Radiflow

Use Case

Cybersecurity for the Oil & Gas Industries

In May 2021, a ransomware attack against Colonial Pipeline forced the company to shut down about 5,500 miles its pipeline system, which runs from Texas to New Jersey and provides approximately 45% of the U.S. East Coast's fuel supply. The days-long shutdown and gradual reopening led to higher gas prices, fuel hoarding and shortages in some U.S. states.

The Colonial Pipeline attack demonstrated the potential catastrophic effect of even a short-term shutdown of a single component of a country's ONG drilling, delivery, distillation, storage and distribution infrastructure. The threat is compounded by the increasing sophistication of attackers, often state-sponsored; the overall increase in attacks against industrial operations; and the ongoing process of digitalization & automation of traditional industries.

Unfortunately, many ONG companies around the world still lack the defenses needed to prevent a major shutdown, and have yet to adopt a systemic approach of continuous cyber risk management.

Protecting the Lifeblood of all Economic Activity

Oil and natural gas derivatives still by far make up the bulk of the fuel used for transportation, manufacturing and energy. Therefore, disruptions to any stage in the supply chain may cause of chain reaction of disruptions:

- Blackouts and brownouts in natural gas-powered isolated electric grids
- Partial of full shutdown of utilities, from water purification and supply to trash disposal
- Shortages of heating fuel in cold areas
- Gasoline and diesel fuel shortages, leading to higher gas prices at the pump, higher shipping costs for goods and higher travel costs
- Oil spills due to storage facility failures or deliberate sabotage
- Damage to ONG companies' equipment and facilities, and heavy losses to stakeholders in the case of longer shutdowns

The Challenge of Securing Oil & Gas Facilities

Like other critical industrial sectors, the ONG industry is embracing digitization, which means greater exposure to an altogether new landscape of attack vectors aimed at real time operational upstream data connections.

Intelligent field instrumentation – the devices that monitor activity levels, collect data and execute operations – have become the preferred target for hackers, as they're typically less protected than central operations systems. By gaining access to device controllers, hackers can change operational values such as pump speed or valve state, and bring down entire swaths of the fuel supply chain.

At the same time, the ONG industry is slow to implement changes due to scale, complex ownership and operational structures, and extensive government regulation and oversight (including API 1164, for pipeline control systems, API 780 for risk assessment methodology, ISA/IEC-62443 for network security, INGAA cybersecurity guidelines for the natural gas sectors and many other local standards and regulations worldwide.)

In addition, the distributed nature of ONG operations and the location of facilities – off-shore rigs or remote unmanned facilities – introduce both physical and cyber-vulnerabilities to the OT network; and the use of multiple vendors' networked devices poses the danger of supply chain attacks, executed through infected data payloads sent by vendors to installed devices.

As a whole, the level of network security in many ONG companies highly differs between companies, according to a February 2020 research commissioned by the US Dept of Energy's Office of Scientific and Technical Information (OSTI). The "general consensus" is that the ONG industry is lagging behind the power supply industry in securing operations, and that the entire sector on a whole is unaware of potentially useful technologies that have been developed to ensure the cyber-security of infrastructure systems.

A Structured Approach to Securing Oil & Gas Production

There's no "silver bullet" for effectively protecting any infrastructure's ICS, and more so cyber-protecting complex ONG operations. Threat mitigation measures need to match each individual network's topology, technology, device and vendor-specific vulnerabilities, sector, locale and existing security measures. Not considering each network's needs and properties would lead to investing in the wrong security controls, lesser security and lower cybersecurity ROI.

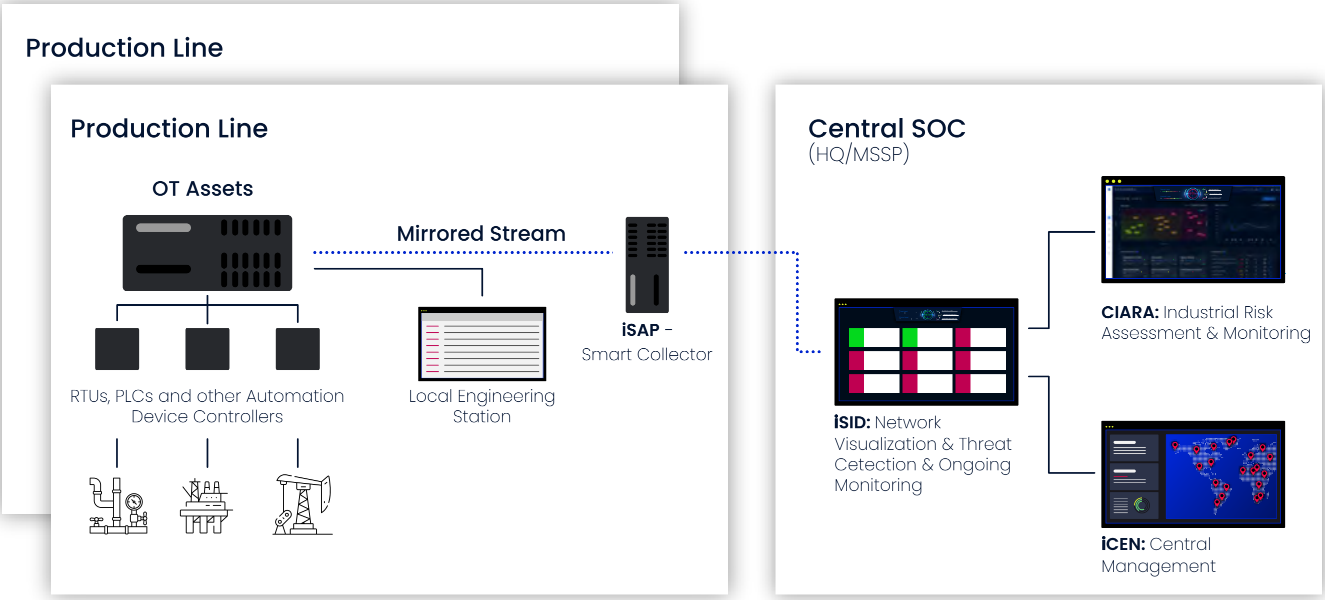
A structured process of implementing an effective ICS security system therefore should include:

