



From Risk to Resilience:

Protecting Automotive Production with Data Diode Security

Implementing Unidirectional Data
Transfer for Secure IT/OT Integration

CUSTOMER

Customer is a leading automotive manufacturer with \$35 Billion global market cap, operating large-scale production facilities across North America. Its manufacturing environments rely heavily on Industrial Control Systems (ICS), Operational Technology (OT) networks, robotics, and real-time production systems to ensure efficiency, precision, and safety.

As part of its digital transformation strategy, the customer has been increasing connectivity between OT (factory floor) and IT (enterprise systems) to enable: predictive maintenance, real-time production analytics, supply chain optimization, and centralized monitoring and reporting. However, this convergence also introduces significant cybersecurity risks, particularly the potential for threats to move from IT networks into critical OT environments.

"With NEOX PacketRoo, we have achieved a level of security and assurance in our manufacturing environment that was previously difficult to attain. The unidirectional architecture allows us to safely leverage critical production data without exposing our OT systems to external threats.

This approach not only strengthens our protection against cyber risks but also enables our teams to maintain real-time visibility and make informed operational decisions with confidence. As a result, we have reduced our overall risk posture, simplified compliance, and ensured uninterrupted production—while continuing to advance our digital transformation initiatives."

Anonymous

Principal Systems Engineer



CHALLENGE

The customer faced several critical challenges in securing its manufacturing infrastructure as it advanced its IT/OT integration. Connecting factory floor networks with enterprise IT systems significantly increased exposure to cyber threats, including ransomware and lateral movement attacks targeting sensitive OT environments. At the same time, the nature of manufacturing operations demanded strict security controls and near-complete isolation to prevent unauthorized access, malware propagation, and any potential disruption to production lines.

Traditional firewalls and bidirectional security solutions were not sufficient to address the risk profile of these high-security OT zones. In parallel, operations teams required real-time visibility into production data, machine telemetry, and security logs to maintain efficiency and responsiveness, but without compromising the integrity or safety of OT systems.

Additionally, the organization faced growing regulatory and compliance pressures, further emphasizing the need for a robust, secure, and auditable approach to managing data flow between IT and OT environments.

SOLUTION

[NEOX Networks](#) is a recognized expert in delivering Unified Network Visibility solutions for both IT and OT observability and security. To address the customer's requirements, NEOX designed and implemented a secure, high-assurance architecture built around its [PacketRoo](#) solution—a unidirectional gateway (data diode) that enforces one-way data transfer from OT to IT environments. Deployed between the OT production networks and the on-site IT systems, PacketRoo ensures hardware-level unidirectional data flow, allowing only outbound data transmission while physically preventing any inbound traffic or potential attack vectors. This approach effectively creates a true air-gap, combining strong security with controlled data accessibility.

At the core of the solution are several key functional capabilities. PacketRoo provides unidirectional security enforcement through a hardware-based data diode that eliminates the risks associated with bidirectional communication, guaranteeing air-gap-like protection while still enabling necessary data sharing. It supports secure data replication by transmitting critical information such as production telemetry, syslog, and industrial protocol data safely to IT-side systems, including SIEM platforms, monitoring tools, and analytics engines. The solution is designed with broad protocol support, ensuring compatibility with both industrial and IT environments and enabling seamless integration into existing infrastructure. Additionally, PacketRoo operates with full transparency, requiring no changes to production systems and maintaining a passive, non-intrusive deployment model that does not impact operations.

Within the customer's manufacturing plants, OT systems—including PLCs, SCADA systems, and robotics—transmit telemetry data through PacketRoo to the IT environment. This data is then used for monitoring, analytics, and threat detection, providing valuable insights without introducing risk. Because the architecture enforces a strict one-way data path, there is no return channel from IT to OT, ensuring zero attack surface and complete protection of critical production environments.

VALUE

The customer selected the NEOX PacketRoo solution due to its ability to deliver absolute security without sacrificing visibility. Clear value provided includes:

Maximum Security (Zero Trust for OT)

- True physical one-way communication
- Eliminates attack vectors into critical systems
- Protects against ransomware and advanced threats

Maximum Security (Zero Trust for OT)

- Real-time access to production and security data
- Safe integration with enterprise monitoring tools

Operational Continuity

- No disruption to manufacturing processes
- Deterministic and reliable performance

Compliance & Risk Reduction

- Supports industrial cybersecurity frameworks
- Simplifies audit and regulatory requirements

Simple & Robust Architecture

- No complex rule tuning required
- Low maintenance, high reliability

NEOX Networks provides Next Generation Network Visibility for IT & OT Observability and Security. The result is strengthened cybersecurity, hybrid-cloud application observability, and business continuity by integrating the network intelligence and real-time data-in-motion. Learn more at neoxnetworks.com