USE CASE

Port Authority Improves OT Network Visibility with Garland Technology

Challenge

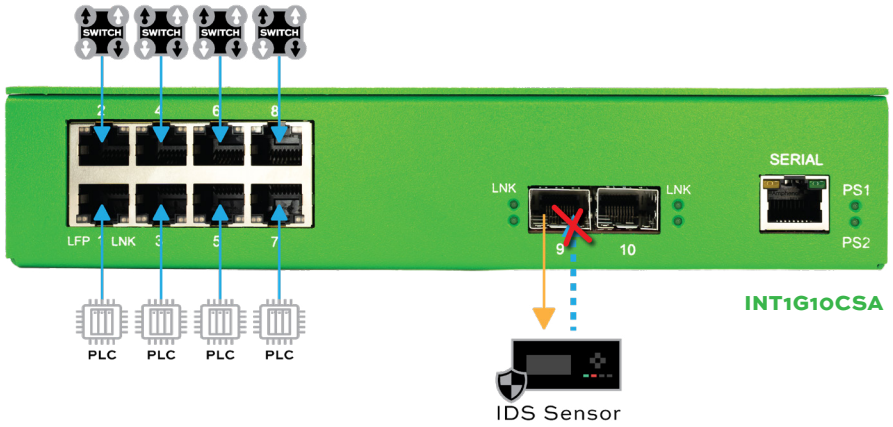
Ports are increasingly becoming a target for cyber attacks from common criminals to foreign nation states alike. A large US port recently came to Garland Technology looking for a way to ensure that traffic from the cranes used to unload cargo ships can be sent to their Intrusion Detection System (IDS) to ensure better visibility into their OT network.

The TAP to Tool™ Solution

1. Garland Technology Copper Aggregator TAPs are used to provide a 100% full-duplex copy of the traffic.
2. Aggregating on the TAP itself allows multiple links to be tapped and sent to the IDS sensor installed locally on each crane
3. The Aggregator TAP has built-in data diode functionality ensuring that there is unidirectional traffic flow, so there is no way to inject traffic from the IDS sensor back into the live network, even if the sensor was compromised in anyway.
4. Designed for unique OT environments, the TAP can be DIN Rail mounted on the crane ensuring a solution that saves on space, is easy to install, and won't be impacted by movement as the crane operates.

Benefits

- Easily install, configure, and copy packets in under 1 hour.
- Affordable solution to secure more for less.
- Invisible to hackers due to no IP or MAC address.
- Hardware Data Diode design.



Have Questions?

sales@garlandtechnology.com | +1 716.242.8500 | GarlandTechnology.com