IT-OT alignment: Convergence isn't the only path Smarter options for operations managers

Your operations, your choice: Converge fully, partially or not at all

White Paper

Alcatel·Lucent Enterprise

Pushing the bounds of operational efficiency with digital automation

Managing operational infrastructure continues to be a challenge. Every enterprise that relies on video surveillance cameras, remote sensors and monitors, automatic switches or one of a dozen other digital systems is facing pressure to use them to do more with less. A stark example of this is in the transportation sector: growing populations[1] are increasing vehicle traffic, forcing transportation departments to look at new ways to more efficiently monitor and manage the flow of traffic on existing road infrastructure.

For many enterprises, digital automation solutions are the answer. In industrial settings, for example, IoT devices are being deployed, including cameras, metering devices, door locks, badge readers, temperature sensors and traffic sensors. Other advanced technologies, including Industry 4.0 applications, advanced edge computing, private 5G networking, AI and machine learning, are being considered to improve both machine-to-machine and machine-to-human communication. Being able to collect and consolidate information from IoT devices, network infrastructure elements, business applications and other systems is important. But even more essential is the capability to communicate this information to people when they need it most.

However, the deployment of more automation solutions creates another challenge. These devices and systems are often mission-critical and life-critical, including water-quality monitors in wastewater treatment facilities, automatic switches for train tracks, asset tracking systems in hospitals, power transformers used by utilities, video surveillance across all verticals and many others. Compromising their functionality, even temporarily, can result in significant monetary losses, legal consequences or even lost lives. To reap the full benefits of automation, sensors, devices, and systems must be on the same network, while remaining properly segmented.

1 https://infrastructurereportcard.org/cat-item/roads-infrastructure/#:~:text=After%20dipping%20drastically%20due%20to,hours%20and%20%24733%20in%202023

Networking: A necessary foundation, but growing in complexity

Effectively integrating digital automation technologies can be complicated. Many devices rely on air-gapped operational systems for security-by-obscurity. Often, these devices have no inherent security and networking them necessitates breaking down existing silos and addressing security concerns at the network level. But the teams that deploy, manage and monitor them have little or no network cybersecurity expertise.

Most workers responsible for these devices also have multiple other responsibilities, limiting the time and attention they can give to network management. Managing operational devices requires a different skillset from deploying, managing and monitoring the networks required to connect them. Effectively managing a network of operational technologies requires an understanding of both ecosystems.

"A flexible, resilient and reliable network infrastructure is critical to ensuring that the Liverpool City Region can run its services efficiently, on a 24hour basis, 365 days a year. The consolidation of networks has allowed us to maximise the return on our investment while underpinning the provision of diverse services to the region's public." -- Ian Hawkins, Head of IT, Liverpool City Region

Read case study

Cost must also be considered. Organizations must account for not only the initial capital investment associated with building the network but also the complete lifecycle cost of the devices and any accompanying network infrastructure.

"Alcatel-Lucent Enterprise's solution has been a game-changer for our efficiency and bottom line, helping us reduce costs by up to 15%. Our services run with near-zero downtime, providing a smoother, more reliable experience to our customers."
-- Aripin, Chief Executive Officer, CGS

Read case study

For enterprises to efficiently leverage digital automation, networks must be easy to deploy, maintain and manage. These networks must enable seamless sharing of real-time information, ensure operational uptime, include cybersecurity measures to prevent breaches and gate access without restricting operational staff.

Deploying the right network architecture to meet operational needs and regulatory requirements of operational teams is the key. Enterprises must determine the network components needed, and whether a fully separate, a partly merged or a fully merged network will best suit their operation.

