

3.2 Malware scanning requirements, after equipment installation and acceptance, outside of support activities is beyond the scope of this Standard.

4 Referenced Standards and Documents

4.1 *FIRST® Standards*¹

Common Vulnerability Scoring System^{®1} (CVSS^{®1}) Specification Document

4.2 *NIST® Publications*²

SP 800-126 — The Technical Specification for the Security Content Automation Protocol (SCAP)

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

5 Terminology

5.1 *Abbreviations and Acronyms*

5.1.1 *CVE* — Common Vulnerabilities and Exposures

5.1.2 *CVSS* — Common Vulnerability Scoring System

5.1.3 *FSE* — Field Support Engineer

5.1.4 *NVD* — National Vulnerability Database

5.1.5 *OSI* — Open Systems Interconnection

5.1.6 *PLC* — programmable logic controller

5.1.7 *SCAP* — Security Content Automation Protocol

5.1.8 *XCCDF* — Extensible Configuration Checklist Description Format

5.1.9 *XML* — eXtensible Markup Language

5.2 *Definitions*

5.2.1 *computing device* — a device that can accept software modifications or execute software to perform an operation.

5.2.2 *equipment internal network* — a network that is only used internally by the manufacturing equipment. This network and computing devices on it are not directly accessible by the factory network.

5.2.3 *equipment supplier* — the provider of manufacturing equipment to the equipment user.

5.2.4 *equipment user* — party that uses the manufacturing equipment for the purposes of manufacturing semiconductors.

5.2.5 *external network* — network not under the control of the equipment user (e.g., Public Internet or equipment supplier network).

5.2.6 *factory network* — a network managed by the equipment user for the purposes of manufacturing equipment connectivity.

5.2.7 *field support* — activities performed on the manufacturing equipment after acceptance by the equipment user and includes maintenance related (intended to keep the equipment in good working order), service related (intended to return components that have failed to good working order) and modifications to the manufacturing equipment (e.g., upgrades, configuration changes, etc.).

5.2.8 *host* — the factory host system or an intermediate system that represents the factory and the user to the manufacturing equipment.

5.2.9 *malware* — a comprehensive term to represent malicious software, such as virus or spyware, specifically designed to disrupt or damage a computer system or disclose secret information possibly resulting in tampering of manufacturing equipment.

¹ Forum of Incident Response and Security Teams, 500 Regency Parkway, Cary, NC 27518, USA; <http://www.first.org>. FIRST trademark is owned by First.Org, Inc.

² National Institute of Standards and Technology, 100 Bureau Drive, Stop 3460, Gaithersburg, MD 20899-3460, USA; Telephone: +1.301.975.6478, <http://www.nist.gov>. NIST trademark is owned by National Institute of Standards and Technology.

5.2.10 *malware free* — the scanned computing device or storage device does not have any malware detected, based on the malware scanning software and definition/pattern files used at the time of the scan.

5.2.11 *manufacturing equipment* — the combination of hardware and software required to perform an operation or activity (e.g., processing, transporting, storing), including all direct auxiliary support or peripheral equipment (e.g., vacuum pumps, heat exchangers, effluent/exhaust treatment equipment).

5.2.11.1 *Discussion* — This definition includes computing devices not physically near the manufacturing equipment. For example, it includes automated material handling systems (AMHS) and group controllers (hardware and software that control multiple manufacturing equipment on a factory floor); the respective equipment suppliers are responsible for complying with this Standard for these computing devices.

5.2.12 *storage device* — a device that contains data and information that a computing device can access.

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

5.2.14 *threats* — anything that has the potential to cause harm to data on the manufacturing equipment or its intended behavior.

5.2.15 *vulnerability* — a weakness that could be used to endanger or cause harm to data on the manufacturing equipment.

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. Refer to 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 border and 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

<i>Format Notation</i>	<i>Purpose</i>
Esss.ss	SEMI Standards Standard identifier. Examples: E87.00, E87.01, E134.00.
RQ	Indicates this is a requirement identifier.
Nnnnn	Unique five-digit number within this Standard. 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.

6.1.1.4 Note that the requirements in Appendix 1 use the reserved requirement numbers noted in Table 1 because they are repeated in other SEMI Standards that use this convention.

6.1.2 Requirements in tables are delimited in one of two ways.

6.1.2.1 Where the requirement occupies an entire row in the table, the requirement identifier (RequirementID) is placed in column 1. No ‘[/RQ]’ is used to mark the end of the requirements text in this case. The table may also contain rows that are not requirements. In this case, the column 1 cell is left blank.

