SECURING OPERATIONAL TECHNOLOGY IN THE OIL & GAS INDUSTRY

FOUR KEY CONSIDERATIONS

BAYSHORE

V2.7217

Executive Summary

A fourth industrial revolution is underway, driven by the interconnection of physical infrastructure and the systems that control it. The Industrial Internet of Things (IIoT), or just the Industrial Internet, is changing how products and services are designed, manufactured, sold, delivered, and operated.

This interconnection of critical industrial infrastructure is unlocking vast potential in business efficiency, transformation, and innovation, none more so than in the oil and gas industry. But this interconnection comes with a cost, and that cost is the need for protection against cyber threats.

This whitepaper will examine general trends in the convergence of IT and OT, opportunities and risks created by the interconnection of oil and gas infrastructure and the need for securing the OT environment, and four key considerations when protecting industrial assets against cyber threats. Lastly, it introduces Bayshore's Industrial Control Platform, which stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet.

State of Cyber Readiness

Given the rise in cyber-attacks in the past few years, much attention is now being paid to the insecurity of the oil and gas industry's infrastructure across its exploration, production, processing, and transportation sectors. "In a study from the Ponemon Institute – The State of Cybersecurity in the Oil & Gas Industry: United States – just 35% of respondents rated their organization's operational technology (OT) cyber readiness as high. Additional key findings related to readiness, risks, and challenges include:

- 59% believe there is a greater risk in the OT environment than the IT environment;
- 61% said their organization has difficulty mitigating cyber risks across the oil and gas value chain;
- Only 41% of respondents said they continually monitor OT infrastructure to prioritize threats and attacks;
- 65% of respondents say the top cybersecurity threat is the negligent or careless insider and 15% of respondents say it is the malicious or criminal insider – underscoring the need for advanced monitoring solutions and critical safety zones to identify atypical behavior among personnel;
- 61% say their organization's industrial control systems protection and security is inadequate."[1]

This lack of cyber readiness is exacerbated by the rapid pace of connecting OT to the Internet. According to Frost & Sullivan, 80% of manufacturing companies around the global will have adopted the Industrial Internet of Things by 2021.[2] That's both an opportunity and a challenge in the oil and gas industry.

The opportunity comes from the ability to derive huge amounts of data from sensors and devices and analyze it to enable more efficient business operations. Connecting OT to IT for data analytics has enabled operators to:

- Improve process optimization and predictive maintenance
- Improve distribution efficiency and ROI
- Enable transformation of industrial data to support business applications
- Increase profitability and uptime

[1] "Study reveals cyber readiness gaps in US oil and gas industry," Hydrocarbon Processing, February 2, 2017. http://www.hydrocarbonprocessing.com/news/2017/02/study-reveals-cybersecurity-readiness-gaps-in-us-oil-and-gas-industry

[2] "Cyber Security in the Era of Industrial IoT," 2017, Frost & Sullivan, sponsored by Bayshore. https://www.bayshorenetworks.com/cybersecurity-in-the-era-of-industrial-iot

One example is an oil field with 200 wells that sends out data such as pressure and flow as well as the amount of hydrogen sulfide and water. SCADA systems use this information to check on well health and also share this information with joint venture partners. If the operator produces 1,000 fewer barrels in a month, the partners will use the SCADA data to understand what happened to lower production.

Another example is the use of SCADA data on trading floors. When oil companies sell product in forward markets as options, the traders will know exactly what the field is going to produce by monitoring the SCADA data rather than waiting until the end of the month to receive information. This enables traders to efficiently sell production and settle contracts, regardless of whether the oil producer is on target or not.

Lastly, operators know well the capital-intensive nature of maintenance, requiring a great deal of planning as well as cost. Being able to predict and plan for maintenance enables a competitive advantage in production strategy as well as managing cash flow. For example, the West Texas oil fields have been able to double oil production because they have been able to justify the capital expenditure of expansion when oil prices jumped. The bottom line is that SCADA data gives companies the opportunity to understand where to make their investments.

