Solution Brief

OT Network Security

TXOne Networks Secures Semiconductor Manufacturing OT With CASwell Network Security Appliances

Semiconductor fabs are complex operations with many steps that need data security. TXOne Networks addresses the challenge with its EdgeIPS™ Pro OT security software running on CASwell network security appliances based on Intel® processors.

Providing network security in operational technology (OT) environments is an urgent requirement for organizations that are embracing digital transformations in their production lines. In the OT environment, a breach can mean a shutdown of production lines or physical damage such as leakage of fuel or other liquids and even explosions. This disrupts not only the organization's financial health and reputation but the surrounding economy and industry as a whole, significantly affecting many.

According to figures from McKinsey & Company[1] there were 64 reported OT cyber-attacks in 2021 with 35% of these involving physical consequences and estimated per incident damages of $140 million. The consulting firm said a 72 percent increase in attacks took place in 2022.

In its "Insights Into ICS/OT Cybersecurity 2022" report TXOne Networks breaks down three main developments in OT cybersecurity, including:

- The expansion of the threat landscape due to IT/OT convergence and ransomware-as-a-service and other new forms of attacks.
- Increased regulations designed to protect instituted in response to huge cyberattacks.
- A new emphasis on OT cybersecurity by large organization combined with a movement towards OT-specific solutions rather than relying on IT-focused solutions.

The OT environment has such diversity of operating systems and tools that using IT-oriented end-point protection solutions alone are not effective. Even foundational security activities such as server and network patching are a challenge in OT environments. Many OT vendors are lacking or just now introducing security by design capabilities. And finally, thanks to IoT and Industry 4.0 initiatives, modern wireless and wireline networks are converging on the OT network.

Semiconductor fabrication facilities are no exception to such vulnerabilities and increasingly so as they require the most complex and precise operational processes. The complex chain of activities that takes an EDA design and turns it into an integrated circuit involves supply chain processes, business processes, and customer processes – all before the design even gets to the foundry (see Figure 1). A malware or advanced persistent threat (APT) attack at any of the steps could cause tens to hundreds of millions of dollars in damages. To protect against an attack, every link in the process must be sequentially reinforced and protected.