Networking must be done right the first time

Properly deployed, the right network infrastructure will give technical directors, specialized engineers and system operators the tools they need for easier operation, management and maintenance of the operational systems they work with. But because operational systems are often industry-specific or even machine-specific, effectively networking operational technologies can be quite difficult. Successful networking of any digital automation solution must:

- Ensure operational uptime
- Integrate and maintain cybersecurity without impeding operations
- Provide a cost-effective solution that considers total lifecycle costs

Efficiency cannot come at the cost of uptime

Maintaining operational uptime is a significant challenge, as many operational technologies are associated with mission- and life-critical operations that cannot fail even temporarily. Asset tracking in a hospital, for example, enables staff to quickly find medical equipment, which can often be the difference between life and death. Traffic light operation, if it should fail or even work imperfectly, can cause slowdowns or put motorists in danger.

Regardless of the vertical market application, all devices need continuous uptime, significant bandwidth and seamless connectivity to transmit large amounts of data. Some operate in harsh environments, including the sides of highways, mines or in office settings where they could be damaged or stolen. To achieve the ideal 99.999% uptime, networks may require significant infrastructure investment and products built on standards-based protocols to create highly available networks capable of using every link simultaneously.

For some industries, uptime is both a practical and legal requirement. Casinos, for example, are required to always have live video surveillance. If video feeds are down, they can't operate. Therefore, continuous uptime cannot be achieved by simply setting up a network and walking away. Even the most robust digital infrastructure will require updating and troubleshooting as it ages, so any network solution must account for applying updates in a way that doesn't compromise uptime.

> *"A casino environment is challenging for many different reasons. We have a collision of different needs from our secured gaming systems, to our enterprise applications, including our guests. So we have to be able to secure and support so many different responsibilities." -- Dom Waters, Director of IT Infrastructure, Cordish Gaming*
>
> Read case study

Security-by-obscurity is no longer possible

Digital automation creates efficiency using interconnectivity. But networking traditionally isolated systems can create security risks by exposing devices to threats they were not designed to mitigate. For example, many of the IoT devices and systems used to enable automation have no built-in security, and the Supervisory Control and Data Acquisition (SCADA) architecture that is commonly used in industrial settings to monitor and control these devices lacks any inherent security.

Making the security challenge worse, operational teams often lack the training to build and run an effective network cybersecurity program. Enabling remote access for management and maintenance procedures could become access from anywhere for cyber criminals. As a result, even simple security breaches could compromise mission-critical systems, and operational teams may not have the training to notice and mitigate them.

The right network should reduce long-term costs

Network infrastructure costs present a different challenge. Networking operational devices can reduce redundant spending on multiple management systems and improve overall operational efficiency, offering potentially substantial cost savings. The challenge is that organizations, operating on limited budgets, must nevertheless deploy sufficiently well-designed and thorough network infrastructures to ensure maximum uptime and cybersecurity. This cannot be achieved when organizations weigh potential solutions based solely on capital expenditure (CapEx) costs.

The ideal solution will provide the lowest total cost of ownership (TCO) based on the right balance of both CapEx and operational costs over the projected life of the network. Therefore, costs should be considered against the network's ability to scale to the enterprise's present and future needs. This is especially important as the cost of many operational devices is amortized over years or decades.

Deploy the right tools in the right network

The best solution to the multi-faceted challenges facing operations teams is a network infrastructure that is as simple as possible to deploy, manage and maintain. Choosing the right components of that network will affect how well it delivers its intended value.

Fast device deployment improves scalability and flexibility, enabling enterprises to extend automation capabilities to more devices and locations as needed. Simplified device management and oversight ensure issues are captured and resolved more quickly and efficiently, maximizing operational uptime without adding costs in staff or training. Constant access to actionable data on device activity and network performance using predictive maintenance solutions reduces downtime and cuts maintenance costs, while the ability to apply data-driven upgrades maintains optimal performance and minimizes unnecessary expenditures.