The challenge comes from securing operational technology (industrial control systems, SCADA systems, PLCs, RTUs) as well as its interconnection with the corporate network. This is difficult because:

1) Whereas OT used to be isolated (air gapped) and therefore physically secure, that is no longer the case due to the need to connect to enterprise systems. With the move to the Internet, the security perimeter is essentially broken. As OT is opened to let data out, malware (WannaCry, CrashOverride, Petya) can get in. A way must be created for data to transit the network securely and be policed at the same time.
2) OT was designed for safety first, not security. Because ICS is mission-critical, it is non-trivial to take it offline to secure. Remote terminal units/wireless modems on cellular networks are typically low-end devices (e.g., sensors pulling telemetry data on pressure and temperature from oil SCADA systems). These RTUs are difficult, if not impossible, to secure because they use outdated technology designed without security in mind.
3) Legacy systems are also out of date. While IT may try to defend the perimeter (at the risk of breaking OT), locking everything down means systems can't intercommunicate and companies can't take full advantage of the interconnection between IT and OT.
4) Engineers with expertise specific to the oil and gas industry are retiring in droves, taking hard-won organizational knowledge with them. Finding talent to replace them is well-nigh impossible. Additionally, security experts familiar with OT environments such as oil and gas do not exist in required numbers.

The Convergence of IT and OT

Given these opportunities and challenges, the convergence of IT and OT is being driven by many factors, including **convenience** (it's much easier to turn off a valve from the comfort of a control room in the plant than in the field), **cost savings** (less expensive as well), **the availability of new technologies** (wireless and cloud), and **the advent of big data analytics** (to take advantage of the output from all the sensors). But the interconnection brings additional security challenges because of different protocols and different networks. Unfortunately, corporate IT networks can be a gateway for cyber attackers to infiltrate the OT network through lateral movement, and the cost of cyber-attacks on your control network is frankly unnerving:

- Oil spills at drilling sites or along the pipeline leading to environmental damage
- Disruption leading to power outages
- Damage or destruction of plant, pipeline, and drilling assets
- Economic fallout and loss of revenue from impact to business operations
- Damage to corporate reputation and consumer preference
- Potential loss of life due to explosions, pollution, or disruption of service

"The protection of such critical infrastructure has never been more important. Oil and gas businesses are taking preventative measures: ABI Research expects that oil and gas companies will be spending $1.87 billion on cyber security by 2018. Nonetheless, the industry still lacks awareness as petroleum companies fall victim to cyber-attacks. Thus, there is a need for more information on what these dangers to the industry look like… Stuxnet, a computer worm targeting industrial programmable logic controllers (PLCs) and SCADA systems, was a wake-up call to every industry. Despite the fact that it was not specifically designed to attack the petroleum industry, several oil and gas companies were infected with the virus."[3]

The problem in securing the Industrial Internet is that IT does not understand OT, and OT issues cannot be solved with enterprise IT tools and processes. There must be a better way.

[3] Alexander Polyakov, "Cyber Security Risks to Be Aware of in the Oil and Gas Industry," April 3, 2017. https://www.forbes.com/sites/forbestechcouncil/2017/04/03/cyber-security-risks-to-be-aware-of-in-the-oil-and-gas-industries/#5ad3f2273f0a

Protecting Against Cyber Threats: Four Key Considerations

While much attention has been paid to securing the IT network, CISOs and CIOs now realize they must also secure their control network. Boards of Directors are asking about their corporate-wide risk maturity level that includes not just IT but also OT**.** Identifying and protecting against cyber threats is a mandatory first step before connecting pipelines, plants, drilling assets, and other industrial infrastructure to the Industrial Internet. Here are four key considerations when assessing solutions:

Improve End-to-End Asset Visibility: You Can't Protect What You Can't See

Ensure your solution continuously maps and monitors industrial traffic, learning as it adapts to observations. You'll want to combine advanced threat intelligence from public and private sources with out-of-the-box policies to establish and maintain a baseline of acceptable behaviors. Look for an approach that helps you optimize and protect your OT environment, including protocols, sources, destinations, manufacturers, models, and anomalies or violations of baseline policies. In addition, ensure that the solution can inspect full messages (regardless of protocol) for both content and context at the transaction level and that all reporting can be integrated into your SIEM/SOC and forensic analysis tools of choice.

Mitigate Cyber Threat Risks: Just Seeing a Threat Won't Stop It

Look for an approach that stops cyber threats in real time, before they can damage your industrial infrastructure or the environment. Look for active alerting and proactive blocking of unauthorized communication and commands, preventing cyber threats from reaching and affecting targeted objects and data. You'll want a solution that operates at line speed, providing protection at a fine-grained transaction level, enabling authorized traffic and normal workflows to continue unimpeded even in the face of ongoing cyberattacks.

