PARTNER | SOLUTIONS | COMPONENTS

Tripwire Industrial Visibility for Oil and Gas Applications

The oil and gas industry has long been in the crosshairs of cybersecurity threats targeted at industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. These advanced automation networks, collectively known as operational technology (OT) networks, are used throughout the entire upstream and downstream operations lifecycle. The extensive use of these automation systems significantly increases productivity, but at the same time it provides an additional attack surface that threat actors can leverage to inflict material harm.

This document focuses on the offshore exploration drilling sub-segment within the upstream oil and gas operations, which is executed by rig contractors for exploration and production (E&P) companies. The rapidly-changing liability landscape in offshore drilling, combined with increased recognition of cyber risk, is driving E&P companies to compel rig contractors to implement sound cybersecurity programs on their vessels as a prerequisite to a drilling contract. This in turn has created an equally strong business imperative for rig contractors to develop cybersecurity policies and procedures and to seek solutions that align with the unique needs of their OT systems.

Tripwire can secure and optimize operational networks running critical processes, like the complex, integrated OT systems that offshore drilling vessels rely upon. Therefore, Tripwire is the ideal partner for a rig contractor that seeks not only to comply with E&P contractual requirements, but to take a leading role in transforming the cybersecurity posture of its vessels.

In this document, we provide a detailed analysis of unique offshore drilling OT attack surfaces and operational challenges and walk through typical offshore installations. This will serve to illustrate the broader cybersecurity and operational challenges that characterize the oil and gas industry.

Offshore Rigs Overview

Mobile offshore drilling units (MODU), used in the exploration and development of wells, are divided into jackup rigs that reside in shallow water sea beds and floaters (drilling ships and semi-submersibles) for mid and deep water drilling. Standard drilling ships and semi-submersibles typically include four major independent OT networks that are each managed by an external contractor and differ from each other in automation equipment and communication protocols.

Security and Operational Challenges

The fragmentation and management of the floaters' OT networks causes the following structural security vulnerabilities:

1. Remote access required by the network contractors for maintenance activities introduces a new attack surface. Compromising a privileged third-party account to gain an initial foothold on the network is a common attack vector that has been utilized numerous times in targeted attacks. (Fig. 2)
2. Drilling ships' OT networks that are not air-gapped. They are often connected directly with the rig contractor's main IT network, which is connected to the internet. (Fig. 3)

It is clear that these structural vulnerabilities pose a significant risk. However, this risk cannot be soundly managed by rig contractors for two reasons:

1. Each network is often separately managed by its respective contractor in a complete silo. Therefore, there is no unified view of all assets across the entire OT network environment.

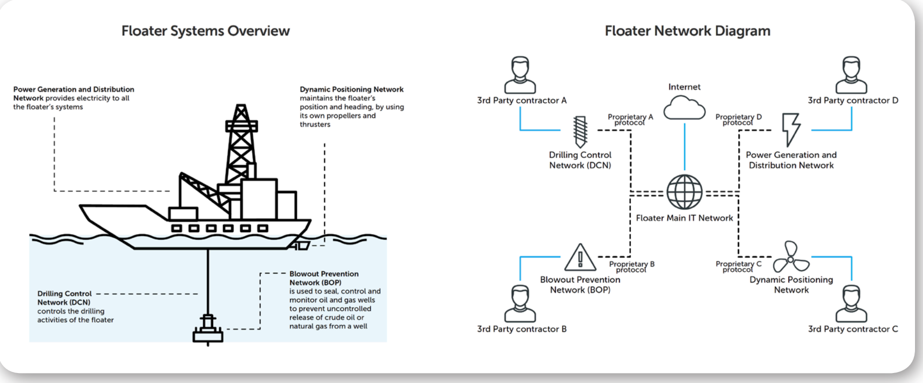
Floater Systems Overview
Power Generation and Distribution Network provides electricity to all the floater's systems
Dynamic Positioning Network maintains the floater's position and heading, by using its own propellers and thrusters
Drilling Control Network (DCN) controls the drilling activities of the floater
Blowout Prevention Network (BOP) is used to seal, control and monitor oil and gas wells to prevent uncontrolled release of crude oil or natural gas from a well
Floater Network Diagram
3rd Party contractor A
Internet
3rd Party contractor D
Proprietary A protocol
Proprietary D protocol
Drilling Control Network (DCN)
Power Generation and Distribution Network
Floater Main IT Network
Proprietary B protocol
Proprietary C protocol
Blowout Prevention Network (BOP)
Dynamic Positioning Network
3rd Party contractor B
3rd Party contractor C

Fig. 1 Example Floater Systems Overview and Floater Network Diagram

2. From the technology perspective, traditional IT security monitoring products do not provide visibility into the entire scope of proprietary OT protocols that are utilized by the assets throughout the floater's networks.

Acknowledging these challenges, rig contractors seek a solution that enable them to attain visibility and regain control over their OT networks and better address the safety and operational risks.

