Industrial: Infrastructure

Providing Visibility and Reducing Network Complexity

With the digital revolution Oil & Gas (O&G) companies are facing, integrating their operations environments through AI, robotics, analytics, and the Internet of Things (IoT), with increasing connectivity chasing the ultimate goal of faster and more efficient systems to improve performance and streamline the supply chain, they inevitably open themselves up to increased cyber security risk.

And the risks are high, as hackers have recently targeted hundreds of US O&G control systems. According to Deloitte University Press, in 2016 energy was the industry second most prone to cyber-attacks, with nearly three-quarters of US O&G companies experiencing at least one cyber incident.

Recently, Garland Technology was tasked by a leading multinational O&G company operating exploration and production, refining, distribution and marketing, petrochemicals, power generation and trading, as well as biofuels renewable energy, wind power, smart grid and solar technology, to provide data diodes to protect network access points.

Challenge: O&G companies are expansive. From upstream and downstream environments of pipelines, refineries, tank farms, to distribution and retail, all relying on industrial control systems (ICS) to maintain consistent and safe operations. New advances in sensor technology, processing power, remote operations, and IoT technology, create a growing list of challenges. Add to that contrasting priorities of OT and IT departments, and we had our work cut out.

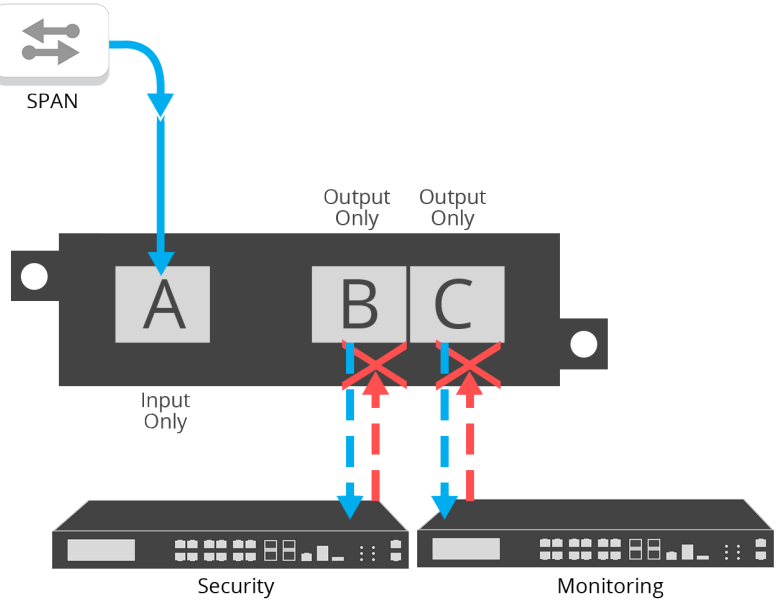
Specifically for this project we faced legacy equipment and devices that heavily relied on SPAN ports for their network operations and security connectivity. There were also specific segments where unidirectional gateways required data not to be injected back into the network - which their SPAN ports couldn't solve. With remote sensors in field locations, they were struggling to keep their virtualized environments safe from cyber threats. Lastly, enabling them to satisfy corporate responsibility initiatives and various regulations, including European Union guidelines like EU Cybersecurity Act published by ENISA and multiple others.

Goal: After multiple network design discussions, they realized Garland's capabilities solved many of the challenges they were facing. The goal of this project adds secure visibility to an aging infrastructure, reduces connectivity complexity, enabling higher performance - helping to bridge the OT (operation technology) and IT (information technology) departments and ultimately, safeguard against cybersecurity risks.

Solution: The visibility architecture proposed by Garland Technology took into account their varied OT infrastructure within numerous locations, utilizing both fiber and copper connectivity, 1G and 100M network speeds, and switches that have SPAN ports. Also, this solution includes sending network traffic to an IDS monitoring sensor.

Garland Technology recommended installing network test access points (TAPs) for all monitoring feeds to guarantee 100% of the network traffic is copied and transmitted to monitoring tools. A monitoring tool can only perform effectively and consistently when receiving 100% of data packets. TAPs are independent and invisible to the network. Network TAPs pass all 7 layers of OSI network traffic including layer 1 and layer 2 errors. As well, TAPs do not have an IP address or a MAC address and can't be hacked. When enhanced with Failsafe technology, TAPs provide an effective way to deliver power redundancy, without being a failure point in the network.

