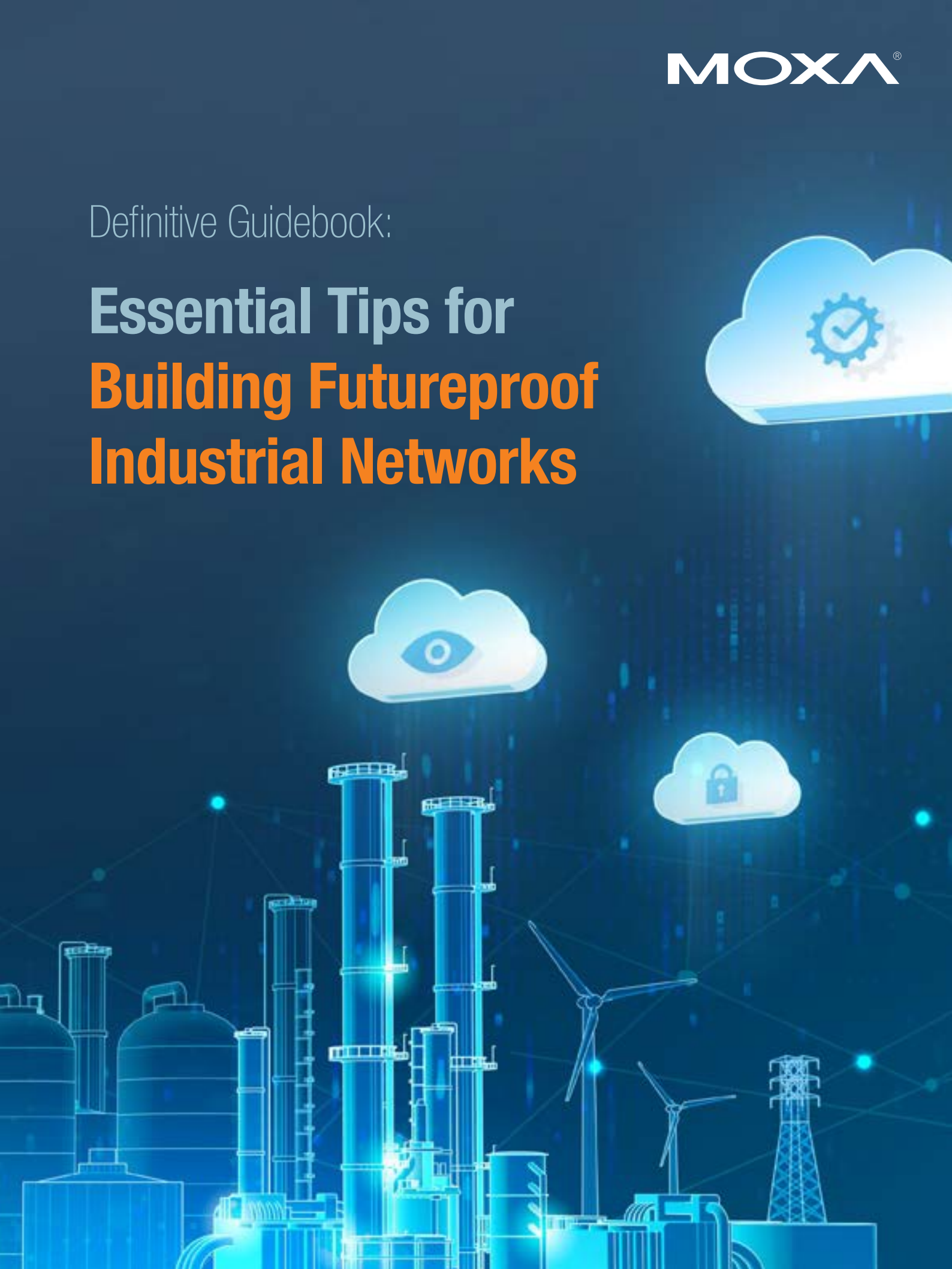
MOXA®

Definitive Guidebook:

