Overcoming Network Challenges in Oil and Gas

ARC White Paper
November 2021

Managing the multiple layers of networks that span a typical oil and gas enterprise is a daunting task. Complexity feeds confusion, delaying proper responses and mitigation and threatens critical data flow.

By Mark Sen Gupta
Research Director,
ARC Advisory Group

ARC Advisory Group

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY

CONTENTS

Executive Overview

Significant technological and external market pressures continue to reshape how the oil and gas industry does business. Technologies are transforming companies into true digital enterprises. Field sensors on platforms, digital twins and seismic models send massive datasets for collaboration amongst global experts to optimize production, processing, and transport. The digital transformation that started decades ago with the connection of key assets to information networks continues to accelerate the convergence of information technology (IT) and operational technology (OT) domains.

The role of the CIO has transformed. Companies also need to understand the threat plane for every device and access point from headquarters' work teams to the most remote refineries and processing plants. The CIO position has become more central in operations planning and execution than at any time in the past.

Critical data from production sites and manufacturing facilities now filter up through the enterprise networks, competing for bandwidth with traditional office traffic. IT must maintain the enterprise networks to ensure all users' digital experiences are performant, but IT can't do that if it can't monitor the networks properly. Visibility is key.

The role of the CIO has transformed. Companies also need to understand the threat surface for every device and access point from headquarter's work teams to the most remote refineries and processing plants. The CIO position has become more central in operations planning and execution than at any time in the past.

Networking in Oil and Gas

Genesis of the Challenges

Networking in oil and gas companies began long before IT came into its own. Leading companies began connecting their assets using modems and telephone lines back in the 1960s. Programmable logic controllers (PLCs) began with point-to-point serial communications and soon implemented multidrop networking in the 1970s. Also in the 1970s, oil and gas companies began implementing distributed control systems (DCSs) that had embedded proprietary networks of their own. These early networks were simple,

isolated, and robust. Industrial control systems support organizations sprung up to maintain and implement these networks.

These industrial network implementations never interacted with the mainframes and minicomputers that were used by back-office staff. The 1980s saw the introduction of the personal computer (PC) for the office environment. The networks implemented for the office met different needs, resulting in a different path. Ethernet slowly made its way into the office as PCs began to replace the dedicated terminals. Ethernet proliferated throughout the office and beyond. Companies quickly realized the value of the connected office worker, and industry responded by quickly adopting Ethernet as the network of choice.

Technology Convergence Increases Burden

The 1990s witnessed the adoption of Ethernet in the industrial space. PLCs and DCSs adopted Ethernet more universally. SCADA systems, HMI software and DCS hardware began to adopt PC technology as an integral part of their architectures. Unlike office networks, industrial networks remained the responsibility of OT professionals.

As bandwidth became a concern, OT networks began implementing routers and switches. Soon, workers at large-scale OT installations like refineries began requesting data from field devices remotely. Cybersecurity grew as a concern, so OT professionals responded with firewalls and demilitarized zones to secure the industrial network.

Depending on the company, an upstream division may have a different approach to IT/OT network implementations than the midstream or downstream divisions. Many upstream and midstream organizations treat the SCADA server system as part of the IT organization due to the intimate relationship with finance and leave the field networks to an OT group. Downstream OT networks have application servers like SCADA, advanced process control, and process historians, all under OT's purview.

It was also in the 1990s that IT began to clash with OT concerning who had dominion over what. Routers are routers. Switches are switches. Why not push tried-and-true IT policies into the OT space? The challenges and misunderstandings revolve around priorities. IT favors confidentiality over integrity and availability, while OT favored the reverse. If a computer or network goes down on the business network, people were inconvenienced. If

that happens on an OT network, the company might make the evening news. This clash led to conflict between the two camps.

Getting Cloudy

Companies began looking for ways to improve their business processes and found that OT systems had valuable data. Creative companies began requesting data from control systems and lab systems for enterprise resource planning (ERP) systems and accounting systems. Some companies began to send data back down to the control systems in order to connect orders to production. This presented a challenge to OT from a security perspective, but it also challenged IT from a bandwidth perspective.

Organizations, especially large enterprises, now recognize the benefits of moving from large on-premise data centers to cloud implementations. The move was slow but has become quite common for many business applications, like ERP. However, the cloud hasn't replaced all the company data centers. Adoption of cloud technologies in the OT domain has lagged the business domain over concerns of security and data ownership. With a growing reliance on software for enhancing control system performance, OT data centers continue to be sizable especially in downstream processes. This has begun to change as many OT vendors offer cloud solutions to OT problems. Some OT cloud solutions connect outside the company's network, while others rely on their own corporate network to handle the large amount of data being transferred. This has created more competition for bandwidth and increased the criticality of the IT infrastructure to the company's bottom line. This also puts the IT network on a critical path for OT.