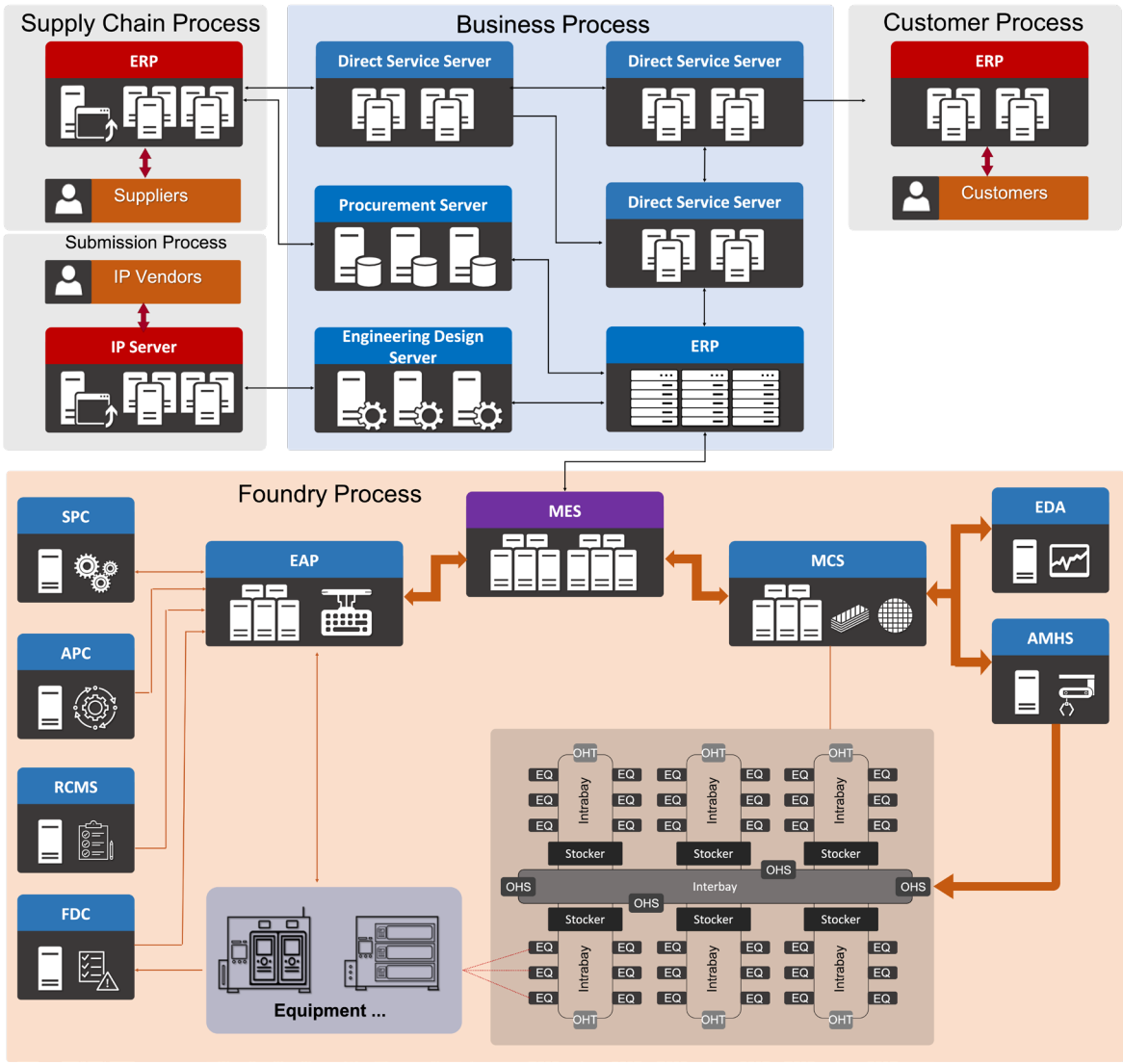

Figure 1. Fab production processes that need protection from cyber security threats.

In this environment network-based security is implemented to address the diversity of tools used to construct the operations. This diversity makes it difficult to secure and manage each asset. It's also important to protect the assets from inside threats either from malicious attacks or from inadvertent misconfigurations and behaviors. An important technology for network-based security is intent-based network segmentation which provides a different network segment for each asset in order to localize an attack, thus minimizing the impact from an attack.

TXOne Networks is a member of Intel® Network Builders program and has developed its EdgeIPS™ Pro family of OT security systems that use OT-optimized servers that are powered by Intel Atom® processors and 3rd Gen Intel® Xeon® Scalable processors. While the focus of this paper is on semiconductor fabrication applications, these systems can be used for OT security systems in a wide range of applications. TXOne Networks chose these processor platforms because they advance the company's commitment to constant performance optimization as a key competitive differentiator.

"The TXOne Edge suite of solutions draws upon Intel's advanced technologies as the foundational hardware elements. This strategic reliance on Intel's cutting-edge technology substantiates our commitment to fortifying industrial processes and critical infrastructural frameworks. By furnishing proactive safeguarding measures for operational technology assets and preemptively eradicating malevolent interventions during pivotal production phases, our suite stands as a bulwark of reliability, safety, and continuity," said Dr. Terence Liu, TXOne Networks Chief Executive Officer.

"CASwell is honored to partner with TXOne Networks to provide a comprehensive OT security solution based on Intel's state-of-the-art high performance network security platform. This collaboration not only enhances the reliability and resilience of semiconductor fabrication facilities, but also facilitates the OT cyber security protection in a new era," said Reaforl Hong, President of CASwell.

"High stakes manufacturing businesses, including semiconductor fab operations, are facing significant cyber security threats every moment of the day, 24 by 7," said Bob Ghaffari, VP of Network Edge Group and GM Enterprise Cloud Network Division at Intel Corporation. "Solutions from TXOne Networks and CASwell are great examples of cyber security systems built on an Intel technology foundation that deliver high-performance real-time security mitigations for organizations with complex and geographically dispersed edge OT requirements."

TXOne's OT Security Products for Semiconductor Fabs

TXOne EdgeIPS™ Pro is a family of purpose-built OT security appliances, available for DIN or rack mounted deployment and equipped with features to enable administrators to easily manage micro-segmentation in a complex environment.

EdgeIPS™ Pro OT security appliances offer protection from internal and external attacks and provide security managers with visibility into OT systems. Each appliance offers multiple ports (from eight to 96) for connecting network segments. Each of these ports offer the full range of security features becoming an integrated multi-port security system offering specific security policies and unified management and monitoring for a specific production asset.

The architecture of the EdgeIPS™ Pro security systems offers three foundational features that define the advantage that the EdgeIPS™ Pro products bring to semiconductor fabrication and other OT environments. These are:

Intent-based Network Segmentation: The security foundation of the EdgeIPS™ Pro is its support for intent-based network segmentation providing individual, secured connections to each of the industrial assets on the network. This functionality leverages multi-port network interfaces on the server that can each support a network segment and offer the full feature set for each segment.

