From Complexity to Opportunity

Ensuring a more secure future for the Oil and Gas industry
Executive Summary

There are over a million oil and gas wells in the United States alone, all connected by pipelines that stretch for millions of miles. Although digitalization can help asset owners in the oil and gas industry operate more efficiently, until recently, oil and gas businesses have been cautious about embracing digitalization. Because of the vulnerability of converged networks to cyber and operational threats, the industry has largely held back on converging their information technology (IT) and operational technology (OT) infrastructures, a key element of the digitalization process.

As pressure on oil and gas margins mounts and the need to squeeze more value from existing assets increases, the potential benefits of IT-OT convergence also increase. One of the major benefits of a converged network is the ability to deploy sensors that provide vital monitoring, measurement and maintenance data to facilitate maintenance cost savings, operational efficiency gains, and downtime reduction that result from fewer equipment failures.

Although existing solutions can usually deliver cyber security for the IT side, OT is a different ball game altogether. In the OT environment, enjoying the opportunities from IT-OT convergence requires enhanced industrial control system (ICS) asset visibility.

This white paper describes an innovative approach to optimizing ICS visibility and asset performance management in the oil and gas industry: using an advanced and mature network monitoring and situational awareness platform for industrial networks. It also explains how OT managers and their colleagues can utilize this type of solution to establish true cyber resilience, reduce their workloads, and deliver increased organizational value.
Opportunity Is a Complex Business

It’s fair to say that oil and gas businesses are behind the curve when it comes to digital transformation. In part, this is due to the understandable prioritization of safe and reliable production and an aversion to the potential risks of connecting drilling fields, pipelines and refineries to the Internet of Things. Nevertheless, there is an increasing realization in the oil and gas industry that to stay competitive this conservative approach needs to change. Specifically, oil and gas businesses need to leverage the potential opportunities offered by advanced robotics, data analytics, and the integration of information technology (IT) and operational technology (OT) infrastructures. These opportunities include finding new markets, optimizing the supply chain, and improving operational performance through preventative maintenance that identifies potential failures before they occur. In fact, the World Economic Forum [1] estimates that the oil and gas industry could generate between $1.6 and $2.5 trillion of additional revenue, depending on how boldly businesses embrace the possibilities.

However, the network convergence required to realize such advantages generates a new level of complexity for IT and OT managers within oil and gas businesses. Previously siloed industrial control systems (ICS) networks become exposed to an increasingly broad range of IT technologies, as illustrated in Figure 1.

---

**Figure 1: New business needs are driving the exposure of ICS networks to multiple technologies**

**DIGITALIZATION DIVIDEND**

Digitalization can generate between $1.6 and $2.5 trillion of additional revenue for the Oil & Gas industry

*(World Economic Forum)*
Initially, integration with ERP systems helped businesses align resource allocation more closely with production. Since then, increasing security threats and the importance of mobile technology in managing operations have required multiple alarming, reporting and update systems to be given access to the ICS network.

As Forrester [2] reported in January 2018, 100% of organizations have IoT technologies connected to their ICS networks, and the average number of external technologies involved is more than 4. Additionally, 64% of organizations surveyed in the same report said they provide third-party IT vendors with complete or high-level access to their ICS networks. The next generation of systems to be integrated into the ICS will be cloud-based supervisory control and data acquisition (SCADA) systems, which will add yet another layer of complexity.

As far as the oil and gas sector is concerned, the criticality of the industry's output for society, as well as the global nature of the infrastructure required to support it, make it particularly vulnerable to criminal attacks. The IT and OT networks involved comprise tens of millions of processors and support the generation, transmission and storage of petabytes of highly valuable data. Moreover, industrial control systems are accessed across multiple regions by a broad range of stakeholders, which means the number of potential points of entry for cyber criminals is enormous. This additional complexity from such a distributed environment greatly increases the chance of potential malfunctions, misconfigurations and operational errors.

In addition to network complexity, diverse teams of C-level executives, business managers, engineers, and IT, OT and IS experts are needed to define IT-OT network infrastructure in its entirety. Most of these stakeholders do not have deep insight into the respective technologies and processes of their colleagues' environments. Moreover, none of them has a complete picture of all the assets connected to the converged network. And, what can't be seen cannot be protected or efficiently maintained. Knowledge about current ICS asset performance, vulnerabilities, status and configuration, also known as ICS visibility, is scarce; therefore, so is the ability to detect and prevent potential incidents before they cause damage to oil and gas businesses.