All these objectives can be achieved with a network comprised of several key components:

- **Wired and wireless networks** with automated IoT device detection, pre-programmable device classification and segmentation simplify deployment and management, extending seamlessly from the data center through the enterprise and to the industrial floor, where ruggedized equipment ensures availability for critical services.
- **Private 5G** provides enterprises with the high bandwidth and ultra-low latency needed to support many industrial devices, such as IoT and Industry 4.0 technologies, advanced robotics and digital twins. It can also complement, extend and enhance existing and new Wi-Fi networks, particularly in uncarpeted and remote areas such as manufacturing facilities, airports, ports, mining sites and oil refineries.
- **A Zero-Trust network architecture** (ZTNA) treats every device on the network as potentially hostile to enhance security without increasing complexity.
- **Unified network management** creates a holistic view and control of every device in the network with synchronous cybersecurity to eliminate gaps by leveraging standardized and interoperable technologies.
- **Continuous monitoring tools** that use integrated AI and machine learning can anticipate and fix network problems to minimize network downtime and optimize performance.
- **Simple configuration and troubleshooting tools** allow even team members with no IT training or expertise to identify and resolve operational slowdowns and issues quickly and easily.
- **Asset tracking** keeps operations teams updated on the geolocation of shared assets and required maintenance.
- **Workflow engines** streamline operational oversight and facilitate more accurate and timely decision-making and issue resolution. They can also enhance responsiveness with automated agile communications in time-sensitive situations, such as leaks or breakdowns, for reduced total cost of ownership over the lifespan of the system.

Equally important as the network components is the network structure. Three architecture options are available to enable enterprises to achieve maximum uptime, security and cost-efficiency.

Fully independent networks provide security with complexity

A fully independent operations network is the most complex to build and deploy but minimizes security risks and exposures and can be a steppingstone to greater network integration. With this architecture, enterprises can converge OT silos, such as building management systems, video surveillance, access control, IoT sensors and alarm systems, and share data between them more effectively.

Fully independent and often at least partially air-gapped networks are the most inherently secure. Enterprises get the greatest control over the infrastructure, management and security policies of the network, letting them shape it to their exact needs. The Nevada Department of Transportation, for example, is building an independent, hardened Intelligent Transportation System (ITS) to support IoT devices deployed along its 5,400 miles of highway, leveraging advanced technologies like Shortest Path Bridging (SPB).

Flexible network overlays balance efficiency and risk

An operational network overlay allows for partial integration with a new or existing IT network. It enables enterprises to add new applications, divisions and agencies to the existing network and treat it as a shared resource, while still limiting access to specific operational technology.

This approach provides cost-savings by leveraging a single infrastructure for both IT and OT needs, while still maintaining a degree of separation and independent control of security policies and management processes. Both teams benefit from the same infrastructure resources while maintaining distinct domains. This network arrangement is also highly flexible, providing as much or as little overlap between networks as needed.

Full integration maximizes interoperability and exposure

Enterprises can also fully integrate their operational devices into an existing IT network. This maximizes visibility of all operations devices to both IT and OT teams, provides the enterprise with complete oversight of all systems from a single dashboard and enables cost-effective use of the full spectrum of IT technologies.

> *"Alcatel-Lucent Enterprise technologies enhance the security and flexibility of our network, reduce configuration complexity and help us fully comply with regulatory requirements."*
> *-- Klaus Dellhofen, Group Leader of Network Technology & Cybersecurity, GELSENWASSER AG*
>
> Read case study

Full integration provides the greatest capacity for cross-domain automation. This can extend to indirectly or directly connecting operational communications infrastructure into IT network infrastructure for seamless internal and external communications, as well as data storage and analytics. By leveraging the advanced data analytics capabilities of an existing IT infrastructure, operational teams can actively monitor operations systems to improve efficiency and spot slowdowns and breakdowns much more quickly for everything from manufacturing floor processes to smart building operations. California State University, for example, was able to save over $100 million in infrastructure costs by unifying network management into a single network.

Irrespective of network infrastructure, enterprises must ensure their networks are capable of delivering information where it's needed, when it's needed. Whether that's personnel managing daily operations or emergency crews responding to a crisis, the backbone of every operational network is its operational team.