Threats Abound

Viruses and malware have plagued IT for decades. The use of off-the-shelf technology for OT complicated the management of OT networks. Lately, nation-state attacks and cyber criminals have begun to target corporations with sophisticated attacks and some very specific malware. Examples include Stuxnet and Triton. Other vulnerabilities may just arise from lack of oversight, like the recent attack on the Oldsmar, Florida water treatment plant. Some of these attacks don't target the OT networks, like the recent case of Colonial Pipeline, which recently paid $4.4 million in a ransomware attack to restore its business network and resume financial operations. Regardless of the purpose, companies rely on IT to monitor and protect from such threats. OT does, too, as IT provides a crucial layer of protection.

Remote Access: from Luxury to Necessity

Remote access to the corporate network had been reserved for a select few -- sales, some corporate staff, and a handful of engineers. Over time, this list grew to include select vendors. The pandemic created a seismic shift in the numbers and types of workers requiring remote access. This quickly became an overwhelming headache to many unprepared IT departments. OT personnel needed help as well, and IT and OT worked together to solve the immediate need. This cooperation is the latest in a growing recognition that IT and OT must cooperate to meet corporate goals. There is a natural synergy, but there must be a respect for the different departmental goals.

Case Studies

Case Study 1: Responding to the Growing Demand for Insights and Action

An international energy and chemical company recently shared its experience in managing its networks. IT supports all IT-related functions for the company's 125,000 employees and all business processes worldwide. Like most larger companies, they have gone through the outsourcing of IT infrastructure and have dealt with challenges of being unable to provide timely incident response. As a result, this company decided to bring the monitoring/troubleshooting function in-house to improve response and "get rid of blame game" among contractors.

One of the goals of the new arrangement was to increase collaboration among the people who knew data (people from both the vendors and the company) to achieve quicker incident triage and resolution. The company then invested in its own tools. In this case, the company invested in Riverbed's Unified Network Performance Management solutions. Deploying this solution led to a 25 percent decrease in major incidents year-over-year for the company.

The company started down this route several years ago. When the COVID pandemic hit, executives began asking where are my people, where are they connecting, and are they productive? Because of its investments in the Riverbed tools, IT was able to answer these questions and ensure that adequate levels of network service were available. IT's response to the pandemic

prompted the company's CEO, to comment during the third quarter update to Wall Street that IT is the hero because IT kept the company up and running while everyone was out of the office. The company's global monitoring operations manager credits that to the IT personnel behind the scenes and the decisions made prior to the pandemic.

The company sees the lines between business and IT blurring -- IT is essential to business. It also sees the pace of change and complexity of underlying IT increasing. Business wants IT to just work, like electricity. Data has become king in many ways and is the pathway to information. The key challenge for IT operations in the future is how to meet the new demands without increasing headcount and costs. The company believes visibility is key because one can't manage what one can't see. As such, it is focused on smart tooling to turn data into useful information. The company is also looking to automate more of its IT processes.

Case Study 2: Offshore Drillers need Reliable Connectivity and High Network Performance for Critical Applications

For drilling contractors, every aspect of the business requires fast access to up-to-date data. Communications standards for rigs are extremely high. If data stops flowing or IP phones stop working, the rig has to shut down. That's costly. Oil-and-gas operators pay upwards of $1 million a day to rent a rig.

Unlike businesses operating on land, rigs generally keep the same equipment for 10 or more years. When it comes time to refresh above-deck and below-deck networks on rigs and offices, they need a solution that can adapt to meet changing business demands.

RigNet, a leading global provider of offshore drilling services required a reliable WAN for emergency communications as well as cloud services like SAP and Microsoft 365. Suppliers aboard the provider's rigs need to connect to their own applications. Crewmembers working 28 days at a time appreciate access to the network for personal use.

To meet the needs of the customers, suppliers, and crews, the goal was to double each rig's bandwidth without doubling costs. The challenge was how to push more data on to the network without compromising performance.

Despite the complexity of ocean deployment—including two weeks of COVID-19 quarantine before engineers boarded helicopters—the solution was ready to use in just four months. Riverbed Professional Services worked side-by-side with RigNet personnel so they could learn and document best practices. As a result, the customer gained expertise and confidence to bring a critical solution to the front line.

Managing service quality in a worldwide network is complicated, even more so in harsh ocean conditions with ships in motion. When rigs cross network boundaries or performance starts to decline, the Riverbed SD-WAN automatically switches to the best transport based on performance SLAs and real-time circuit conditions. This maintains a near-seamless user experience.