6.1.2.2 Non-requirements text related to a requirement row may be included in an adjacent row. The relationship between the rows is indicated by a broken line separating the two.

6.1.2.3 Where the requirement occupies only one cell, the text in the cell includes the RequirementID prefix and suffix similar to requirements in the body text.

6.1.2.4 No cell in a table will contain both requirement and non-requirement text.

6.1.2.5 Cells that contain requirements are shaded light green.

6.1.2.6 Table 2 provides an example of requirements in a table. Note that in this example, the same requirement is presented in two alternative formats. In practice, mixing the two approaches in the same table is not typically done.

Table 2 Example Table with Requirements

<i>RequirementID</i>	<i>Statement</i>	<i>Additional Detail</i>
Esss.ss-RQ-nnnnnn-nn	The light shall be the sole blue light.	There shall be no similar color in the light panel.
	The blue light is typically placed at the leftmost position in the light panel.	
	[Esss.ss-RQ-nnnnnn-nn] The light shall be the sole blue light. There shall be no similar color in the light panel. [/RQ]	The blue light is typically placed at the leftmost position in the light panel.

6.1.3 Only text marked with the RequirementID is a requirement of this Standard.

6.1.3.1 Clarifications, examples, and related recommendations may be provided near a requirement, but are not part of the requirement.

6.1.3.2 Note that the word ‘should’ is used in some non-requirements text, where it denotes a recommendation or a best practice, not a requirement.

6.1.3.3 Note that the words ‘must’ and ‘will’ are used in the Implementation Overview section to illustrate the logical result of requirements specified in the prerequisites and requirements section. Such statements should not be considered requirements.

6.1.4 Parent-child relationships of requirements are noted in Appendix 1, Table A1-1. Where a parent requirement includes conditions or selection criteria, these are passed to their children. For example, if a parent requirement is stated to apply only to photolithography equipment, any child requirements also apply only to such equipment. The condition need not be restated for each child requirement.

6.1.4.1 Compliance to a parent requirement includes compliance to all of its child requirements.

6.1.4.2 Some cells or rows in a table may contain headings that are assigned a RequirementID. These are parent requirements for other requirements in the table—typically for the rows that immediately follow that heading.

7 Overview

7.1 This Standard aims to prevent equipment suppliers from introducing or spreading malware in the factory network. It refers equipment suppliers to respected third party organizations for information about existing vulnerabilities and best known practices on hardening systems which they can use to evaluate against their manufacturing equipment.

7.2 This Standard does not target any one specific operating system, software, or networking component, but instead provides an infrastructure and process that can be applied to any computing device within the manufacturing equipment. Figure 1 illustrates how different components, network layout and terminology used in this Standard relate to each other.