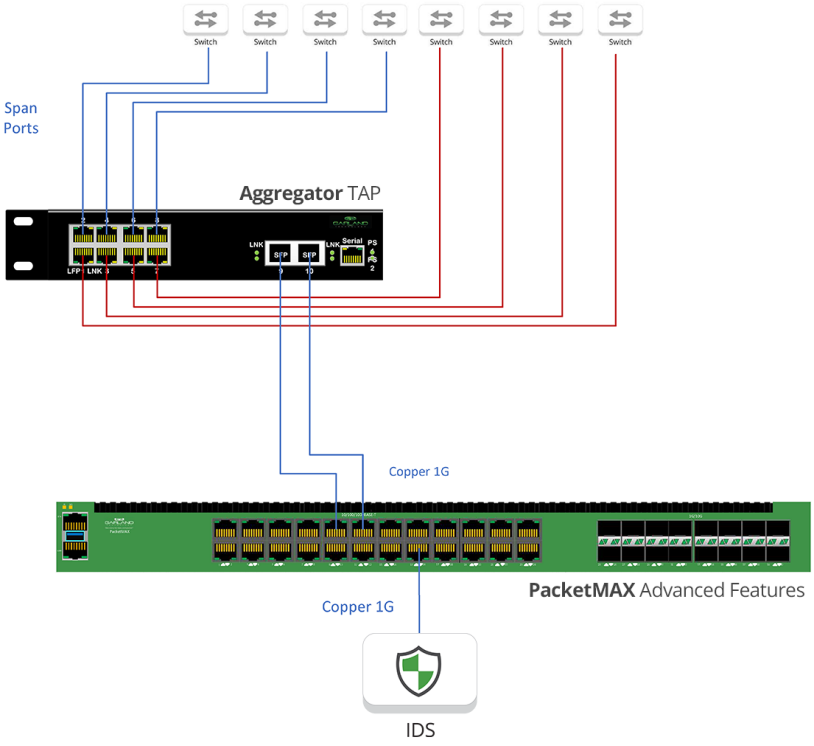
For the unidirectional gateway segments, Garland Technology's Data Diode TAPs ensure data is never injected back into the network by physically forcing traffic to flow in a single direction. When traffic is locked in a unidirectional path there is zero risk of data flowing back into the network and creating security risks. This was a key component in guaranteeing information security or protection of critical digital systems, for their SCADA/industrial control systems, from inbound cyber attacks.



Many companies across various industries run into architectural complexity challenges, now add in the requirements from both OT and IT and it's easy to see how industrial environments need to reduce complexity for future growth and streamlined performance.

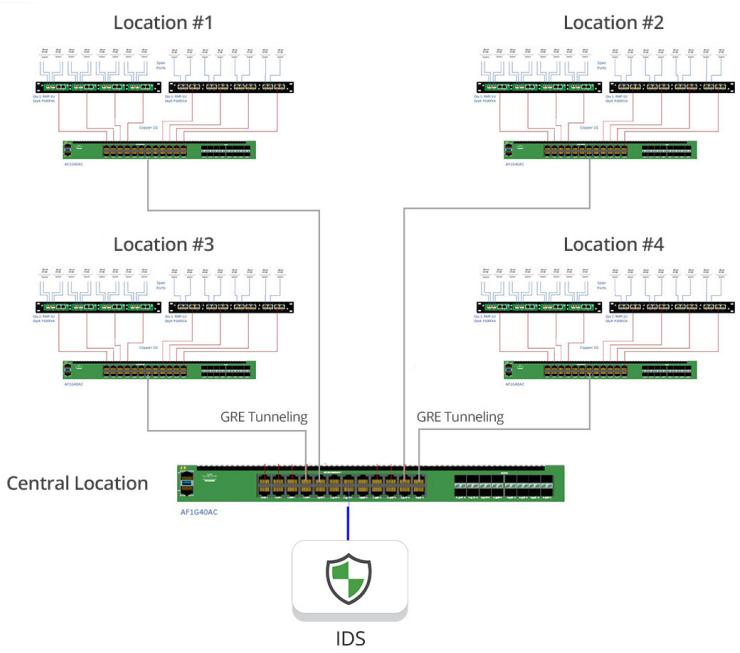
For instance, we faced a web of existing SPAN ports, which was their main packet capture solution, adding a whole layer of complexity as well as adding risk, through dropped packets creating blind spots for the monitoring tool. As well as easily being misconfigured or turned off unintentionally transmitting zero network traffic to the monitoring tool.

A good best practice to follow if SPAN port usage is required is installing TAPs between the switches on each individual network segment. This will provide safeguards and prevent performance degradation of the switch. Network TAPs allow you to easily manage access points in the network to instrument and deploy new monitoring and security tools. If you still need to utilize some SPAN links, Aggregator TAPs allow you to take those SPAN and consolidate them into just one or two links.



The next step in optimizing network complexity was adding an aggregation layer to manage all of these links. Garland's PacketMAX packet brokers aggregated, filtered and load balanced the TAP traffic, streamlining the data collection for analysis during troubleshooting or security incident response, allowing OT and IT access to the data they need, at the right time.

With multiple sites Garland's PacketMAX can move traffic from one location to another through Tunnel Encapsulation (GRE, L2GRE) - a routed external network link was required for this feature. This creates the ability to connect the individual power stations to a master control location or even another power station. The monitoring tool can be located separately from the network being monitored because tunnel encapsulation can send monitored traffic from one location to another. This provides cost saving by reducing the quantity of monitoring tools required and delivers redundancy should a monitoring tool within the network fail.



With their recent virtualized SCADA deployments, they face drastically reduced visibility and blindspots into their remote operation VMs. Deploying Garland Prisms traffic mirroring, eliminated these data blind spots, providing the SCADA platform and other connected system access and visibility. But adding our new air gapped private solution and TLS encryption option provided the added security assurance they were looking for.

Implementing a proper network visibility fabric for this Oil & Gas company provided the OT teams enhanced productivity, accelerated resolution of service degradation or downtime and improved IT/OT collaboration. Network aggregation improved the network performance and ROI by reducing administrative overhead, improving data quality, also improving tool collaboration and data sharing, while reducing the cost of the overall visibility solution.

Benefits:

- Reduce network complexity and administrative overhead
- Enable infrastructure upgrades
- Improved the network performance
- Improve effectiveness of tool performance
- Added infrastructure security

Looking to add visibility and reduce network complexity, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do.