txOne networks

SEMI E187 : What You Need to Know

Keep the Operation Running.
Keep Assets Working.

Semiconductor manufacturers struggle with long equipment life cycles, patch deployment, and meeting strict requirements for availability and performance, which they must balance against cybersecurity concerns.

Long equipment life cycle

In semiconductor manufacturing, the life cycle of production equipment generally spans more than 20 years. Typically, more than 20 versions of operating systems exist within a Fab, and one or two of these will face End-of-life (EOL) issues each year.

Difficulty deploying patches

Asset owners in a semiconductor Fab must carefully take compliance issues into account to ensure the continuation of production processes, high availability, and forestallment of disruptions to production.

Security monitoring

Continuous security monitoring and auditing are becoming more and more important, but much of the equipment still lack the standard interfaces required to collect security-related logs.

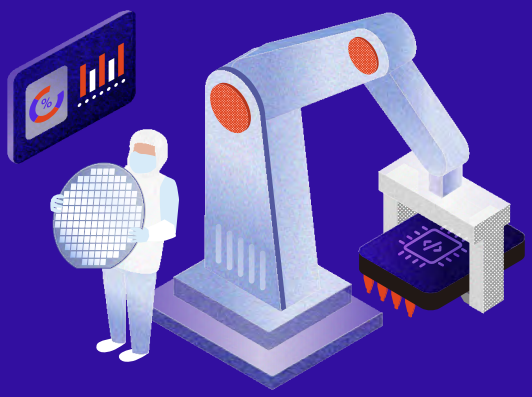
By using SEMI E187 to define baseline cybersecurity requirements, technicians stop malware from spreading to the factory both during initial equipment onboarding and throughout ongoing production activities including field service repairs, software patching, and maintenance. SEMI E187 explicitly focuses on improving the defenses for operating systems, networks, and endpoints to better facilitate semiconductor manufacturers' cybersecurity management.

Four essential ways a Fab can be improved when it comes to computer operating systems, network security, endpoint protection, and security monitoring are discussed below :

- ☑ Stop the delivery of equipment with an end-of-life (EOL) operating system and provide documentation illustrating how to perform security updates when equipment faces End-of-Life issues.
- ☑ Support secure transmission network protocols and provide a method to disable unnecessary network ports and protocols for Fab equipment.
- ☑ Provide vulnerability and malware scan reports before each shipment.
- ☑ Support recording security event logs to optimize troubleshooting for asset owners.

txOne networks

Semiconductor Cybersecurity with OT Zero Trust



Achieving OT Zero Trust Through the Asset Security Life Cycle

The goal of the OT zero trust approach is to eliminate all threats, whether they originate from inside or outside the network. The central principle is that it is not safe to trust anything inside or outside the OT environment – including stakeholders, the network, or assets – without first conducting identification and classification. Many global leaders in semiconductors use the asset life cycle architecture together with OT zero trust to plan and deploy cyber defenses for semiconductor work sites. They've found OT zero trust to be an effective as a strategy for mediating and adding defensive underpinnings to the asset planning phase, where improving long- and short-term cyber defensive outcomes is critical.

01 Onboarding

Before an asset is shipped to a foundry, suppliers should scan each asset with Trend Micro Portable Security 3 Pro™ to create a record of OT health that proves the equipment is malware-free. In the past, attackers have launched large-scale attacks and exploited the supply chain by compromising assets prior to shipment. Similar to going through each country's customs on either side of an international flight, both the supplier and the asset owner must keep a record as they independently confirm device safety and security for themselves on their own side of the transaction.

02 Staging

During the staging phase, prepare assets by patching vulnerabilities and shutting down non-essential services such as system applications, permissions, ports, and user accounts. For fixed-use and legacy endpoints, Stellar™ deploys trust lists that only allow applications related to the endpoint's job. For modernized endpoints that carry out various and complex tasks, Stellar™ has a library of trusted ICS applications and licenses that shows next-generation antivirus software which files and applications should be denied and or given priority, preserving resources for operations. Manage locked down legacy and modernized assets from one centralized console through Stellar.

03 Production

Network segmentation is an advanced OT zero trust-based methodology whereby different assets on the operational network are split into productivity-based groups. As the asset enters the production phase, network security must be secured to guarantee operational integrity. Assets are grouped into segments before specialized policies are applied based on their work needs. Virtual patching shores up vulnerabilities in legacy and otherwise unpatchable assets so that they cannot be exploited by attackers. All network appliances and policies can be easily observed and maintained through a single, centralized console (OT Defense Console™).

04 Maintenance

From the moment an asset is put into its intended production use, it begins to age and depreciate, and regular maintenance begins. Not only repairs, but also ongoing software configuration changes, system upgrades, and security updates. Locked down assets are routinely checked for malware by Stellar™ lockdown software, while stand-alone and air-gapped assets are scanned with Trend Micro Portable Security 3 Pro™, which generates detailed information of all scanned assets including IP address, MAC address, host name, OS version, patch list, and installed application list for. This creates a neatly-updated OT asset inventory to streamline the identification of vulnerabilities and other cyber risks.