1. **Network modeling and visibility**: this stage involves creating a model of the oil company's OT network, including network topology,device properties, state, vulnerabilities, and potential inter-zone attack vectors, protocols and ports, etc. This model (or "digital image") is used for breach and attack simulations, and also provides the user with full network visibility.

2. **Risk assessment**: this stage includes simulating numerous breach attempts into the oil & gas production operational environment, and the ability of installed and proposed security measures to defend the network, accounting for the impact of a shutdown of different industrial units.

3. **Implementation**: Using the simulation data, an ROI-optimized OT security plan is generated (matching the user's security preferences and budget constraints), as well as key indicators and reports for the network's risk state. The user is presented with a prioritized list of mitigation measures toward strengthening and optimizing OT security, in accordance with IEC62443.

4. **Long-term security management**: In time, systems grow and evolve, new components are added, and hackers become more sophisticated and determined. The key to long-term system security is ICS network monitoring, which provides constant identification and mitigation of intrusion attempts, as well as ongoing risk posture evaluation due to new threats.


Production Line
Production Line
OT Assets
Mirrored Stream
iSAP - Smart Collector
Local Engineering Station
RTUs, PLCs and other Automation Device Controllers
Central SOC
(HQ/MSSP)
CIARA: Industrial Risk Assessment & Monitoring
iSID: Network Visualization & Threat Cetection & Ongoing Monitoring
iCEN: Central Management

Radiflow Solutions for for ONG Operations

MAP - Digital Imaging & Network Visualization

Through non-intrusive self-learning, Radiflow's ***iSID industrial threat detection and monitoring system*** constructs an accurate digital image of the ONG production network. The digital image is presented in map form as a visual management tool, down-drillable to all device properties, vulnerabilities and inter-asset attack vectors.

For distributed ONG production networks, the ***iSAP smart collector*** provides WAN/ LAN-friendly data transfer of real-time data traffic (up to 90% reduction in data volume) from multiple operational units to a central instance of iSID for analysis and monitoring.

KNOW - Risk Posture & Network Characteristics

Using the learned digital image of the network as well as MITRE ATT&CK and other TI sources, the ***CIARA industrial risk assessment and management platform*** conducts numerous non-intrusive/nondestructive Breach & Attack Simulations (BAS) to assess the Risk, Control and Threat levels to different operational units, as well as the effectiveness of installed and available mitigation controls. The structured discovery process covers all fundamental requirements (FRs) specified in IEC62443 and allows simulating other threat types including supply chain attacks. The risk assessment findings are presented to the user in the form of customizable planning and auditing reports.

ACT - Ongoing hardening & ROI optimization

Based on its breach simulations and on the user's budgetary constraints, CIARA produces an ROI-optimized mitigation plan which prioritizes the effectiveness of security measures vis-à-vis the user's cybersecurity preferences (e.g. improve compliance or focus on securing critical production units).

Radiflow's platform empowers users to take control over alerting rules and device communication policies, and improve the lifecycle management of networked assets.

For remote ONG production locations, Radiflow offers a DPI Secure Gateway/Firewall with work order-based remote access management, to ensure the integrity of maintenance operations and prevent both erroneous and malicious technician activity.

MONITOR - Continuous Threat & Risk Monitoring

All OT networks, and especially those used for critical ONG operations, need to be continuously monitored. Radiflow provides tools for efficient real-time monitoring and handling of operational and security alerts, including early indications of breach attempts, generated by a single or an array of iSID threat detection systems, all through a single pane of glass at the ONG company's SOC.

About

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant OT security data. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow | For more info: radiflow.com