Offshore drilling companies look for ways to relieve crewmembers' stress and improve quality of life. By optimizing WAN bandwidth, the Riverbed solution also helps crew members stay connected with friends and family. They appreciate having the network performance needed to video chat, watch movies, and even play games. It's a morale-builder and a competitive advantage for recruitment and retention.

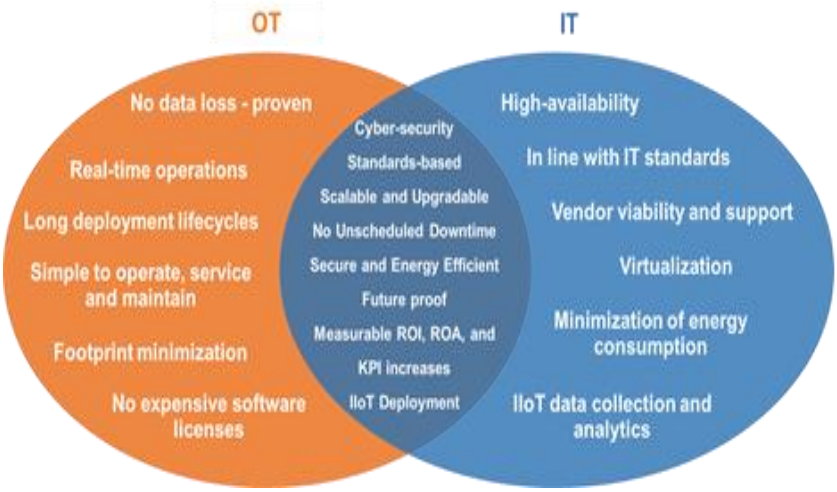
Crewmember satisfaction is so crucial on rigs, in fact, that some customers give personnel a direct line to the CEO for complaints. The Riverbed solution helps manage service quality because it provides visibility into all network activity from a single portal. Personnel can monitor service quality for users, and even see detailed stats like the number of people on Microsoft 365, FaceTime, or YouTube.

The oil-and-gas industry is marked by frequent mergers and acquisitions. RigNet's managed service reduces the time to onboard a new location to the network from weeks to hours. In terms of challenging network conditions, oil rigs are similar to the International Space Station. Riverbed SD-WAN helps make the best use of the customers' bandwidth by combining all the techniques—SD-WAN, WAN optimization, SaaS acceleration, and advanced security—in one device.

Summary

The forces of digitization and digital transformation demand all networks be performant and available. OT data demands have expanded beyond the

manufacturing "floor" and have proportionately become dependent on IT for its success. IT, as the Global Monitoring Operations Manager mentioned, is essential to all aspects of business. Solutions, like those from Riverbed, provide the needed visibility and analytics that allow IT departments to identify and address problems quickly, maintain security, and optimize network traffic for the best digital experiences for end users and maximum productivity for the organization. OT should embrace greater collaboration with IT to ensure its own success. IT needs to understand the needs of OT and the benefits OT provides to the business.



With Convergence, IT and OT Share common Needs

Almost 70 percent of companies believe they are already on IT/OT cybersecurity convergence journeys, with a large percentage indicating that they were already converged. ARC addresses this issue through three different convergence models -- collaboration, integration, and unification. These models reflect tradeoffs between convergence and isolation goals. ARC also emphasizes the need for strategies that incorporate all these models. The individual models provide a basis for establishing site-specific convergence goals and mile markers for journeys to fully unified programs.

ARC research consistently shows that most OT security professionals recognize the limitations of isolation-based strategies. Sophisticated attackers can still find ways into OT systems, and management of these compromises requires more advanced solutions and external support. Demands for connectivity are also growing, requiring investments in better management of privileged access and security of external systems and devices. The major concern is to ensure that OT has a proper role in decisions about how IT technologies are applied to ensure that basic OT constraints are respected.

The reality of digital transformation and the underlying technologies demand a one-ness or cohesiveness within the network for resiliency and integrity. Following a continuous improvement methodology for organizational design can provide a systematic and rigorous way to approach a redesign effort. It makes little sense to maintain networks as uniquely separate. Recognize the synergies and embrace the commonality.

Analyst: Mark Sen Gupta
Editor: Larry O'Brien

Acronym Reference:

ALM	Asset Lifecycle Management
APM	Asset Performance Management
CPAS	Collaborative Process Automation System
CMM	Collaborative Management Model
CPM	Collaborative Production Management
CRM	Customer Relationship Management
DCS	Distributed Control System
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
MES	Manufacturing Execution System
OT	Operational Technology
PAM	Plant Asset Management
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
POC	Proof of Concept
ROA	Return on Assets
SCM	Supply Chain Management
WMS	Warehouse Management System

3 ALLIED DRIVE DEDHAM, MA 02026 USA 781-471-1000