OVERCOMING NETWORK CHALLENGES IN MINING

ARC White Paper
January 2022

Managing the multiple layers of networks that span multiple continents is a daunting task. Complexity feeds confusion, delaying proper responses and mitigation and threatens critical data flow. The boom-and-bust cycle of the mining industry demands efficiency. An efficiency that demands world-class communication.

By Mark Sen Gupta
Research Director,
ARC Advisory Group

ARC
Advisory Group

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY

CONTENTS

Executive Overview

Previously, we discussed networking challenges in the oil and gas industry. Significant technological and external market pressures continue to reshape how the mining industry does business, as well. Technologies are also transforming mining companies into a true digital enterprise. Field sensors on mobile equipment, digital twins, and production data send massive datasets for collaboration with experts globally to optimize production, processing, and transport. The digital transformation of the mining industry continues to accelerate with the convergence of information technology (IT) and operational technology (OT).

IT must maintain the enterprise networks to ensure all user experiences are performant and secure. However, IT can't do that if it can't monitor the networks completely. Visibility to network dynamics is crucial to maintain a performant network.

Critical data from the pit and processing sites filter up through the enterprise networks, competing for bandwidth with traditional office traffic. IT must maintain the enterprise networks to ensure all user experiences are performant and secure. However, IT can't do that if it can't monitor the networks completely. Visibility into current network dynamics is crucial to maintain a performant network.

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

Networking in Mining

Genesis of the Challenges

Much like other industries, networking in mining companies began long before IT came into its own. Programmable logic controllers (PLCs) began with point-to-point serial communications and soon implemented multidrop networking in the 1970s. These early networks were simple, isolated, and robust. Industrial control systems support organizations sprung up to maintain and implement these networks.

The 1980s saw the introduction of the personal computer (PC) for the office environment. The networks implemented for the office met different needs and went a different course. Ethernet slowly made its way into the office as PCs began to replace the dedicated terminals and proliferate throughout the office. Companies quickly realized the value of the connected office worker, and industry responded by quickly adopting Ethernet as the network of choice.

Technology Convergence Brings Challenges

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

As bandwidth became a concern, OT networks began implementing routers and switches. Soon, workers remote from the OT installations, but still on-site, began requesting data from field devices. Cybersecurity grew as a concern, so OT professionals responded with firewalls and demilitarized zones to secure the industrial network.

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 bad feelings amongst the two camps.

The Challenges get 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 mobile and immobile mining equipment for maintenance, enterprise resource planning (ERP) systems, and other accounting systems. This presented a challenge to OT from a security perspective, but it also challenged IT from a bandwidth and security perspective.

Organizations, especially large enterprises, now recognize the benefits of moving from large on-premises data centers to cloud implementations. The

move was slow but has become quite common for many business applications, like ERP and office applications. However, the cloud hasn't replaced all the company data centers. Some OT applications continue to operate in onsite data centers. Some OT cloud solutions connect outside the company's network, while others rely on the company 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.

Challenges from the Internet

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 organized crime syndicates have begun to target corporations with sophisticated attacks and some very specific malware. Examples include Stuxnet and Triton. Other vulnerabilities may just be lack of oversight like in the case of recent attack on the Oldsmar, Florida water treatment plant. Some of these attacks don't target the OT networks, as in the recent case of Colonial Pipeline which recently paid $4.4 million in a ransomware attack in order to restore its business network and resume financial operations. Closer to home, the recent attack on Weir is another example of a growing trend of cyberattacks in the mining industry, as attackers look to exploit outdated cybersecurity systems that struggle to keep up with such a rapidly changing industry. The latest threat is a vulnerability in a popular Java Log4j library. Each company relies upon IT to monitor and protect the company from such threats. OT does, too, as it provides a crucial layer of protection.

Remote Access goes from Luxury to Bare Necessity

Remote access to the corporate network had been reserved for a select few; sales, some corporate staff, and a handful of engineers. This had been growing over time 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: Managing, Monitoring, and Optimizing a Complex Hybrid Network

One of the world's largest mining and resources company operates over 100 sites around the world including some in extremely remote locations. The company has employed Riverbed solutions for the last ten years to help manage and troubleshoot its network issues. This has resulted in fast, accurate performance resolution for both applications and network.

It faced a number of challenges regarding the management of its huge network of varying types. The main challenges were managing and troubleshooting network connectivity issues; reducing latency across diverse environments; maintaining user experience, wherever they are located; and unifying visibility across different regional carriers for a wholistic view.

The nature of its global business requires the ability to support thousands of users across some of the world's remotest locations. Some of the mission-critical applications it runs involve the transfer of vast quantities of data and immense graphics files. The company also needs to support mine workers with high performance entertainment for off-shift relaxation and enable them to keep in touch with family and friends at home.

Performance of the enterprise network is just as critical to its over 100 operational sites as it is to its head office staff. One of the main challenges is identifying the causes of performance issues accurately and quickly with the goal of resolving them before they impact on the productivity of its global user community.

Like other large mining organizations, the company operates a series of diverse environments, including a range of private and public clouds, on-premises equipment, and SaaS applications. All of which can make identifying and resolving network and application performance issues a complex and lengthy procedure, without full visibility and the ability to filter data quickly to identify root causes.

With multiple network carriers involved and information and communication technology (ICT) outsourced to service providers, the company needs to hold everyone in line with a single version of truth. This means having accurate data about the root causes of performance degradation to best manage supplier service level agreements (SLAs) – keeping vendors honest and avoiding unproductive finger-pointing and wasted time when issues do arise.

The company turned to its long-term technology partner Riverbed. Together with the company's global network provider, Riverbed developed a solution based on different modules within Riverbed's Unified NPM platform. The entire suite of tools is available via the Riverbed Portal, which provides the "big picture" with integrated network and application insights.

The solution helped provide a detailed analysis of the performance and utilization of the company's communications and collaboration platforms early, when the COVID pandemic triggered migration to a remote workforce. By charting pre- and post-pandemic usage, it illustrated the patterns of traffic for future capacity planning. When a site's primary network link failed, Unified NPM tools quickly identified and resolved performance, routing, and utilization issues on several backup links throughout the outage. Unified NPM tools also helped with network optimization when numerous sites in a remote region experienced performance issues.

The networks and applications support teams now have over 50 dashboards to give them full visibility and insight over their infrastructure. Typically, the dashboards are role-based – either by application or site. Others provide greater overview of groups of applications or regions.

Enhanced reporting allows IT to observe exactly what is happening over the network at any given time, including how users and applications are actually using data. IT can then identify the busiest links and those performing the worst. The platform is also aids with capacity planning – enabling the network team to optimize links to different applications and volumes of traffic. Monthly reports enable them to look back at trending analysis and look forward for capacity provisioning.

The principal objective the IT team is achieving with the help of Unified NPM is to detect, diagnose and resolve performance issues before users are even aware of them. This enables them to provide an overall better user experience.

Case Study 2: Improving Application Performance

A global mining services company of over 8000 employees, IT must ensure its customers have an excellent IT experience. With sites throughout the world, ensuring that connectivity is performant regardless of the technology utilized, is a challenge. Because mines are not always located near population hubs, the company must rely on networking technologies like cellular and satellite for connectivity. IT is tasked with ensuring personnel at these sites have as good, or nearly as good an experience as at a main office. In order to do so, IT must monitor the network and optimize it.

The company's manager of technology planning and architecture shared that maintaining performance of the corporate network in 12 different countries across four continents presented quite a challenge. It has standardized on cloud applications like Microsoft 365, SharePoint, and Teams so all of the field offices must also use these applications. Due to the nature of its projects, field offices must be established quickly, but only for the duration of the project. This means that more permanent, high bandwidth networking solutions aren't deployed. However, IT must ensure network performance levels at or as near to the office environment. This not only includes the office applications, but the engineering and safety collaboration, as well. To accomplish this, the company has deployed Riverbed Technology's SteelHead and SaaS Accelerator.

While the company had a significant SteelHead deployment, it found the addition of the SaaS Accelerator boosted the user experience by around 50 percent. Interestingly, the technology manager recounted a meeting with executives to discuss the initial proof-of-concept trial of the SaaS Accelerator, the team accidently disabled the WAN optimization. The users immediately began calling the help desk because the loss of performance was so noticeable. This optimization opens up bandwidth for other applications and is especially crucial for remote locations.
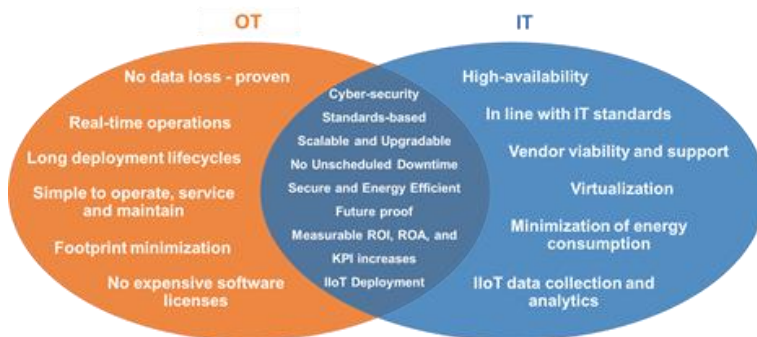
As a result of its successes, the company has begun a pilot of the SDWAN solutions in order to help with failover, load link aggregations, and optimization. Due to the nature of the solution, it will be able to simplify operations by utilizing one device platform for the three solutions: SD-WAN, SteelHead, and SaaS Acceleration. The company believes this will give IT end-to-end visibility of its network and quicker response to issues.

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 has proportionately become dependent on IT for its success. IT is essential to business, all aspects of business. Solutions, like those from Riverbed, provide the needed visibility and analytics that allow IT departments to identify and problems quickly, maintain security, and optimize network traffic for the best experience. OT departments must 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.

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.

With Convergence, IT and OT Share common Needs

ARC research consistently shows that most OT security people 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 sepa-rate. Recognize the synergies and embrace the commonality.

Analyst: Mark Sen Gupta

Editor: Larry O'Brien

Acronym Reference:

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

ARC
arcweb.com

3 Allied Drive Dedham, MA 02026 USA   781-471-1000

USA | Germany | Japan | Korea | China | India | Singapore | Bahrain & UAE | Brazil