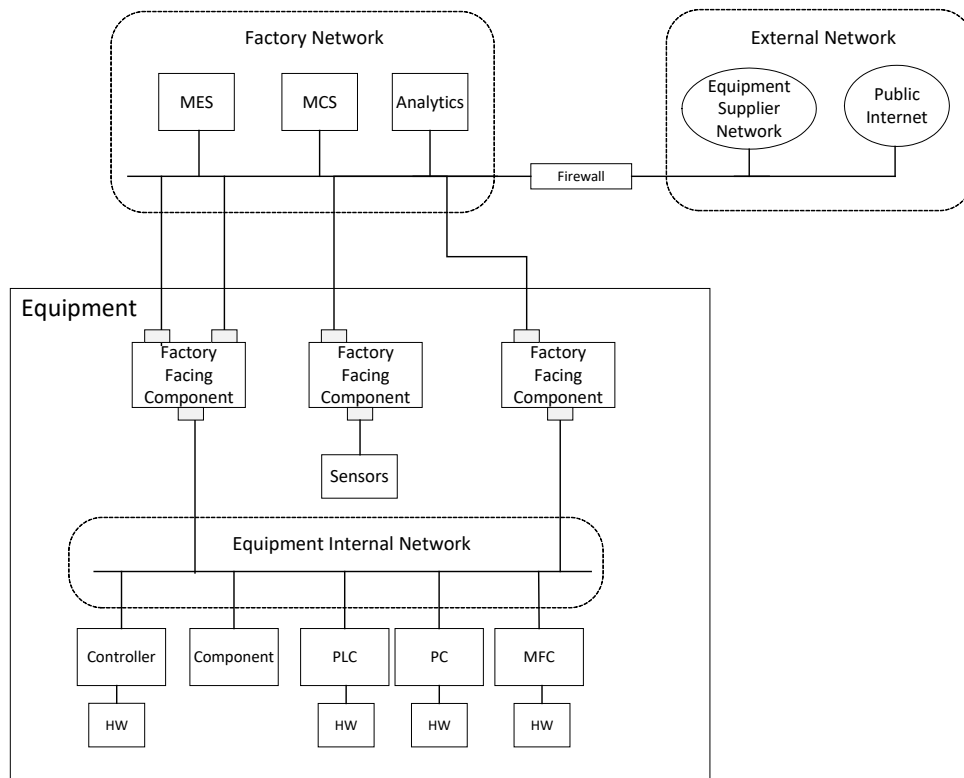


Figure 1
Network Architecture

7.3 In the context of this Standard, ‘malware free’ means the scanned computing device or storage device does not have any malware detected, based on the malware scanning software and definition/pattern files used at the time of the scan. It is possible there is malware on the device that could not be detected at the time of the scan, based on the technology used. It is important to adopt regular malware scanning practices to detect new malware, using updated technology (malware scanning software and definition/pattern files).

7.4 This Standard has several requirements that refer to providing information to the equipment user or to the equipment supplier. For example, malware scan results, SCAP scan results, vulnerability assessments, etc. The equipment user and equipment supplier should agree on which specific equipment user representative or department should receive this information and the delivery method (e.g., some information may be emailed to the account representative, and some information may be uploaded to the security department’s portal). These agreements are outside the scope of this Standard.

7.5 Some equipment suppliers may have computing devices that live in the equipment user’s data centers, rather than be physically located on the factory floor. In these situations, the equipment user’s native IT policies have priority. For example, an analytics server provided by the equipment supplier has access to the factory network but runs on server hardware provided by the equipment user in their server farm. The equipment suppliers’ Field Support Engineers (FSE) do not have access to the server, so requirements related to SCAP scanning are not applicable. The equipment supplier is still responsible for performing malware scans on any software updates and patches to be applied to the analytics server.

NOTE 1: Support contracts between the equipment supplier and equipment user outline what the equipment supplier is responsible for. These agreements are outside the scope of this Standard.

7.6 The equipment supplier is accountable that the manufacturing equipment they provide complies to this Standard.

7.6.1 The equipment suppliers provide a list of components, software applications and operating system services that are delivered and supported as part of the manufacturing equipment. Figure 1 details provides an example of some

common components and possible network architecture. This list is used to determine what items the equipment supplier is responsible for configuring and monitoring for newly discovered vulnerabilities (refer to § 9).

NOTE 2: If the equipment user installs additional software on the manufacturing equipment (e.g., remote access software), the equipment supplier is not responsible to monitor that software for new vulnerabilities unless it is agreed to by both the equipment user and equipment supplier. This is outside the scope of this Standard.

7.6.2 An equipment supplier is accountable to ensure the components they provide comply with this Standard. The equipment supplier may maintain a list of approved suppliers they use. Components provided by these approved suppliers also need to comply with this Standard. Figure 2 illustrates some common scenarios.

NOTE 3: Specific areas of responsibilities can be negotiated between the equipment supplier and their suppliers and is outside the scope of this Standard.