Virtual Patching Provides a "Shield" of Security: The EdgeIPS™ Pro appliance can protect legacy systems, unpatched devices and other assets from network vulnerabilities using its virtual patching capability which watches data flows on the network for malicious attack signatures. The virtual patch acts as a network-based "shield bubble" that protects the device by ensuring the validity and security of traffic going in and out of the device and alerting the security operations center (SOC) to any abnormality.

Deep Packet Inspection for Operational Intelligence

The EdgeIPS™ Pro utilizes the TXOne One-Pass DPI for Industry (TXODI™) for very fast deep packet inspection (DPI) that inspects layer 2 to layer 7 to provide operational intelligence. This foundational capability provides the ability for the intrusion protection system (IPS) to inspect all the data in a flow and detect malicious attacks in real time.

Other features include:

- Reduced administrator workload through the Auto Rules Generation feature that uses machine learning to facilitate auto-learning of network connections and generation of allowlists.
- Support for an extensive list of industrial network protocols including Modbus, Ethernet/IP, CIP, FINS, S7Comm, S7Comm+, SECS/GEM, IEC61850-MMS, IEC-104 and more.
- Centralized security management for large scale pattern updates and firmware management via the TXOne EdgeOne.
- Support for Zero Day Initiative (ZDI)'s vulnerability reward program, provides fast response protection from undisclosed and zero-day threats.
- Research-supported, up-to-date signatures enable antivirus and virtual patching protection.

