



Solution Brief

Improving Operational Technology (OT) Cybersecurity and Reducing Risk Through Complete Network Visibility

A Joint Solution From Honeywell Technologies and Garland Technology

Critical infrastructure entities seeking protection for their OT networks turn to Honeywell Technologies to leverage their deep experience in industrial and building automation to deliver complete OT cybersecurity solutions. Enabled by Garland Technology OT network visibility solutions, Honeywell Technologies Cyber Insights, OT SOC, and AI prioritization tools Proactive Defense secure OT networks using the data from Garland's Network TAPs, Network Packet Brokers, Aggregators, and Hardware Data Diodes. 100% network visibility fueling 100% OT cybersecurity.

Joint Solution Use Cases

Use Case 1: Port Authority Improves OT Network Visibility

A large cargo port needed to monitor crane network traffic for suspicious cyber activity without disrupting critical crane operations. Garland Technology's Aggregators passively copy network traffic from the cranes and send it one-way to Honeywell Technologies security platforms for centralized threat detection.

Use Case 2: Simplifying OT Monitoring Across Job Sites

An oil and gas company with multiple distributed job sites needed real-time visibility into industrial control systems and IoT devices from a single centralized security stack. Garland Technology's Network TAPs capture traffic at each site, consolidate it through a packet broker, and feed it into Honeywell Technologies unified monitoring solution.

Use Case 3: Electricity Provider Improves Substation Security Monitoring

An electricity provider with dispersed substations needed a safe way to send mirrored network traffic to a cybersecurity sensor while meeting industry regulations. Garland Technology's Hardware Data Diode physically enforces one-way data flow from each substation to Honeywell Technologies security platform, eliminating any risk of reverse traffic.

Start Protecting Your OT Network Today

Every OT security team should be able to deliver continuous, consistent security regardless of their skills or experience. Together, Honeywell Technologies and Garland Technology deliver a proven approach that combines deep industrial cybersecurity expertise with trusted network visibility and isolation technologies, enabling organizations to protect their most critical OT environments—safely, compliantly, and at scale.

Use Case 1: Port Authority Improves OT Network Visibility (Aggregator)

■ CHALLENGE

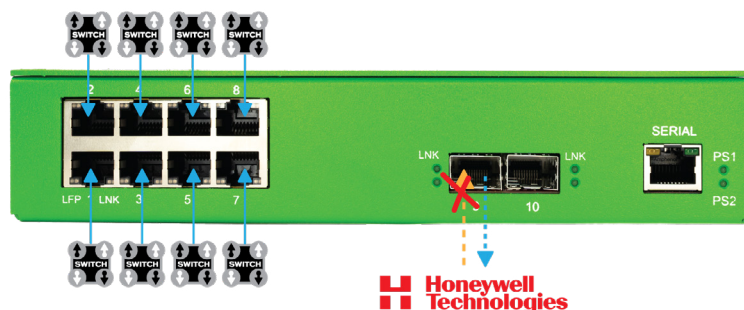
Digital Transformation within industrial environments, enterprises, and critical infrastructure continues to drive the convergence of IT and OT data, systems, and services. The result is an increase in attack surface, threat vectors, and potential asset exposure, necessitating a comprehensive approach that enhances threat monitoring and threat detection.

Ensuring the security of inherently insecure ICS networks has shifted to the purview of both IT and Security Operations Center (SOC) teams. At issue: Traditional IT security tools and methods are often not adapted effectively to suit OT environment safety, productivity and reliability, rendering them invisible to SOC teams. This invisibility poses significant challenges, including an incomplete inventory of IT/OT assets and an inability to effectively detect, assess, and mitigate the threats and associated risks they pose. To address this issue, organizations must develop a cohesive strategy that combines threat mitigation and threat visibility and monitoring.

■ SOLUTION

Digital Transformation within industrial environments, enterprises, and critical infrastructure continues to drive the convergence of IT and OT data, systems, and services. The result is an increase in attack surface, threat vectors, and potential asset exposure, necessitating a comprehensive approach that enhances threat monitoring and threat detection.

Ensuring the security of inherently insecure ICS networks has shifted to the purview of both IT and Security Operations Center (SOC) teams. At issue: Traditional IT security tools and methods are often not adapted effectively to suit OT environment safety, productivity and reliability, rendering them invisible to SOC teams. This invisibility poses significant challenges, including an incomplete inventory of IT/OT assets and an inability to effectively detect, assess, and mitigate the threats and associated risks they pose. To address this issue, organizations must develop a cohesive strategy that combines threat mitigation and threat visibility and monitoring.



Benefits

- **Safe, Non-Disruptive OT Monitoring :** Passive, unidirectional traffic collection preserves crane availability and safety while enabling continuous security monitoring.
- **Enhanced OT Asset and Network Visibility:** Honeywell Technologies solutions transform raw network traffic into actionable insight identifying assets, communication paths, and abnormal behaviors across crane operations.
- **Faster Time to Value:** Aggregators can be installed and operational in under one hour, accelerating deployment of Honeywell Technologies OT security capabilities without complex re-architecture.
- **Scalable, Future-Ready Architecture:** The combined Garland + Honeywell Technologies approach supports expansion to additional cranes, terminals, and port OT environments as cyber maturity grows.
- **Stronger Alignment Between OT and Cyber Teams:** Honeywell Technologies provides a common operational view that helps OT, IT, and security stakeholders collaborate effectively on risk reduction and incident response.