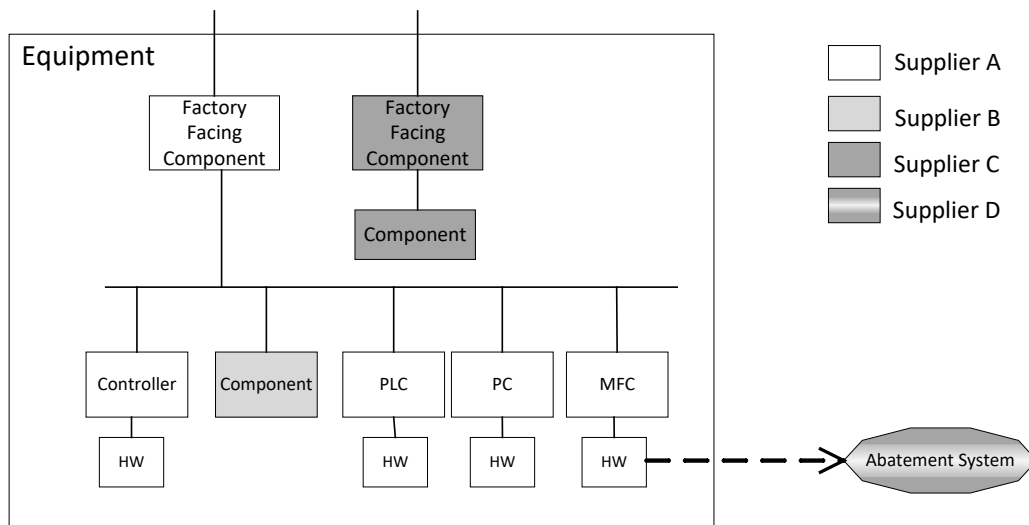


Figure 2
Equipment Supplier Ownership

7.6.3 If Equipment Supplier A's equipment connects to a component from another supplier (e.g., the factory's abatement system), Equipment Supplier A is not accountable for those components complying with this Standard.

7.6.4 Sometimes, an equipment supplier may include components in their equipment that they did not provide. For example, Equipment Supplier A includes a computing device provided by Equipment Supplier B at the equipment user's direction, and Equipment Supplier B looks after maintaining and servicing that computing device. For the purpose of this Standard, the entity who has the support agreement with the equipment user for the component is accountable to ensure that component's compliance to this Standard.

NOTE 4: Specific areas of responsibilities will be outlined as part of agreements between the equipment suppliers and equipment user and is outside the scope of this Standard.

7.6.5 Occasionally, additional components may be installed after the equipment is installed and accepted by the equipment user. If the equipment user directs that components will be provided and maintained by another entity, the equipment supplier is not accountable for their compliance to this Standard. For example, additional sensors from Equipment Supplier C are connected to the manufacturing equipment and information is sent to the factory on a separate connection from the equipment. Equipment Supplier C is accountable to ensure their components comply with this Standard.

7.6.6 Sometimes an equipment supplier may contract the integration or field support of their manufacturing equipment to another third-party entity. The equipment supplier is still accountable for ensuring compliance to this Standard by the third party. For example, any computing device or storage device used by the third party for field support work are properly scanned per § 10.

NOTE 5: A different agreement may be approved by the equipment user, equipment supplier and third party to transfer accountability for some of this Standard's requirements to the third party. These agreements are outside the scope of this Standard.

7.7 This Standard defines a minimum set of requirements. The equipment user may have their own policies and procedures that are more comprehensive than what is required in this Standard. The equipment user and equipment supplier may agree that parts of this Standard do not need to be performed because the equipment user's policies make them redundant. For example, if the equipment user requires a FSE's laptop to be scanned for malware onsite before it can be brought onto the property, they may allow the FSE to skip the requirement in this Standard that the FSE has to run a malware scan on the laptop before entering the factory (refer to § 10).

NOTE 6: Such exceptions are negotiated between the equipment user and equipment supplier and are outside the scope of this Standard.

8 Manufacturing Equipment Malware Scanning

8.1 Overview

8.1.1 Malware scanning is common practice to mitigate threats posed by malicious software. As such, pre-shipment malware scanning of equipment provides a proven method to prevent the transmission of malicious code.

NOTE 7: To be most effective, the pre-shipment scanning should be executed just prior to powering down the manufacturing equipment to minimize the chance of new malware being introduced.

8.2 Malware Scanning Software

8.2.1 There are many malware scanning software available. Some are free and some are commercial applications. This Standard refers to external organizations to evaluate malware scanning software to determine if they provide an acceptable level of protection. This Standard does not maintain a list of approved malware scanning software providers (which can change over time).

NOTE 8: Unless otherwise specified, the organizations listed in Table 3 only list malware scanning software that meet their approval criteria.

Table 3 Malware Scanning Software Evaluation Organizations

Organization	URL ^{#1}	Acceptable Malware Scanning Software
AV-Comparatives	https://www.av-comparatives.org/enterprise/test-results/	List of malware scanning software under the "Enterprise Area"
AV-Test.Org	https://www.av-test.org/en/antivirus/business-users/	List of malware scanning software under the "Security for Business Users"

#1 URLs are provided as a convenience to help readers find the appropriate section of the organization's website.

8.3 Malware Scanning

8.3.1 As part of the ensuring the equipment is installed malware free, the equipment supplier checks the manufacturing equipment before it is shipped to the equipment user.