Provide Managed Remote Access: Protection Means Control over Access and Actions

Allowing vendors to remotely access industrial equipment for maintenance and troubleshooting offers obvious advantages. Providing industrial data to service providers may help improve business outcomes. However, opening industrial infrastructure to 3rd parties creates significant risk. Traditional VPNs can help with controlling access, but once a connection is made, owner/operators have no way to know or control the actions that remote users undertake on their open ports. The porous lack of cyber protection provided by VPNs is simply unacceptable in the industrial world. Look for a Managed Remote Access solution that goes far beyond traditional VPNs to create an on-demand, encrypted, policy-protected, bi-directional tunnel between remote users and your industrial infrastructure.

Ensure that every element of communication between you and 3rd parties is verified, managed, and blocked if necessary. Look for Managed Remote Access that enforces authentication, authorization, white lists, and other security controls at the device command and individual transaction level.

Secure Your Industrial Internet: Protect Your Assets Before You Connect

When you are ready to interconnect your industrial infrastructure and data to take advantage of all the Industrial Internet has to offer, look for a solution that offers bi-directional, access-controlled, and policy-protected tunnels between your organization and your chosen IIoT partners. This means that not only is access limited to specific sources and destinations, but also that content and context is controlled by policy so that every element of communication between the organization and its external IIoT ecosystem can be verified, alerted, and blocked if necessary.