Human connections must always be considered

Every enterprise has different needs: some will prioritize security, others efficiency and for some interoperability is the most important consideration. But one thing every organization has in common is people, and the human element of effective networking cannot be overlooked. A great deal of the efficiency and effectiveness of networked digital automation technologies, no matter which network architecture is deployed, will depend on how well they facilitate human interactions.

A networked digital automation solution can facilitate more efficient machine-to-human and human-to-human interactions to manage workflows via an advanced communications platform. By automatically providing operational teams with contextual information and allowing personnel to quickly connect when issues arise, enterprises can maximize uptime and reduce the average time-to-resolution of operational issues.

Reliable and secure communication is fundamental for coordinated emergency responses and information sharing. An advanced communications platform allows quick broadcast of an alert to stakeholders when an issue is detected at the level of an IoT, so device slowdowns and failures are caught sooner. It can also automatically create collaboration spaces where relevant personnel can connect with each other (using instant messaging, audio or video) and receive real-time notifications and alarms from connected devices. This ensures the right people have the information they need to make swift, informed decisions in any situation.

For example, Jeju Shinhwa World in Korea required an effective communications platform to build its innovative hospitality environment across 2.5 million square miles of hotels and theme parks. The resort wanted to deliver a "Smart Connecting Room" experience, allowing guests to control their room environment such as air-conditioning, lighting and Do Not Disturb notices, as well as access phone services via touch screen. By integrating a workflow engine into the solution, administrators could seamlessly manage human-machine interactions through phones and smartphones while gathering valuable usage data to enhance service quality and maintain smooth operations. An IoT hub at the heart of the solution provides a simplified framework for later integrations to fuel future digital experiences.

"Jeju Shinhwa World Resort plans to continue to improve its system to become a world-class smart hotel that provides the best customized service. In order to improve the guest service, we plan to upgrade the system to maximize digital interaction and to support custom services." - Lee Jongrae, Vice President IT, Landing Jeju Development Co. Ltd

Read case study

Leverage broad networking, integrated communication channels and deep industry expertise

The diversity of digital automation devices and networking options can be daunting. Sorting through everything that's available to find the ideal combination of hardware, software and services to meet your enterprise needs can be slow and inefficient, costing both time and money. Even small mistakes can have outsized consequences: something as simple as incompatible protocols can compromise the efficiency and security of the entire network.

Therefore, it's crucial to work with a partner with a deep understanding of the entire digital automation space, the specialized industry knowledge and the networking expertise needed to craft the right networking solution for your enterprise. An experienced provider that offers end-to-end, full spectrum networking solutions simplifies development, deployment and management of any type of network, whether it's fully independent, a network overlay or fully integrated with an existing IT network. Effective multimedia communications are at the heart of any Operations Command Center (OCC). Having a secure, reliable communications platform that integrates with IoT devices and sensors and uses advanced AI and analytics is critical. Seamless integration with any type of network will ensure operational teams can effectively collaborate and coordinate for both day-to-day and emergency operations.

"Technology is the backbone of our school's safety system. Alcatel-Lucent Enterprise Visual Notification has greatly improved our E911 setup. When an emergency call is made, we get the right address to the emergency responders right away."
-- Eric Veach, Executive Director Information Technology, Kennewick School District

Read case study

Alcatel-Lucent Enterprise has proven experience developing and deploying advanced network and mission-critical communications solutions for a variety of operational requirements, including:

- Video surveillance
- Smart buildings
- ITS
- Healthcare
- Education
- Manufacturing
- Government
- Energy & Utilities

Our experts provide more than just technical expertise. We take organizations through a multi-step process to ensure their operational network and communications solution is aligned to their needs. This starts by setting goals and gathering information about existing traffic and usage, taking stock of existing network infrastructure and ownership and outlining what the network needs to accomplish and the components required to make that happen. We identify the regulations the network and communications platform must comply with, what the cost to maintain the network will be and help organizations determine the budget required to execute the process.