[E188.00-RQ-00001-00] The equipment supplier shall conduct a pre-shipment malware scan of any manufacturing equipment provided to an equipment user to ensure it is malware free. The malware scan satisfies the minimum conditions outlined in Table 4. [/RQ]

Table 4 Minimum Malware Scanning Conditions

	<i>Subject</i>	<i>Acceptable Condition</i>	<i>Additional Information</i>
A	Malware scanning software evaluation	The latest evaluation was performed within the past 365 days by one of the organizations described in Table 3. ^{#1} The latest evaluation deemed the software as being reputable	
B	Malware scanning software update check	An update check was performed, for malware scanning software updates and updated definition/pattern files, within the past 5 days from the validation scan date.	
C	Scanning engine and definition/pattern file versions	The scanning engine and definition/pattern files are the most recent, or released within the past 5 days from the validation scan date.	
D	Scanning engine configuration	The scanning engine is configured to scan and remove malware from all files (including compressed and non-executable), system memory, and boot partitions.	
E	Scanning coverage	The malware scanning software performs malware scans of: • every computing device capable of executing malware scanning software • every storage device in the computing device. EXCEPTION: If there is a computing device or storage device on the equipment internal network that cannot execute the scanning software, malware scanning software running on a different computing device needs to scan that device.	The malware scanning software checks for persistent and non-persistent malware executing on the computing device.

#1 Equipment users may choose to allow equipment suppliers to use malware scanning software that are not on any lists recommended by these evaluation organizations. Such agreements between the equipment user and equipment supplier are outside the scope of this Standard.

8.4 Malware Scanning Reporting

8.4.1 The equipment user can review pre-shipment scan results to ensure the equipment is being sent to them malware free.

[E188.00-RQ-00002-00] The equipment supplier shall provide a report in electronic format to the equipment user detailing the configuration and results of the pre-shipment scan. At a minimum, the report provides the information listed in Table 5. [/RQ]

Table 5 Malware Scan Report Contents

	<i>Report Information</i>
1	Scanning software name
2	Scanning engine revision
3	Definition file revision
4	Execution time and date
5	Number of files scanned
6	Number of files not scanned
7	Number of threats detected

8.4.2 Some files on a computing device or storage device cannot be scanned by malware scanning software (e.g., the file is a password protected file the scanning software cannot open).

[E188.00-RQ-00003-00] The equipment supplier shall provide documentation assuring no malware is present in the unscanned files. [/RQ]

8.4.3 There are some components where there are no malware scanning software available that can scan them (e.g., dedicated real-time systems such as PLCs).

[E188.00-RQ-00004-00] If there are no public or commercial malware scanning software available for a computing device or storage device in the manufacturing equipment, the equipment supplier shall provide a method to demonstrate the computing device or storage device is malware free. [/RQ]

NOTE 9: The equipment supplier may propose an alternative method of demonstrating a computing device is malware free. Agreement on alternative reporting methods should be agreed to prior to shipment.

8.4.4 Table 6 can be used to report the list of computing devices and storage devices that malware scanning software cannot scan, and proposed alternatives to demonstrate the computing device or storage device is malware free.

Table 6 Alternative Malware Scanning Report Contents

<i>Computing Device/ Storage Device</i>	<i>Operating System</i>	<i>Proposed Alternative for Malware Scanning Software</i>

8.5 Malware Scanning Prior to Connecting to the Factory Network

8.5.1 Malware is constantly evolving, and malware scanning software and definition files are updated.

8.5.2 Equipment suppliers and/or equipment users should perform a check with an updated definition/pattern files before the manufacturing equipment is connected to the factory network. This is to guard against the follow situations:

- Malware is introduced to a computing device or storage device in the manufacturing equipment between the time when the pre-shipment scan is performed and when the computing device is powered down.
- New malware is discovered between the time when the pre-shipment scan is performed and the manufacturing equipment is assembled at the equipment user's factory floor and connected to the factory network.

8.6 Post Installation Malware Scanning

8.6.1 After manufacturing equipment installation and qualification, on-going malware scanning of the manufacturing equipment should be performed. This is outside the scope of this Standard and should be agreed between both equipment supplier and equipment user.

9 Computer System Hardening

9.1 Overview

9.1.1 There are many different approaches to 'harden' a system to reduce the attack surfaces for malware. This can include, but is not limited to, configuring the system to avoid common pitfalls, turn off unnecessary functionality and ensure issues identified by the supplier have been addressed with patches.

9.1.2 Rather than trying to define such approaches in this Standard (as they are constantly evolving as new malware and vulnerabilities are detected), this Standard will refer to respected external sources.

9.1.3 As well, vulnerabilities are continuously being discovered in software and systems after it has been released (operating systems, drivers, libraries, applications, etc.). It is important that they are assessed to see if they are applicable on the manufacturing equipment running on the factory floor and expose the equipment user to risk.