The challenges and risks associated with the lack of asset performance and security visibility in a converged IT-OT network environment are explored in more detail below.
The 6 Challenges and Risks of IT-OT Convergence

1. Rising Costs

Lack of asset visibility generates costs by making it more difficult to overcome the challenges and risks described below. These costs can be direct, such as the additional man hours required to manage and achieve compliance across a more complex environment or the revenue lost during unplanned downtime caused by an ‘invisible’ network asset. Operational continuity is especially critical since downtime in the oil and gas industry is particularly expensive. An article published by Deloitte [3] in 2017 estimated that one day of lost operations for an oil refinery producing 100,000 barrels per day could cost over $5.5 million in revenue and $1.4 million in profit.

To illustrate this, let’s consider the process for commissioning a Distributed Control System (DCS) or a full plant. This is a team effort which requires that the testing and design documents be accurate, well written and executed in orderly phases. Despite the likelihood of mid-project changes, at some point the implementation team must trust the commissioning plan 100%. Within this context, how can a single change such as adding a device to the network be executed successfully without slipping through the cracks? After all, the device must be included in the new design, the drawings, the design specification documents, the factory acceptance test (FAT) and site acceptance test (SAT). Smooth, visible integration of the device can only be achieved by ensuring real-time awareness of the asset inventory, even across remote and unmanned stations.
2. Unplanned Operational Downtime
According to a recent report by technology market research specialists Vanson Bourne [4], achieving zero unplanned downtime is high board-level priority among almost three-quarters (72%) of organizations surveyed. This is unsurprising, given the huge costs generated when operations are disrupted. Unfortunately, the risk of unplanned downtime caused by the network complexity described above, and by a lack of asset visibility, is increasing. In fact, the Vanson Bourne report states that some level of asset inventory ignorance caused by a lack of visibility affects around 70% of organizations.

In the oil and gas sector, internal negligence or malicious activity can exacerbate this problem. For example, the Ponemon Institute’s [5] latest report on “The State of Cybersecurity in the Oil & Gas Industry: United States” reported that 65% of respondents cited a negligent or careless insider as the greatest cybersecurity threat to their business. The same report revealed 15% of respondents believe malicious or criminal insiders pose the greatest risk.

Ironically, positive business results can adversely affect enterprise asset management (EAM) activities. For example, 39% of respondents to a Gatepoint Research [7] survey entitled “Asset Management Strategies for Oil and Gas Businesses” stated that rapid business growth presents a challenge to the capabilities of their current EAM practices, and 42% reported that they would like to improve the timeliness of the information provided by their EAM solution.

Because of these factors, implementing advanced monitoring that can provide real-time updates is crucial.

“Only 14% of oil drilling operations have fully operational security monitoring.” [6]
3. Increasing Cyber Threats
In recent years, the number of Internet-connected devices accessing OT networks has increased dramatically. As a result, OT networks, proprietary systems and legacy technologies that were isolated from cyber incidents in the past now need protection from Internet-based threats. Sensors, wi-fi enabled controllers, and the latest cloud-based industrial control systems such as SCADA-as-a-Service all provide potential entry points for cyber adversaries. In fact, the Forrester survey [8] cited above revealed that 79% of SCADA/ICS operators reported a breach in the past 24 months. Every breach of this kind can potentially compromise the safety of employees and the financial stability of affected organizations, and statistics from the Repository of Industrial Security Incidents indicate that the petroleum industry is second on the list of most targeted industries. In terms of specific vulnerabilities, Deloitte defines seismic imaging and geographical surveys as the least vulnerable areas, which also face less severe consequences if they are compromised. At the other end of the scale, development drilling and production are, not surprisingly, the most vulnerable and the most likely to suffer serious consequences, especially because less than half of drillers use any monitoring tools on their upstream operations networks. Of those, only 14% have fully operational security monitoring centers.