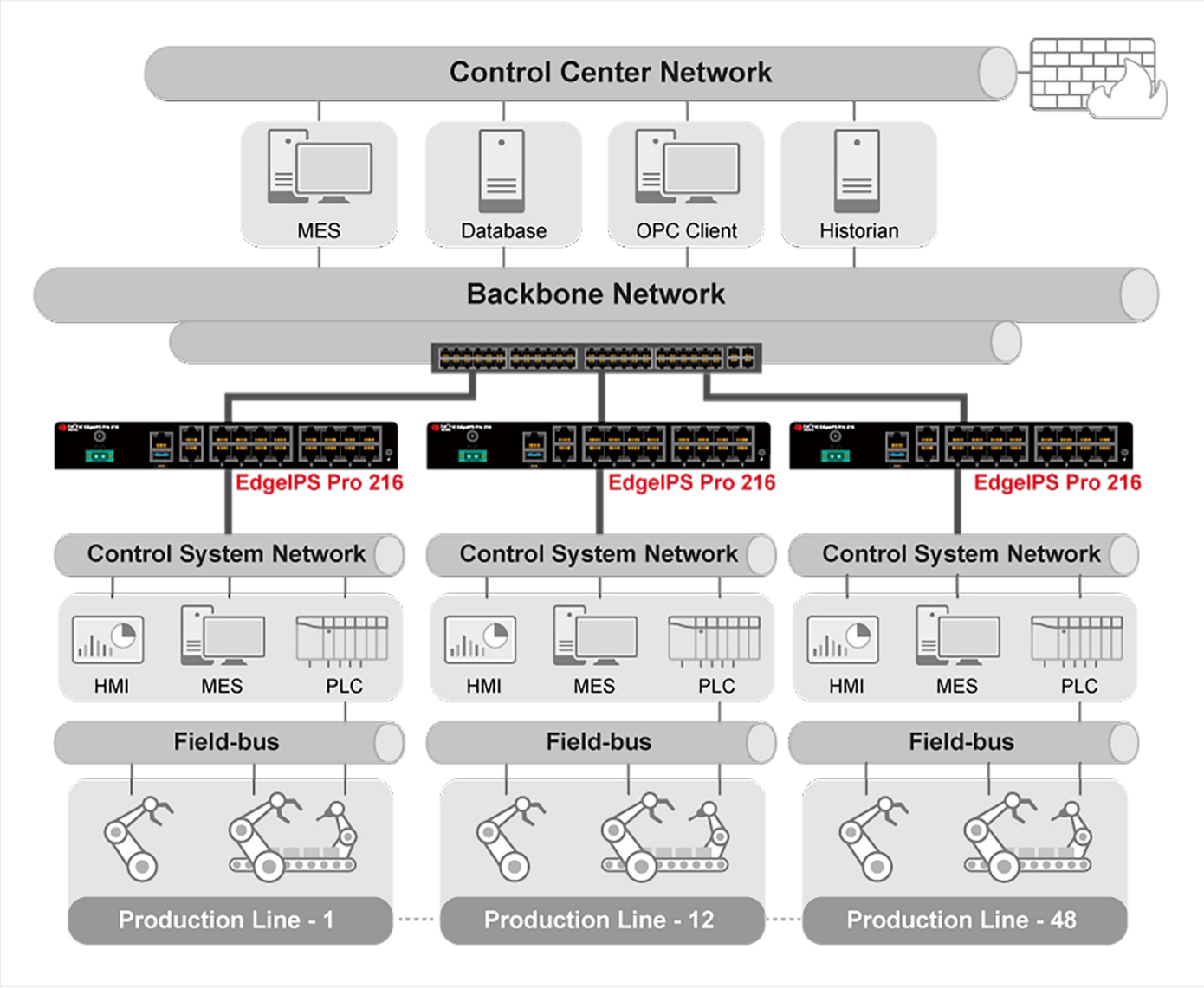

Figure 2. EdgeIPS™ Pro-216 in an OT security application.

Three EdgeIPS™ Pro systems protect fabs

The TXOne EdgeIPS™ Pro product family has several OT security appliances that offer these features at different performance levels for different network sizes:

EdgeIPS™ Pro 216 is a 16-port appliance with firewall/ threat protection throughput of up to 12 Gbps (based on 1518-byte UDP packets) with a latency of less than 500 ms and supporting up to 200,000 concurrent connections. The system connects to the network using up to a 1GbE connection. The EdgeIPS™ Pro 216 supports up to 8,000 policy enforcement rules and up to 256 ICS protocol filter profiles. Figure 2 shows an OT application.

The EdgeIPS™ Pro 216 runs on the CASwell ruggedized desktop network security appliance powered by Intel Atom® processors. The EdgeIPS™ Pro 216 provides the performance needed for in-depth OT protocol filtering to enable administrators to easily manage micro-segmentation for a complex fab environment. The EdgeIPS™ Pro 216 Is hardened for a harsh production environment and supports installation into any DIN rail-based cabinet.

For performance and micro segmentation, TXOne offers the **EdgeIPS™ Pro 1048** with 48 ports or the **EdgeIPS™ Pro 2096** offering up to 96 Gigabit Ethernet ports. The EdgeIPS™ Pro 2096 is 2RU high, double the height of the 1RU EdgeIPS™ Pro 1048. It is also double in most performance categories. The threat prevention throughput for the EdgeIPS™ Pro 1048 is 20 Gbps (with 1518 byte packets) whereas it is 40 Gbps for the EdgeIPS™ Pro 2096 with the same size packets.