Once a network is designed, our open-source APIs provide the fundamental framework any networking solution needs to add new digital automation devices and systems. All the heavy lifting has been done, greatly accelerating and simplifying integration of operational devices.

ALE has developed a comprehensive IT-OT convergence framework built on three foundational pillars: Infrastructure Consolidation, Security and Operational Efficiency. This framework accelerates digital transformation initiatives across industries by improving data flow between IT and OT environments, simplifying day-to-day operations and reducing operational costs—regardless of the complexity of their infrastructure or business model.

Infrastructure consolidation

ALE's unified platform streamlines and consolidates network infrastructure demands across both enterprise and industrial environments:

- The secure and resilient OmniFabric provides high-availability, scalability and secure connectivity across enterprise and industrial environments. Designed to adapt to each customer's specific architecture and performance needs, it supports advanced technologies such as SPB, Multiprotocol Label Switching (MPLS) and Ethernet VPN (EVPN)—individually or in combination—to ensure seamless, end-to-end network reliability and flexibility
- Support for both the conventional Alcatel-Lucent OmniSwitch® and the ruggedized industrial-grade OmniSwitch—all running the same unique operating system (AOS)—enables seamless end-to-end deployments regardless of complexity or environment
- High-performance wireless connectivity with Alcatel-Lucent OmniAccess® Stellar Wi-Fi 7, delivering multi-gigabit speeds for mission-critical applications
- Extended wireless connectivity through Private 5G, delivering advanced mobility and ultra-low latency for edge operations in uncarpeted, mission-critical environments ideal for supporting high-mobility Industry 4.0 devices and applications
- Comprehensive service consolidation: PROFINET support for wired and wireless Industry 4.0 devices, Zigbee and Bluetooth Low Energy (BLE) device onboarding
- Long-term support with lifecycle coverage of up to 10 years

Security

Security is at the core of ALE's convergence strategy, ensuring that all environments—regardless of complexity—benefit from robust, automated protection mechanisms including:

- Secure, automated IoT connectivity
- Zero-Trust Network Access powered by Private 5G microslicing technology for both macro and micro segmentation
- Operating system (AOS) hardening and independent verification
- A secure supply chain for hardware and software components
- Compliance with global security certifications

Operational efficiency

ALE enhances operational agility through intelligent tools and seamless integration capabilities that simplify deployment, maintenance and workflow management through appropriate means of communication. Key components include:

- The AI-driven maintenance tool Alcatel-Lucent OmniVista® Network Advisor to reduce downtime and improve reliability
- Real-time geolocalization of equipment and people in industrial and enterprise environments with OmniAccess Stellar Asset Tracking
- An API platform that supports system-wide integration
- A unified management tool that spans both enterprise and industrial deployments
- Intuitive installation support via the ALE Installer's Toolkit and OmniSwitch Lightning Config, enabling non-experts to easily deploy and operate the networking infrastructure without specialized hardware
- A platform for critical communications with OmniPCX® Enterprise Purple and Rainbow™ by Alcatel-Lucent Enterprise, which connect people, machines and processes through instant messaging, voice and video for efficient workflow management. Adaptable to all environments, the platform can be customized and integrated with the equipment used by staff (operations control center, mobile devices or connected objects).
- A simple and flexible, easy-to-install, intuitive multimedia mass notification system, the Alcatel-Lucent Visual Notification Assistant, is particularly efficient in situations where many people need to be notified instantly and simultaneously, wherever they are in a building, either at their desks or on the move

Most importantly, we deliver customized solutions, not off-the-shelf technologies, ensuring enterprises deploy the right solution to meet their specific needs. And to simplify deployment, all our networking products are enabled for auto-configuration in any network environment.

Contact us to learn how Alcatel-Lucent Enterprise can help you build the right network for your operational requirements.

DID25080802EN (September 2025)

Alcatel·Lucent Enterprise