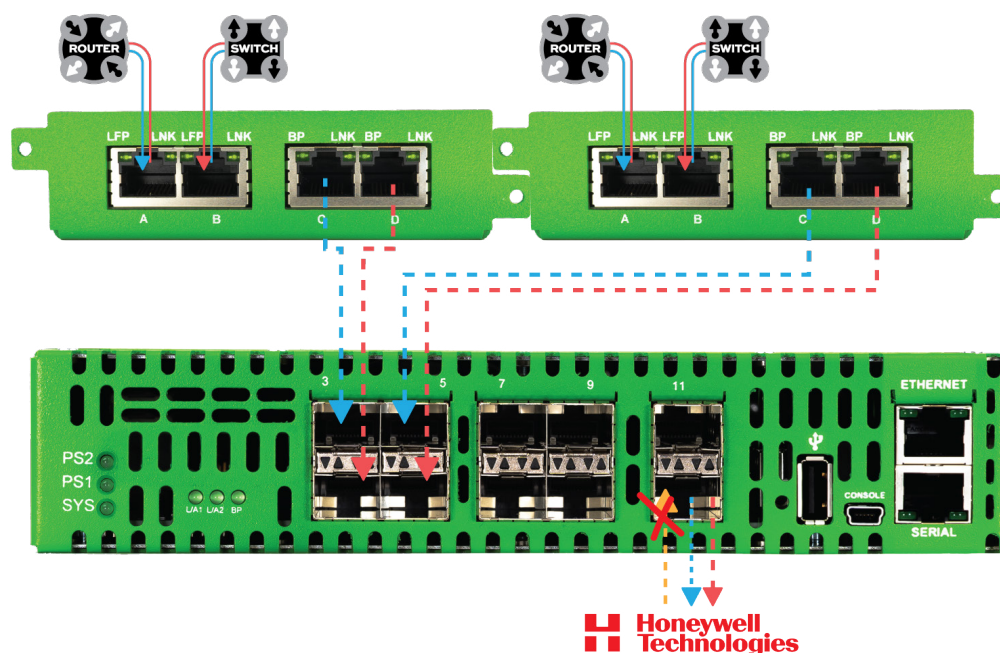
Use Case 2: Simplifying OT Monitoring Across Job Sites (Network TAP to Agg)

■ CHALLENGE

An oil and gas company managing multiple job sites needed real-time network visibility to monitor industrial control systems (ICS), IoT devices, and on-site security systems from one centralized OT security stack.

■ SOLUTION

Garland Technology's Network TAPs provided full access to traffic from the various locations, which was then consolidated through the use of a Network Packet Broker (NPB) to aggregate and load balance the traffic to a centralized Honeywell Technologies aggregated monitoring solution.



Benefits

- Reduce downtime and blind spots: Continuous visibility into OT network communications helps identify abnormal behavior and potential issues before they escalate into outages or safety incidents.
- Identify issues before they disrupt operations: Network TAPs ensure full, passive access to critical ICS and IoT traffic, while aggregation enables consistent monitoring across all job sites.
- Improve ROI by increasing the amount of data sent to Honeywell Technologies: By increasing the quality and relevance of data sent to Honeywell Technologies, customers gain more value from their existing OT cybersecurity and monitoring investments without expanding tooling at each site.
- Centralized OT Security at Scale: Honeywell Technologies solutions provide a unified view of OT environments across distributed locations, simplifying security operations and reducing the burden on local staff.

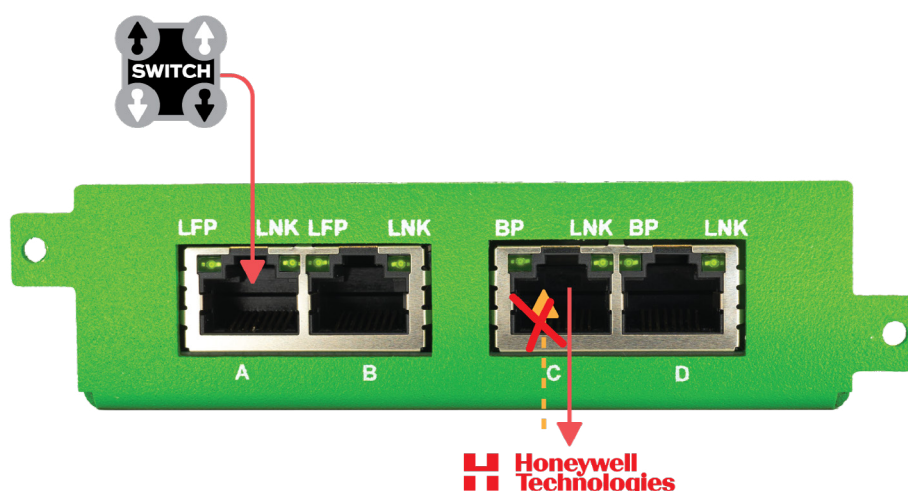
Use Case 3: Electricity Provider Improves Substation Security Monitoring (Hardware Data Diode)

■ CHALLENGE

Electricity provider dealing with disparate substations needed a simple and safe way to send SPAN traffic to a cybersecurity sensor to comply with industry regulations.

■ SOLUTION

Garland Technology's SPAN Hardware Data Diode passes copies of network traffic from SPAN Mirror Ports at each substation to Honeywell Technologies and, most importantly, eliminates bidirectional traffic flow by enforcing one-way data flow for SPAN links with physical hardware separation inside the Hardware Data Diode.



Benefits

- **Strong Regulatory and Compliance Posture:** Physically enforced one-way data transfer aligns with electric sector cybersecurity requirements and supports audits and regulatory frameworks without relying on software controls alone.
- **Scales with Substation Size and Complexity:** The solution easily adapts from small substations to large, complex environments without redesigning network architecture or adding operational risk.
- **Leverages Existing Switching Infrastructure:** Uses current SPAN/mirror ports, avoiding the need for new switching equipment or substation reconfiguration.



Have Questions?

sales@garlandtechnology.com | +1 716.242.8500
GarlandTechnology.com/honeywell-technologies

