SEMI PUBLISHES FIRST CYBERSECURITY STANDARDS

By James Amano, Senior Director, International Standards, EHS & Sustainability, SEMI

In recent years cyberattacks on companies have proliferated, and the semiconductor industry has not been immune. In 2018, for example, a major foundry was forced to pause production to investigate machines infected by ransomware in 2018. To help protect against future cyberattacks on factory equipment, SEMI launched two major Standards Program initiatives and, following a major industrywide effort, I am pleased to announce the publication of two new standards:

SEMI E187 - Specification for Cybersecurity of Fab Equipment

SEMI E188 - Specification for Malware Free Equipment Integration

SEMI E187: Specification for Cybersecurity of Fab Equipment

The Fab and Equipment Information Security Task Force, led by Leon Chang (TSMC) and Ares Cho (ITRI), developed E187, which defines a common, minimum set of security requirements for fab equipment that will serve as a security baseline for fab

equipment. The requirements will focus on four major components of fab equipment: operating systems, network security, endpoint protection, and security monitoring. Over time the requirements will evolve to meet new malware threats.

"TSMC took the lead in promoting the *E187: Specification for Cybersecurity of Fab Equipment*, to raise overall supply chain security, build supply chain resilience through cybersecurity, and achieve corporate social responsibility with suppliers," said Dr. James Tu, Head of Corporate Information Security at TSMC.

SEMI E188: Specification for Malware Free Equipment Integration

Led by Ryan Bond of Intel and Richard Howard of Cimetrix, the Fab & Equipment Computer and Device Security ask Force developed SEMI E188, which focuses on protecting against factory equipment malware attacks during initial integration, field service repairs, patching and maintenance. This new Standard defines requirements for equipment, computing devices, and systems brought in by suppliers to operate on the manufacturing facility's factory network, setting out security safeguards and reporting for implementation across different types of equipment entering the manufacturing facility. In particular, SEMI E188 will:

- Define minimum malware scanning requirements to ensure suppliers scan equipment, and devices used in maintenance and support operations for

malware before shipment in preparation for delivery. Malware scanning is a proven way to protect against malicious code.

- Refer to trusted external sources for approaches to *harden* a system in order to reduce the malware attack surface and to identify and report vulnerabilities. This includes the Security Content Automation Protocol (SCAP) and the National Vulnerability Database (NVD) - Common Vulnerability Scoring System (CVSS) provided by National Institute of Standards and Technology (NIST).
- Specify configuration documentation for users to prevent equipment from introducing insecure network configurations to factory networks.

Many manufacturing facilities already implement their own network and security policies for databases and servers that are connected to the production floor. SEMI E188 offers additional layers of security for equipment and devices provided by suppliers for operation on the factory network.

“As demand for semiconductor products increases, it is critical to protect manufacturing equipment from cybersecurity threats,” said Task Force leader Ryan Bond of Intel. “This standard improves overall equipment security while providing a shared set of expectations between device makers and equipment manufacturers.”

Moving Forward

The first of a planned series, these new SEMI Cybersecurity Standards support the advancement of the *connected fab* by creating a robust secure data exchange infrastructure that meets the security needs of manufacturing environments that rely on big data and artificial intelligence, The next step for the semiconductor manufacturing industry will be to develop a *Specification for Application Accesslisting* to outline how accesslisting applications should protect equipment and systems. These implementations can be tailored to the security management plans of individual equipment users or fabs. The Fab & Equipment Computer Device Security (CDS) Task Force invites industry members experienced in using application accesslisting to contribute to the development of this new SEMI standard.

The growing number of direct data exchanges are essential for Smart Manufacturing within and beyond the factory. Industry stakeholders will leverage the common set of definitions, procedures, and best practices established by these Standards to define new security targets and protect these exchanges.

The publication of these security standards is a major milestone in a global collaboration among industry stakeholders working within the SEMI Standards Program. Security

standards will help protect factory equipment against malware attacks while enabling the data-driven technologies needed for Smart Manufacturing.

SEMI Standards meetings are held throughout the year in all major manufacturing regions. For information on how to become involved, contact your local Standards staff or visit the SEMI Standards web site.

Standards Watch

SEMI

www.semi.org

March 7, 2022