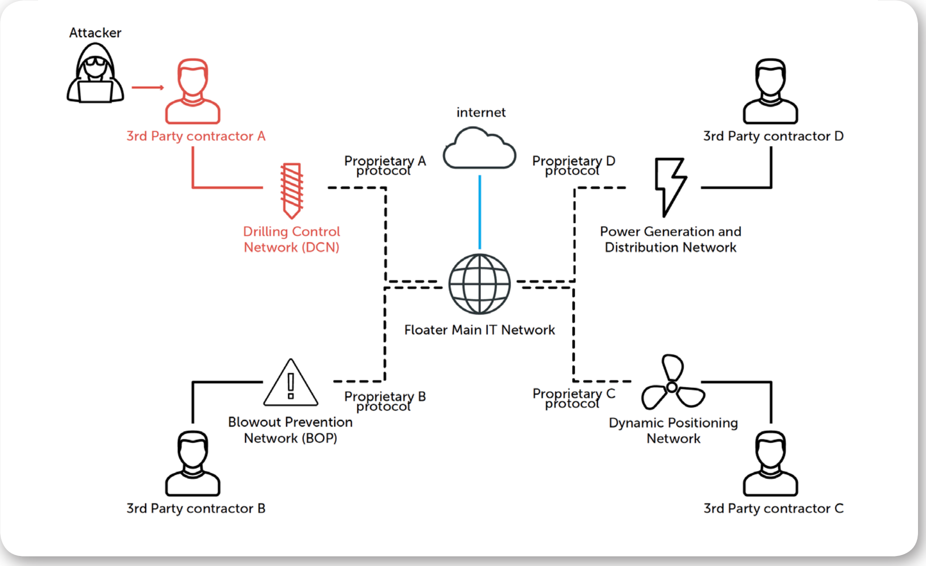

Fig. 2 OT Network Attack 1: Compromise the Third-party Contractor

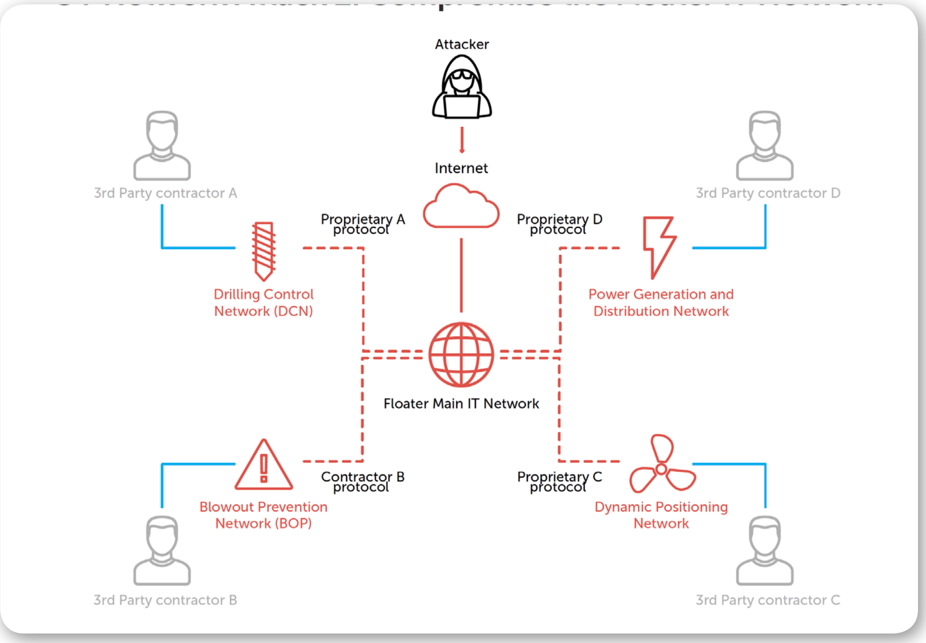

Fig. 3 OT Network Attack 2: Compromise the Floater IT Network

The Tripwire Solution

Preparatory Steps

OT Contractor Approval

The external management of the OT networks usually require a preliminary approval stage. This includes rigorous testing in each vendor's lab to validate that the solution would not cause any operational disruption.

Deployment Process: Network Infrastructure Assessment

Tripwire solutions can be deployed on top of any networking infrastructure. However, Tripwire's recommended best practice is to connect to managed switches capable of relaying replicated traffic over a switch port analyzer (SPAN) port.

Passive monitoring is executed by connecting to SPAN ports on managed switches. This configuration replicates all the traffic these switches relay. When assessing the network to determine which switches to tap, the following considerations are made:

Top priority: Coverage of all traffic that directly involves level one assets, including all connections of programmable logic controllers (PLCs) with level two and above asset such as engineering workstations (EWS), human machine interfaces (HMIs) and various network servers. It is paramount that all traffic that directly impacts physical process is replicated and monitored.

Secondary priority: Following the completion of level-one communication coverage, the assessment team searches for level-two and above, which includes strategic switches, such as intersection points between network segments and working zones. A common example is the intersection point between the IT and OT networks. The number of monitored switches is derived from the network topology. A network that features a main switch that aggregates all the traffic can be monitored from this single point. In a network that is more segmented, or features independent level one clusters, Tripwire can port-mirror each of the relevant switches. The guideline is to balance between maximum coverage and minimum redundant traffic.