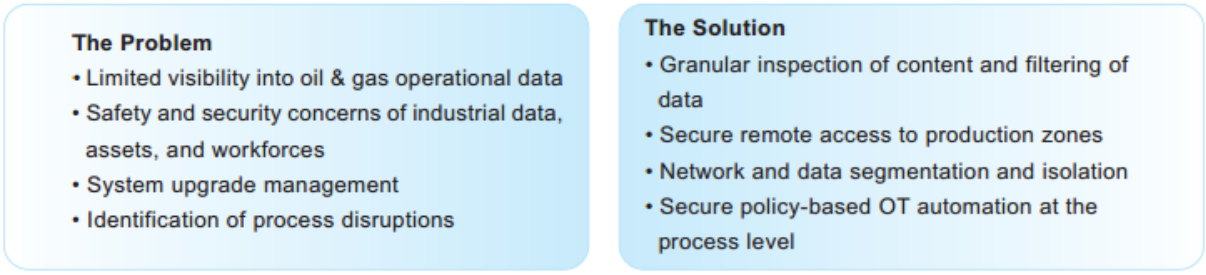


Figure 1: Oil and Gas Customer Use Case

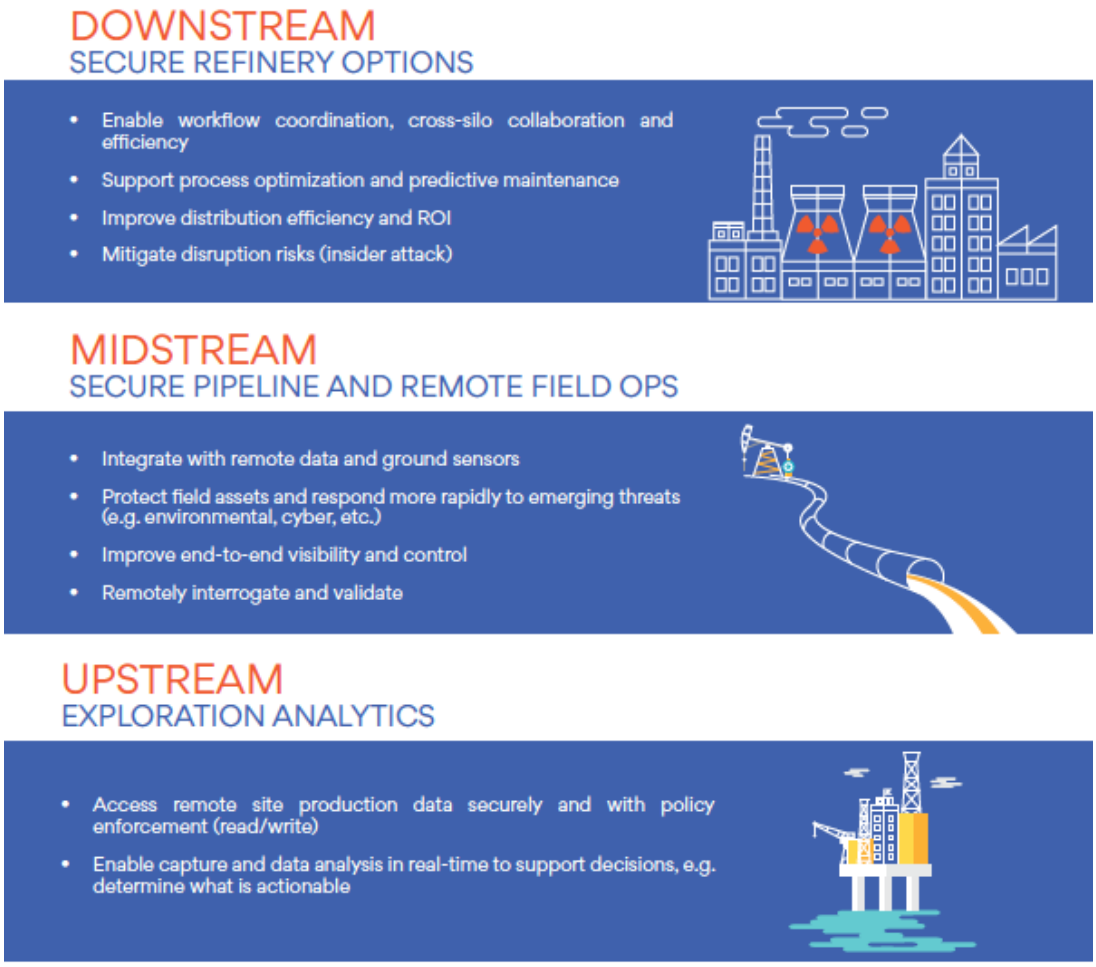
How Bayshore Networks Can Help

The Bayshore Industrial Cyber Protection (ICP) platform stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet of things (IIoT).

The Bayshore ICP platform delivers a comprehensive set of capabilities required to protect and defend against sophisticated, complex attack systems. Bayshore empowers industrial enterprises with safe and efficient production, operational insights, and improved business outcomes, while blocking cyber threats to industrial plants, machinery, and people. It is designed to support customers throughout the entire industrial cyber protection life cycle, leading to improved business outcomes.

The journey begins with mapping networks assets and progresses to identifying anomalies, preventing attacks and incidents, optimizing business efficiencies, and finally, to enabling innovation and digital transformation, such as creating new revenue sources and product markets.

The comprehensive industrial cyber protection platform uniquely offers customers a long-term solution by providing the following capabilities and features in a single, tightly integrated, extensible, and scalable architecture.



Summary

New cyber security threats to the Oil and Gas infrastructure are emerging every day, risking safety, environment, downtime, operational disruptions, and costly physical damage to plants, machines, and products.

Bayshore inspects machine-specific industrial protocol traffic such as upstream and downstream telemetry from oil field equipment. Cyber threats are eliminated before they reach critical equipment, protecting OT applications, networks, machines, workers, and the environment.

Additionally, Bayshore's Managed Remote Access solution allows owner/operators to grant tightly controlled access to 3rd parties, such as equipment vendors, for maintenance and troubleshooting. This can be especially valuable for offshore and remote operations.

Bayshore protects refinery operations, filtering process control system network traffic and eliminating unauthorized commands and attempts to exfiltrate valuable information.

Next Steps

For more information on the Bayshore Industrial Cyber Protection platform, visit www.bayshorenetworks.com/platform.

About Bayshore Networks, Inc.

Bayshore Networks® is the leading provider of industrial cyber protection. The Company's award-winning technology unlocks the power of the Industrial Internet of Things (IIoT), providing enterprises with unprecedented visibility into their Operational Technology infrastructure while safely and securely protecting ICS systems, industrial applications, networks, machines, and workers from cyber threats. Bayshore's strategic partners include among others Arista, AT&T, BAE, Cisco, Dell, SAP, VMware, and Yokogawa. Bayshore is a privately held company headquartered in Washington, DC and backed by Trident Capital Cybersecurity, Yokogawa, Samsung Next, and BGV Capital. For more information, visit www.bayshorenetworks.com.

BAYSHORE

www.bayshorenetworks.com