79% of SCADA/ICS operators reported a breach in the past 24 months

Figure 3: Most targeted industries (global)
*Source: RISI Online Incident Database*
The lack of asset visibility described above is also a source of increased cyber threat risk. As the SANS Institute [9] recently reported, 15% of companies affected by a breach needed more than a month to realize they had been breached, and 44% were never able to identify its source. In one case managed by Forescout, many devices that should have been decommissioned were found to be active and communicating within IP sub-networks. These devices were unmapped and had not been updated for some time, posing a huge security risk. This kind of asset invisibility can exacerbate the severity of both direct and indirect financial consequences of any downtime caused by a breach. Additional indirect costs can also be generated, such as the reputational damage caused by a security breach that could not be identified in advance. Cumulatively, these costs can also represent millions of dollars in unplanned expenditure.
4. The IT-OT Relationship Puzzle

IT and OT are very different departments with very different responsibilities. IT’s top priority is protecting data. OT’s top priority is protecting the availability and integrity of the industrial process. However, modern business conditions require that IT and OT managers cooperate to protect the ICS network. CIOs and CISOs also now must accept responsibility for any unexpected downtime, equipment damage or safety hazards in their industrial environments caused by cyber incidents. To fulfill this responsibility, they need to have maximum visibility into ICS network asset inventory and performance.

The results of the oil and gas industry report from the Ponemon Institute cited above provide evidence of this challenging situation. Just 33% of respondents said they believe there is full alignment between OT and IT with respect to cybersecurity operations. Furthermore, 60% said they are understaffed, and just under half said they have the internal expertise to manage cyber threats to the OT environment.
5. Limited Resources and Increasing Workloads

IT and OT managers in the oil and gas industry already have heavy workloads without the additional layer of complexity generated by IT-OT convergence. Moreover, while IT and OT network visibility solutions exist individually, they rarely intersect. Manually piecing together information from such solutions is imprecise and gaining contextual intelligence from them is an even bigger task that can break already overstretched teams. Unless complete visibility and control is established over everything that is happening within their respective environments, it is inevitable that their jobs will become even more difficult and stressful. And where IT visibility has already been achieved, it’s often OT visibility that is the missing link.

The stress on OT resources is particularly acute in the producing fields environment, where engineers with decades of experience in specialized roles, such as rod pumping, are leaving the workforce without being replaced. Those still in the field can’t manage thousands of wells effectively or make informed operational adjustments rapidly when conditions change.
6. High-Effort Compliance Fulfillment

Any framework for achieving compliance requires solid asset management and visibility as a foundation. Increased network complexity, as well as constantly changing internal policies and external regulations, make this task more difficult and time consuming. This in turn exacerbates the resource and workload challenge described above.

Despite the costly and labor-intensive compliance efforts many companies implement, the possibility of fines being imposed remains relatively high. Moreover, future compliance costs and efforts are likely to rise. One cause is illustrated by a recent Ponemon Institute [10] report, which highlights the fact that two-thirds of senior IT security leaders expect to increase the frequency of audits and assessments, with board directors becoming more involved in overseeing overall IT security effectiveness. These factors tend to support the other findings of the Ponemon Institute report, which also provide insight into the relationship between simplifying compliance and improving security. For example, the report revealed a 90% year-over-year increase in the number of survey respondents who believe a reduced compliance burden contributes to a stronger cybersecurity posture. The same survey also revealed that just 48% of oil and gas industry respondents believe their organization is effective at complying with industry-specific security standards and guidelines.
Increasing ICS Asset and Threat Visibility Is Key

So, how can oil and gas businesses make informed decisions about how to prioritize spending and create security plans that will safeguard their employees, reputations, and bottom lines?

Using data to improve business operations certainly isn’t a new concept in the oil and gas industry, but the way that data is accessed and leveraged to drive value continues to evolve. Within the last decade, technology has advanced beyond basic data analysis tools and simple algorithms to intelligent EAM.

Built on the foundation of the Industrial Internet of Things (IIoT), intelligent EAM automates data collection from sensors on physical assets and aggregates that data into usable formats. Analytical algorithms then process the data to deliver outputs that drive increased operational efficiency and decreased unplanned downtime.

However, in recent years the oil and gas industry has still lagged in return on their asset investments. A key reason for this is that optimizing ICS visibility management is fundamental to achieving the benefits of intelligent EAM, and many organizations struggle with this. For example, a 2017 survey by the SANS Institute found that 40% of ICS security practitioners “lack visibility or sufficient supporting intelligence into their ICS network.” In the oil and gas industry, where avoidable accidents and spills can generate significant clean-up costs and regulatory fines, this situation is particularly dangerous.

Figure 4: Average annual return on operational assets by industry 2010-2014

Source: Public data and EY analysis; ROA calculated as: net income/total assets; Asset intensity calculated as: operating assets/total sales
Optimizing ICS visibility management enables oil and gas organizations to have a thorough understanding of the ICS environment and its connections, making it easier to design effective security architectures, identify attack vectors and locate blind spots, among other things. Improved visibility also enables OT managers to resolve unknown and unchecked operational security issues. These include vulnerabilities, misconfigurations, access policy violations, faulty design in the form of weak security controls, as well as unplanned or unauthorized changes.

However, traditional approaches to achieving visibility are flawed. For example, random network scanning can cause process interruption or system downtime that leads to financial loss. In more extreme cases, it can even damage the industrial environment or result in employee injury if safety controls are compromised. Physical inspections on the other hand, are safer but extremely labor-intensive, time-consuming, costly and error-prone.

Fortunately, there is a technique that can identify assets and help manage their performance accurately, safely and cost-effectively: ICS network security monitoring.
An optimal approach to achieving ICS visibility involves the adoption of an advanced and mature passive network monitoring and situational awareness platform for industrial networks. These monitoring solutions are invisible to the network and have no impact on running processes. They collect asset information such as type, version and location by listening to traffic already traveling through the network. Because of the automated and passive nature of this method, operators can continuously track asset information and behavior. This greatly increases the efficiency of a traditionally expensive operation like maintaining an accurate asset inventory. Optionally the asset owner can decide to deploy additional non-intrusive active modules. Driven by the passive system, the active modules can more extensively query specific nodes of the network to gain additional information, while helping to guarantee the total absence of impact on the network.

NON-INTRUSIVE MONITORING
The collection of asset information such as type, version and location by listening to traffic already traveling through the network optionally combined with active modules for enhanced collection.
Solutions like this leverage powerful machine learning capabilities called full deep packet inspection (DPI). They also feature vast libraries of ICS-specific threat indicators and vulnerabilities for analyzing standard and proprietary industrial protocols from all the major SCADA manufacturers. Other key capabilities include:

- Asset inventory and management, including dynamic business asset classification
- OT vulnerability management, including those with and without CVE identifier
- Anomaly detection, to detect not only new attacks and techniques but also deviations from normal process behavior
- API integration with IT security management tools
- Broad ICS protocol support
- Optional non-intrusive active modules which can more extensively query specific nodes to gain additional information

These features enable non-intrusive monitoring solutions to detect operational threats including network connectivity problems, device malfunction and misconfiguration, dangerous process operations, use of insecure protocols and default credentials, advanced cyber-attacks, and exploit attempts. Alerts about potential threats to operational continuity are then delivered to a central visibility management platform in real time. From there, they can be escalated appropriately within the organizational ecosystem.

By combining sensor-derived information from across the network with other data sources such as controls configuration and asset management, a comprehensive, visual and interactive model can be constructed. This gives OT managers complete ICS visibility and a clear path towards achieving true cyber resilience.

“This gives OT managers total ICS visibility and a clear path towards achieving true cyber resilience.”
With enhanced ICS visibility and asset performance management analytics, oil and gas OT managers can tackle the challenges associated with greater IT-OT infrastructure convergence. The benefits range from cost savings to lower workloads and simplified compliance.

### The 6 Benefits of Optimized ICS Visibility Management

1. **Improved Investment Decision Making**
   - Increased ICS visibility and intelligent asset management enable managers to make more informed investment decisions about which assets to repair and which to replace, providing a solid foundation for optimizing operational costs.

2. **Significant Cost Savings**
   - Increased visibility means potential threats can be identified quickly and addressed cost-effectively. When all assets can be viewed on a single pane of glass, the asset owner can check that the right asset is being monitored and that maintenance is progressing as it should, without expensive site visits. This decreases the cost and effort involved in investigating attacks or vulnerabilities, as well as those associated with troubleshooting, mitigating and resolving them. Additionally, using asset performance analytics to perform proactive, condition-based maintenance of equipment extends the lifespan of assets. Additional cost savings can be measured in the avoidance of downtime, service or delivery disruption and the reputational damage caused by successful cyber-attacks. According to McKinsey [11], it is estimated that better asset visibility can reduce overall maintenance costs by up to 13%.

**SAVINGS FROM**

- Improved maintenance
- Fewer site visits
- Reduced downtime
3. Reduced Unplanned Operational Downtime

According to the Vanson Bourne report cited above, 49% of respondents believe that machines requesting assistance automatically would be helpful in avoiding downtime and 45% would also like to enable engineers to access historical asset data. A network monitoring approach to ICS visibility management provides the tools that enable this.