The replicated traffic that the SPAN port relays can be pushed through the existing network wiring. However, Tripwire's recommended best practice is to have this data sent through dedicated cabling for the following reasons:

- Physically decoupling the replicated traffic ensures that there is zero impact on the actual traffic.

- Switches, by design, treat SPAN traffic as low priority when there are bandwidth constraints. Routing the monitored traffic to a dedicated physical route ensures that it is always prioritized, ensuring full, real-time visibility.

Deployment Process: From Learning to Operational Mode

Real-Time Network Topology

Initially, Tripwire is configured to run in learning mode. During this time, it learns the networks' standard behavior and establishes a comprehensive behavioral baseline. This learning period enables the Tripwire team to review aggregated findings with the customer and to share immediate insights. These insights cover various aspects, from pure security findings such as insecure remote connections, inadequate segmentation or week passwords, to various network misconfigurations that can impact operational workflow.

Network Behavior

Tripwire discovers network assets (PLCs, HMIs, EWSs and networking gear), gathers detailed data about each asset and profiles the communication patterns between assets each time they communicate. Different assets generate traffic in varying time intervals depending on the specific function and environment. The common time frame that is required for the entire set of OT assets to generate their routine traffic is approximately 2–3 weeks.

Anomaly Detection

Once the learning mode is completed, Tripwire shifts into operational mode where it raises an alert when it detects deviations from the baseline, critical changes (such as PLC configuration download or mode change) or distinct malicious activity. All OT network data is now visible and controlled from a single screen, enabling the rig contractor to track changes and respond to security and operational alerts.

End-to-End Security

During the learning period, it is important to acknowledge the possibility that the environment might be already compromised. The Tripwire deployment team ensures that any malicious presence is detected and eliminated, so that it is not incorporated into the baseline.

Deployment Process: Connect to Security Operations Center

The final deployment step is to extend the successful on-site installation to a central site management interface, where the customer can gain full view of the security posture across multiple vessels.

If the vessels on a rig contractor's fleet communicate with the onshore HQ via satellite connection (satcom), Tripwire runs on top of the existing satcom network to provide a consolidated multi-site view. Tripwire can utilize a proprietary approach to overcome two important satcom constraints—relatively low-bandwidth and frequently-dropped connections.

The data Tripwire generates on site is continuously replicated and sent through existing satcoms to the Tripwire Industrial Visibility Management Hub residing in the rig contractors' onshore security operations center (SOC).

Tripwire Industrial Visibility Management Hub is a central management console deployed in SOCs that provides a single aggregation and management interface across multiple remote sites.

Conclusion

It is only through visibility and control of all assets and traffic that a true shift in security posture can occur. Tripwire rises to this challenge with fully-integrated solutions that provide security insights to enhance the network's security hygiene, advanced filters for proactive threat hunting within the network, real-time anomaly detection that pinpoints any critical changes in network traffic and monitoring for remote connections.

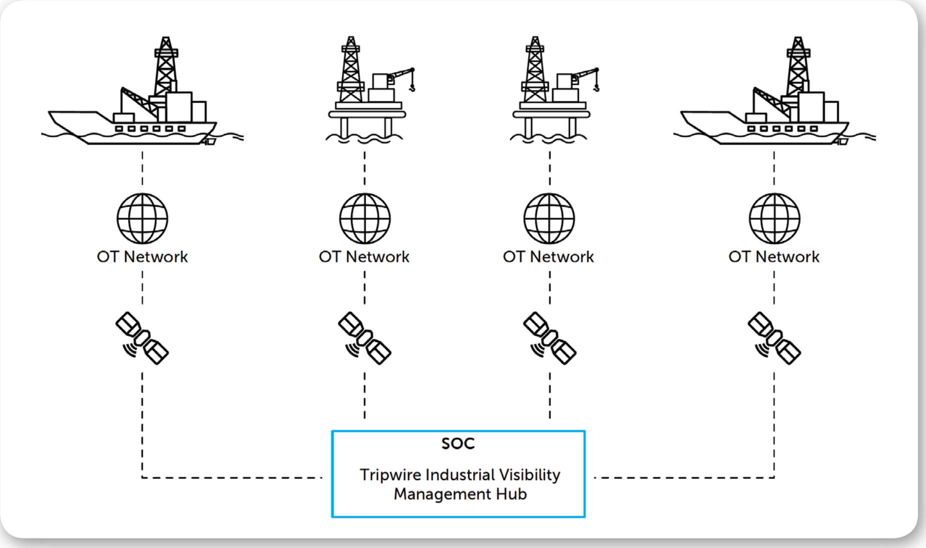

Fig. 4 Vessels connected to Tripwire Industrial Visibility Management Hub.

As a Belden company, Tripwire is uniquely positioned to bridge the cybersecurity gap between your IT and OT environments. Tripwire solutions integrate seamlessly with the industrial products you already have in play, like Tofino firewalls and Hirschmann switches.

tripwire®

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

The State of Security: **Security news, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook