IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Moxa

IT/OT convergence is the path to achieving operational resilience, but to do so requires a robust, secure, industrial network backbone that is evolving in capabilities and scale compared to the past. Combining purpose-built OT networking and cybersecurity is one path to ensuring success and avoiding unexpected roadblocks.

Building Operational Resilience with a Secure Industrial Network Backbone

April 2022

Written by: Jonathan Lang, Research Director, Worldwide IT/OT Convergence Strategies

Introduction

For many years, the primary objective of industrial enterprises was to become more efficient. Process automation, vertically integrated operational technology (OT) systems, and fixed processes enabled this efficiency through speed and repeatability.

Now, shifting market conditions and customer requirements, coupled with new technologies, are causing a shift to focus on adding resiliency – or the ability to predict and react to changes without disruption – to operations without sacrificing efficiency.

Technology is the main method enterprises are using to become more resilient, and integration of IT and OT systems is the method that they use to take advantage of technology capabilities inside operations, remotely, and in the cloud. This convergence has been accelerated dramatically by COVID-19, as companies look to deploy more remote and contactless processes and working models in their businesses. The need to build operational resilience has never been higher, and companies in turn are accelerating their convergence of IT and OT systems to achieve it.

AT A GLANCE

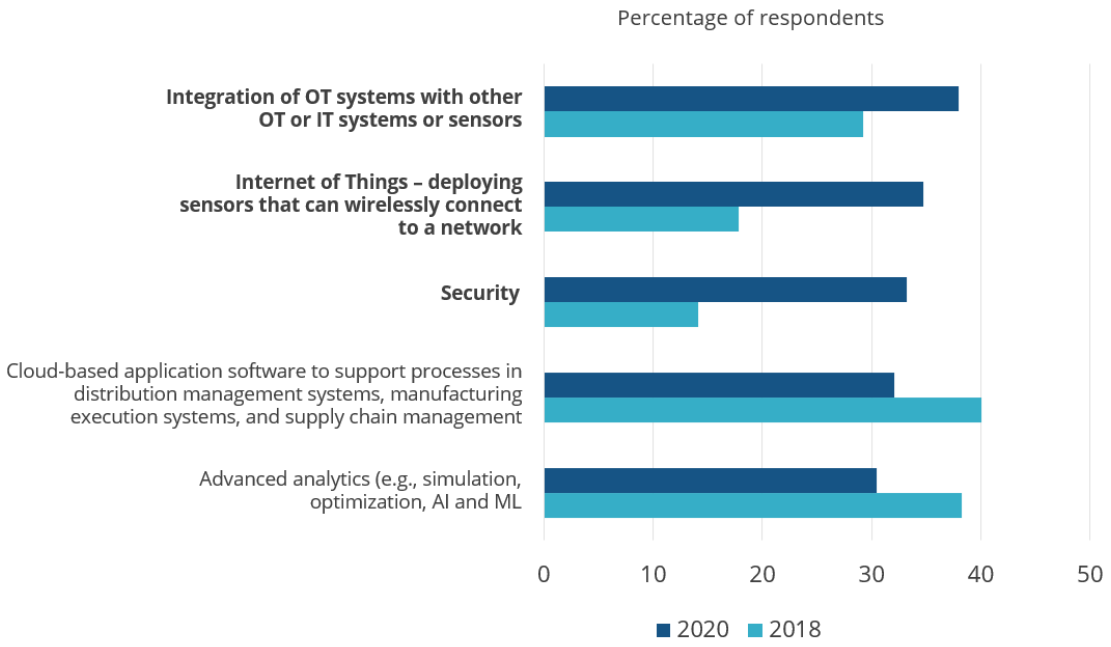
KEY TAKEAWAYS

- IT and OT convergence is accelerating, creating urgency for a robust and secure industrial network
- OT networks and cybersecurity are unique and complex, requiring industry expertise and capabilities
- To create a future-proof foundation for the future of operations, enterprises must combine expanded networking and purpose-built OT cybersecurity into one capability

According to IDC's 2021 Future of Operations Survey, 34% of organizations are now monitoring and diagnosing almost all of their devices, equipment, assets, facilities, and processes remotely with limited onsite staff. When asked the same question about how they will work 3 years from now, 33.7% will work this way.

This shows that the new working models that have been required due to COVID-19 are here to stay, and the required digital capabilities to support them cannot be ignored by organizations. The shift in necessary capabilities and its impact is reflected in companies' investment priorities.

FIGURE 1: *Investment Priorities for IT-related Initiatives in OT*



Source: IDC's IT/OT Convergence Surveys (n=1,014 , 2020 and n=905, 2018)

In Figure 1, we have the integration of OT systems, traditionally fully-hosted and managed locally at the operational site, with IT systems which exist in the cloud and in enterprise networks, the Internet of Things, and security as the top 3 investment priorities. Compared to 2018, integration of OT and IT systems rose nearly 10% and Internet of Things and security rose nearly 20% each, showing a sharp rise in the speed and importance that companies are requiring secure networking capabilities. In the same survey, more than 30% of organizations are planning to integrate operational data from systems such as a data historian, an industrial control system, and asset management, into their enterprise data governance model for the first time. Clearly, an enhanced, more capable industrial network backbone is now even more critical to business resilience. Prevailing trends outline a need for secure industrial networks in particular:

- **Connections everywhere**. Connectivity is exploding, and more devices require a secure, reliable network to communicate and perform their functions. Companies are moving to more remote monitoring and diagnostic models to reduce unplanned asset downtime, optimize operations including external supply chains, and enhance centralized analytics capabilities.
- **Increasingly borderless connectivity**. Because this connectivity extends outside of operations, air-gapped industrial networks are no longer a viable strategy for keeping operations secure. Cybersecurity is now a critical requirement for OT environments and the networks connecting them outside of the operational environment.
- **Rising network complexity**. The system has become more complex overall, with new devices and software workloads being deployed all the time in operations. In some manufacturing facilities, for example, there may be 5,000 or more network switches and rising. Companies must now balance the cybersecurity risks among the reliability, performance, and productivity requirements in operations. Oftentimes this can result in companies prioritizing highly-visible assets and systems, and neglecting systems which may pose a greater risk but which are less visible.

Calculating and managing risk across these vectors is complex, and the network represents a significant opportunity to deliver that risk assessment as well as harvest the greatest return by focusing on securing network traffic directly. This makes the role of the network and network monitoring more strategic in managing reliability and risk overall.

But the industrial network carries many unique considerations which must be addressed in an effective IT/OT convergence strategy, and which vary considerably compared to managing an IT network:

- **Many unique devices**. Heterogeneous assets and devices running proprietary protocols are challenging. It means that you cannot deploy agented endpoint device security. Even if the security technology can communicate with an asset, it poses too much risk of disruption to the operation of the asset. It also means that security providers must be able to understand the unique communication standards and protocols of OT network traffic from a variety of unique assets and devices with the right context to be accurate. An IT approach to reading common network traffic cannot succeed in the OT environment.
- **Availability is the priority**. In IT security, confidentiality, integrity, and availability, or the CIA triangle, is a common model. But in operations, the CIA triangle must be upside-down because availability is the most important operational objective. That means that networks must always remain operational in this rugged setting. It also means that security cannot actively intervene within the OT network. Therefore, the network devices and management itself are very critical to both reliability and security, reflecting a greater focus in OT security compared to the more endpoint-oriented strategy of an IT network.
- **A secure edge is needed**. The rise in edge devices represents a pathway into the operation. They are being deployed at a high rate and utilize more open architectures and capabilities compared to the vertically-integrated OT devices of the past. These devices must, therefore, be securely developed throughout their lifecycle for both software and hardware elements as well as integrate seamlessly into overall network and security management capabilities.
- **Compliance with existing and emerging standards**. Industry requirements are increasing around standards and cybersecurity capabilities. Anyone supplying these critical infrastructure environments such as energy supply and delivery need to work within them, from hardware and software design all the way through the supply chain. These existing and emerging requirements will vary by country and industry, and enterprises must now consider these at every step of their digital transformation.

The key to successfully navigating the IT/OT convergence necessary for resilient operations is to combine network and security disciplines and capabilities. Too often today, these efforts are pursued in siloes. The result is a general neglect or heavy set of roadblocks for security initiatives. These combined capabilities and efforts must be supported by industry-specialized technologies and partners that understand the unique challenges OT environments face and develop purpose-built products for delivering end-to-end industrial networks, from OT power and connectivity through the edge of the environment. The network infrastructure itself is the essential foundation for secure, resilient, and digitally-transformed operations.

The key to successfully navigate IT/OT convergence necessary for resilient operations is to combine network and security disciplines and capabilities.

Benefits

When delivered effectively, secure industrial networks can give enterprises the confidence and capabilities to advance their IT/OT convergence maturity and realize the benefits of digital transformation. These benefits span people, process, and technology:

- **Unified management** of OT network and cybersecurity in operations ensures staff can monitor OT networks in a scalable way and connect with necessary subject matter experts to identify and remediate real issues. In an un-converged strategy, intrusion detection systems that are not specialized for OT environments result in massive, streaming event logs that overwhelm engineers and administrators, often resulting in real issues being overlooked.
- **Industry-specialized network and security approaches** reduce the work necessary to gain visibility into heterogeneous assets and unique device protocols. This gives a more comprehensive understanding of the threat and network performance landscape, enabling prioritization of risk and remediation. This also reduces the barrier to entry for smaller companies who may not have as many dedicated resources to support network and security initiatives. They are only responsible for the last mile understanding and action.
- **Vetting incoming traffic**. Traffic can flow out of the operation to take advantage of operational data in the cloud, but traffic entering the operation is thoroughly vetted to ensure it does not create any risk of reliability or security impact. This enables confidence and expands the possibilities for remote monitoring and diagnostics as well as other IT and OT-converged capabilities and initiatives, such as integration with supply chain partners.
- **Bandwidth and network reliability as well as security** can support the increasing amount of high-speed traffic inside of operations coming from the explosion of connected assets and new edge compute devices. This removes one bottleneck to scaling IT/OT initiatives and provides the confidence to work with agility when adding, removing, or reconfiguring workloads – a key characteristic of resiliency.
- **Defense in depth**. For critical infrastructure in particular, defense-in-depth approaches are being recommended. A combined network and cybersecurity approach delivers high benefits to this strategy with minimal cost, because security is inherent to the combined system and the devices and components inside it. This is in contrast to expensive, dedicated security systems which provide only one layer of protection.

Trends

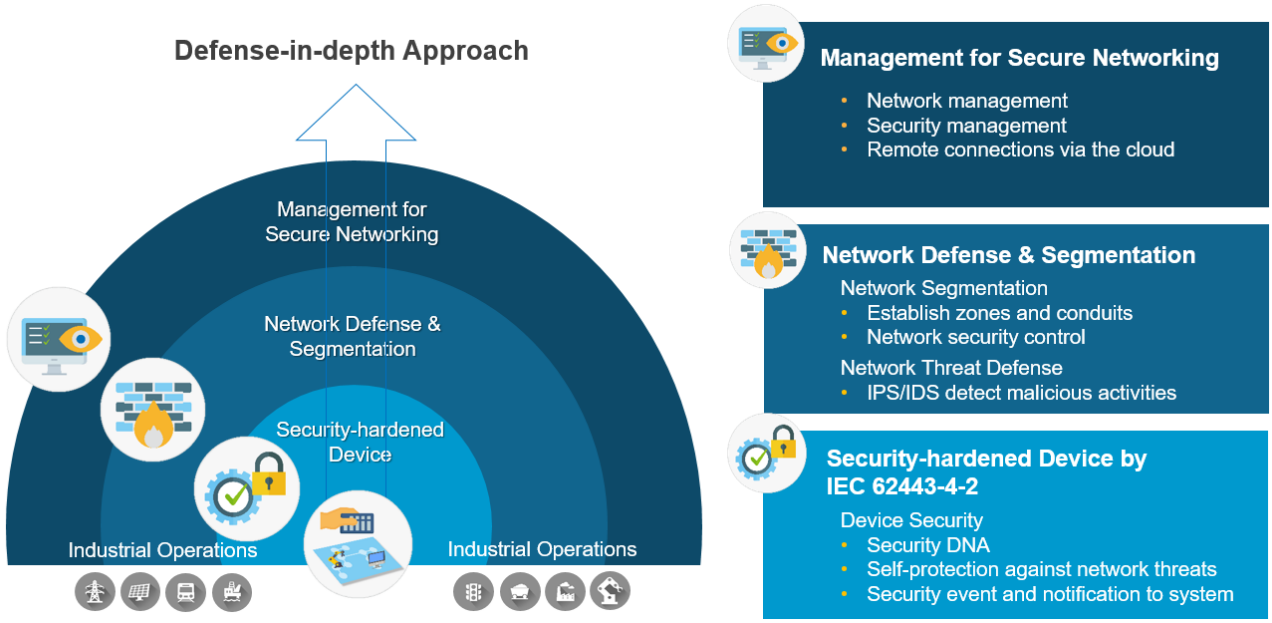
- **Hybrid cloud and containerization** is rising as companies look to build remote operation capabilities. This synchronization between cloud management and local containerized applications and capabilities provides many benefits, but also creates more demand and the need for secure, non-disruptive network connections at the edge of the operation.
- **Smart, connected assets**. Assets are becoming more embedded with intelligence and connectivity and utilizing more common communication capabilities. This improves capabilities for the asset but means there is a need for greater network bandwidth and creates a more complex network landscape to monitor and secure.
- **Increasing focus on critical infrastructure and cybersecurity** due to a rise in attacks. Many companies have advanced their digital transformation capabilities but neglected to mature their cybersecurity capabilities. It will be impossible to bring their security capability up to standard if the technology was developed in isolation from the network and delivered without industry expertise. Additionally, government regulation around critical infrastructure will continue to rise globally and will not be a priority for generalized technology providers.

Moxa's Role

Moxa strives to enable connectivity for the automated world of today and tomorrow while aiming to enhance cybersecurity for industrial automation systems. With a distribution and service network to serve customers in more than 80 countries, Moxa has connected more than 82 million devices worldwide. Its OT experience and domain know-how in vertical markets including rail, power/energy, smart manufacturing, oil and gas, intelligent transport systems (ITS), and marine have spanned more than three decades. This industry knowledge and approach are critical to delivering OT security with fidelity and in alignment with industry requirements. Some quick facts about the company:

Moxa is the world's first IEC 62443-4-1 certified networking solution provider and one of the few suppliers that can offer both networking and cybersecurity solutions purpose-built for OT operations. Moxa's solutions aim to unite networking and OT cybersecurity with layered defense-in-depth protection ranging from security hardened networking devices based on the IEC 62443-4-2 cybersecurity standard, advanced IT and OT network segmentation and threat prevention, and tailored OT deep packet inspection (DPI) featured by industrial intrusion protection system (IPS) protection. These offerings are built with reliability at the forefront and end-to-end connectivity to provide robust hardware, as well as high-performance and dependable networks. Moxa's solutions also enhance visibility with simple management for on-premise and remote management software.

FIGURE 2: *Moxa's Defense-in-depth Approach*



Source: Moxa, 2021

Moxa strictly follows secure by design practices, utilizes distributed OT IPS capabilities — enabled by Moxa's DPI engine — and provides an array of hardened networking portfolios to perfect defending industrial applications in depth. This DPI engine is designed to give users more granular control over network traffic, and also to allow the implementation of agented endpoint device security into OT systems.

Moxa's industrial IPS features OT-centric DPI technology, enhances IT network security visibility, and ultimately helps mitigate risks and protect industrial networks from security threats. Moxa's DPI is capable of identifying multiple

industrial protocols and whitelisting or blacklisting specific functions, such as read or write access. Based on the identified protocol, the industrial IPS can then help to prevent any unauthorized protocols or functions.

Moxa's latest family of future-proof networking solutions is due to launch in 1Q22, and its first IEC 62443-4-2 certified product will be one approach that helps asset owners and system integrators achieve the security requirements for industrial control systems (ICS).

The IEC 62443-4-2 certified product is embedded with security features that are designed to meet security requirements for various applications. Devices with the security capabilities are referred to device security (also known as device hardening). The device security definitions help simplify technical specifications and technology selection. Some other security capabilities include user authentication, the ability to preserve the integrity and confidentiality of data, and an authentication layer for controlling network access. These are standard concepts and features across the consumer and business technology landscape, but have been traditionally lacking in industrial settings. In many cases, default usernames and passwords can be found in industrial settings today with little or nothing in the way of vulnerability management capabilities. Moxa approaches these as basic requirements necessary to ensure a secure, future-proof industrial network backbone.

Challenges and opportunities

- The OT network space has become more competitive due to increased interest from IT network providers as well as new entrants to the market. Moxa's opportunities lie in demonstrating differentiation and industry expertise as well as raising exposure to gain share in this highly competitive market.
- The OT cybersecurity market has also become more competitive with the rise of many new offerings attempting to resolve OT cybersecurity challenges. This is a difficult market in which to gain recognition and adoption. Highlighting customer successes and a track record in OT networking and security is one way to gain recognition. Demonstrating comprehensive, proactive, defense-in-depth capabilities will also help to compete against some of the more fragmented point solution approaches.
- Edge computing providers are offering more proprietary devices to communicate outside the network. These devices and their traffic will need to be incorporated into the overall OT network in a way that will maintain performance and security overall. This will be a moving target for Moxa to support but is well suited to a network-focused security strategy.
- For the OT network, and especially cybersecurity, global enterprises prefer to work with vendors they are already working with and have deep relationships with. It is a difficult space to convince a potential customer to change providers. Partnerships with trusted providers and adherence to various global standards and compliance requirements may alleviate this hesitancy.

Conclusion

IDC believes IT/OT convergence is posing a significant opportunity for enterprises to advance their capabilities and become more resilient and competitive. But it also creates new challenges and breaks old models for operating and securing the OT network. To what extent a vendor can address these unique considerations presented by the OT network while offering the capabilities to support IT/OT convergence, they are positioned to succeed.

About the Analyst

Jonathan Lang, *Research Director, Worldwide IT/OT Convergence Strategies*

Jonathan Lang is Research Director for IDC Manufacturing Insights responsible for the IT/OT Convergence Strategies practice. Mr. Lang's research focuses on digital transformation strategies in environments where operations technologies are deployed including Manufacturing, Utilities, Oil & Gas and Healthcare Provider settings. As IT capabilities redefine and extend the core value drivers of operations technologies, Mr. Lang's research examines strategies, roadmaps, and governance models to drive this convergence and manage the new data and processes it requires.

MESSAGE FROM THE SPONSOR

Networking Evolved, Strengthened Resilience

Moxa is redefining futureproof industrial networks, providing enhanced security, reliability and simplified management to help industrial enterprises overcome roadblocks and achieve operational resilience by combining purpose-built OT networking and cybersecurity. Security, reliability, and simplified management are the three keys to advancing industrial automation to the next stage, and they define Moxa's design DNA which is used to develop its next-generation networking solutions. The recently launched EDS-4000/G4000 Series of futureproof industrial Ethernet switches fully incorporate this DNA of security, reliability, and simplified management

Click here to learn how Moxa's next-generation industrial Ethernet switches, developed according to the IEC 62443-4-1 and compliant with the IEC 62443-4-2 industrial cybersecurity standards, ensure a secure, futureproof industrial network backbone.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Asia/Pacific
83 Clemenceau Avenue
#17-01 UE Square West Wing
Singapore 239920
T 65.6226.0330
Twitter @IDC
idc-insights-community.com
www.idc.com