**Continuous network health checks** give oil and gas OT managers a complete picture of current asset status within a single interface.

**Intelligent EAM** aggregates and processes the data collected from physical asset sensors and delivers outputs that drive higher operational efficiency and minimize downtime.

**Automated alerts** help managers identify potential problems at their earliest stages and gather the information required to respond as quickly as possible.

**The history of all the config changes** applied to assets is also preserved and can be easily accessed to analyze behaviors and issues.

**NO MORE PRODUCTION PANIC**

Additionally, the insight gained from every incident can be used to help managers pinpoint future weak spots and inefficiencies. This means many potential problems can be anticipated and addressed before they cause downtime and any associated operational, financial or reputational damage.

“The insight gained from every incident can be used to help managers pinpoint future weak spots.”
4. Complete Visibility

Full knowledge of ICS assets, and performance, vulnerabilities, additions and changes, ensures oil and gas OT managers are no longer working blindly. This helps them make informed decisions about which controls to implement for risk mitigation and how to prioritize security and maintenance plans and spending. In addition, a unified view of the organization's entire attack surface, including vulnerabilities across IT and OT networks, virtual- and multi-cloud networks, can determine potential attack path exposures. Overall, a higher level of cyber hygiene and early detection capabilities enhance the ability of oil and gas businesses to prevent and/or detect and respond to ICS cyber incidents.
5. Reduced Workloads
Using an asset inventory solution based on network monitoring gives oil and gas OT managers the insight they need to define the network accurately and maintain that precise definition continuously. The result, a synergy is created that empowers them to collaborate closely with their IT and IS colleagues. This helps all stakeholders understand the interconnectedness of the environment, pinpoint the biggest risks and plan how to deal with them. All of which helps the organization protect network integrity and achieve cyber resilience across the board. And because enhanced ICS visibility and asset performance management make the network easier to control and protect, OT managers are also better positioned to increase the value they deliver to the business with less effort, and less cost.

6. Simplified Internal and Regulatory Compliance
The complete inventory information and controls delivered by ICS network monitoring simplify and reduce the cost of maintaining compliance with:

- Standards and frameworks such as the NIST Cybersecurity Framework, IEC 62443 and FISMA.
- Guidelines such as the American Petroleum Institute (API) 1164, API – Recommended Practice 780, Risk Assessment Methodology, ISA/IEC-62443 and the INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry.

Asset inventory data is made available through powerful automated reporting capabilities that eliminate error-prone and costly manual data entry. The data includes critical information such as manufacturer, model, serial number, part/type (e.g. IO card, communication module), firmware version, hardware version, device name, vulnerabilities, changes, and Purdue network level. A comprehensive inventory list and an interactive network map that groups assets and communications by device type and network also enables accurate reporting and auditing to help avoid potential penalties with minimal effort.
Conclusion

Leveraging the potential benefits of converged OT and IT infrastructures offers a competitive advantage for oil and gas businesses, but only if ICS visibility and asset performance can be managed efficiently, and possible cyber or operational incidents can be identified and prevented. While existing security management tools can cover the IT side of the IT/OT equation, the oil and gas ICS world needs a dedicated solution. An optimized non intrusive monitoring approach to ICS visibility management is the best solution available.

The advantages of achieving ICS visibility and improving asset performance management include complete asset performance transparency, a significant reduction in OT management workloads and costs, lower business risk through cyber and operational incident prevention and simplified compliance. Ultimately, optimized ICS visibility and asset performance management helps oil and gas businesses leverage all the advantages of IT/OT convergence, while significantly lowering the cost and effort required to achieve true cyber resilience.

Resources

[7] “Asset Management Strategies for Oil & Gas Businesses” - Gatepoint Research
[10] “2018 Study on Global Megatrends in Cybersecurity” - Ponemon Inst., 2018
About Forescout

Forescout empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary and comprehensive network monitoring platform has been successfully deployed by customers worldwide. And, unlike some other providers, we already offer the flexibility and completeness to effectively protect IT and OT assets in multiple industry-specific usage scenarios. In 2018 Forescout was recognized by Frost & Sullivan for its game-changing industrial cybersecurity solution, earning the 2018 Global Customer Value Leadership Award for protecting industrial companies' information/operational technology (IT-OT) system networks against malware and zero-day attacks.

Want to Learn More?
Click here to read more about eyInspect (formerly SilentDefense) from Forescout and its benefits.

Talk to us today by sending an email to: info-ot@forescout.com