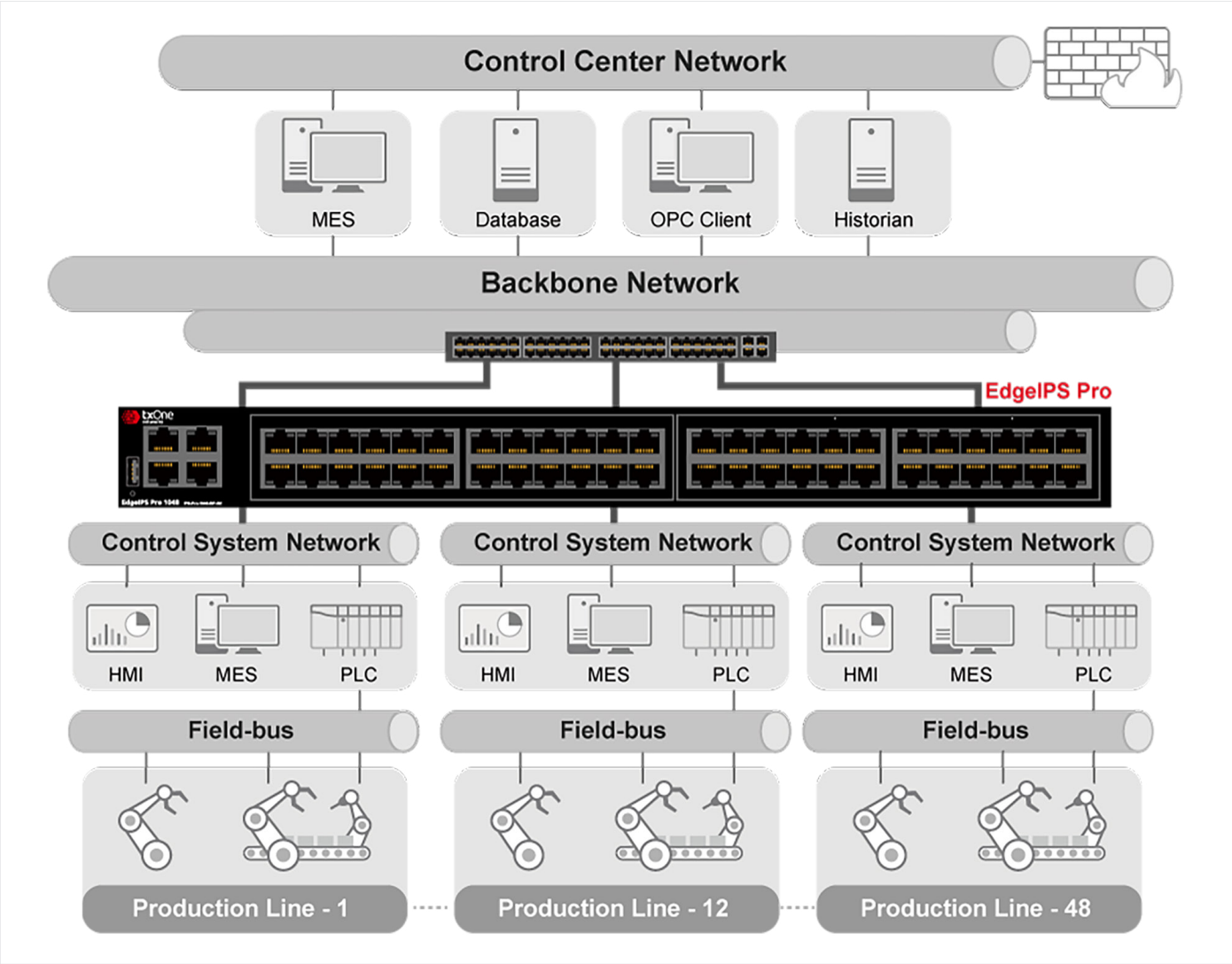

Figure 3. EdgeIPS™ Pro 2096 in an OT security application. The 96 port, 2RU-high security appliance offers two times the performance and port count of the EdgeIPS™ Pro 1048.

While both systems deliver a latency of less than 500 ms, the EdgeIPS™ Pro 1048 delivers up to 2 million concurrent connections and the EdgeIPS™ Pro 2096 delivers up to 4 million concurrent connections. Both systems support up to 256 ICS protocol filter profiles, while the EdgeIPS™ Pro 1048 supports up to 50,000 policy enforcement rules and the EdgeIPS™ Pro 2096 supports up to 100,000 policy enforcement rules.

EdgeIPS™ Pro 1048 / EdgeIPS™ Pro 2096 are based on the CASwell family of servers that come in single or double RU configurations both powered by 3rd Gen Intel® Xeon® Scalable processors. The TXOne networking solution, using its TXODI™ core technology, integrates the Data Plane Development Kit (DPDK) platform and Intel® QuickAssist Technology (Intel® QAT) cryptography and compression acceleration technology to deliver the most suitable industrial control network cybersecurity solution for OT applications.

All EdgeIPS™ Pro systems are managed by the EdgeOne management system that provides centralized OT network security management. Administrators can use the EdgeOne to enforce security policies and automate security processes. The management system can be integrated with other IT/OT security systems. The system dashboard can be used to monitor cases, analyze activities and receive notifications across very large scale and multiple location networks.

Conclusion

Protecting against OT cyber-attacks can be costly and challenging, especially for industries like semiconductor manufacturing facilities. Traditional IT tools come up short due to the heterogenous compute nature of an OT environment. Complex environments such as semiconductor fabs have a much larger attack surfaces making it even more difficult to provide effective cybersecurity protection.

TXOne Networks has tackled this challenge with a network-based defense system that features IPS, antivirus, virtual patching and other security and management functionality designed to protect the OT environment and to allow security managers to have visibility into the system. Powered by CASwell network security appliances based on Intel processors with network security performance and features, the systems offer the features and throughput to ensure proper security screening at wire speeds.

Learn More

CASwell Systems homepage

TXOne EdgeIPS™ Pro Product Family

Intel® Network Builders ecosystem

Intel Atom® Processor

Intel® Xeon® Scalable Processor

Intel® QuickAssist Technology (Intel® QAT)

[1] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/how-to-enhance-the-cybersecurity-of-operational-technology-environments#

0923/DC/H09/PDF ♻Please Recycle 356988-001US