Essential Tips for Building Futureproof Industrial Networks



Contents

1. The Digital Transformation Is Accelerating P.2
2. Seamless Connectivity Is the Way Forward P.3
3. Industrial Networks Are Evolving. Are You Ready? P.4
4. Overcoming Challenges With Futureproof Industrial Networks P.5
5. Applying Digital Transformation in Industrial Applications P.11
   - Focusing on Intelligent Transportation Systems (ITS)
   - Focusing on Power Substations
6. Conclusion: Get Ready to Futureproof Your Networks P.14

MOXA®

The Digital Transformation Is Accelerating

With the global impact of supply chain disruptions, the pandemic, and the push towards carbon neutrality, there is an urgent need to transform the way industrial organizations are running. Businesses across the globe are now beginning to see operational resilience as an imperative to maintain market share, avoid disruptions, and embrace innovation.

"Resilience" has never been more important than it is today.

Many businesses are investing in **digital transformation** and technology to ensure operational resilience. For example, some are shifting towards remote operations while others focus on adding more predictive capabilities. Automation investments have also boomed as manufacturers navigate the complex and fast-changing new landscape. Using digital technology, organizations can adapt quickly to changes in the networking environment.

34% **of organizations are now monitoring and diagnosing almost all of their devices, equipment, assets, facilities, and processes remotely with limited on-site staff.**

— IDC's 2021 Future of Operations Survey

Seamless Connectivity Is the Way Forward

To fully realize the transition to digitalized industrial organizations, it's not enough to just implement advanced digital technologies. Its success depends on the ability to seamlessly integrate these new solutions into existing legacy networks, infrastructure, and processes to create a unified digital ecosystem. **The seamless and real-time transmission of data is key.** By merging IT and OT systems, businesses can take full advantage of the technological capabilities to enhance local, remote, and cloud-based operations. According to IDC's IT/OT convergence survey*, more than 30% of organizations are planning to integrate operational data from systems such as data historian software, industrial control systems, and asset management, into their enterprise data governance model for the first time. Compared to 2018, convergence of OT and IT systems rose nearly 10%.

Merging these traditionally separate systems presents its own set of challenges. While seamless integration of these systems is an irreversible trend, OT systems need to embrace a more open architecture to sustain the growing number of connected applications. With that in mind, enhanced, robust industrial networks become even more important.

** Worldwide IT/OT Convergence Survey Findings, 2020*

"IT/OT convergence"
is the path to achieving operational resilience.

Futureproof industrial network communication is the key to success in this converged, digital future.

MOXA®

Industrial Networks Are Evolving. Are You Ready ?

Facing the rapid growth of IT/OT converged applications that introduce countless sensors and machines into industrial networks, it's no longer just about whether devices are connected or not. It's about the seamless transfer of data to the right place at the right time with the necessary reliability to ensure continuous operations.

Futureproof industrial networks are being redefined:

network connectivity + data connectivity

Robust network connectivity is important, no doubt. However, it should not be your sole focus, as you might miss out on opportunities for innovation that would let you stand out from the competition.

"Functional reliability" is an important concept that you should keep in mind when building futureproof industrial networks. It's the idea that you should not only focus on stable and seamless network connectivity, but also design your network to support seamless data connectivity. By combining these two, you can incorporate intelligent functionality into your operations such as remote control commands and incident response mechanisms.

Looking ahead, digital transformation is the key to unlocking business growth. Industrial networks will evolve to adapt to this new direction. However, since this is unfamiliar territory for most businesses, there will be some hurdles to overcome as you shift towards this new generation of networking. With this guidebook, we want to provide you with some essential tips to help you futureproof your industrial networks.

Overcoming Challenges With Futureproof Industrial Networks

[Challenge 1]:

As more devices are connected and communicating over the same network, system complexity is increasing exponentially. Any delay or data loss can lead to costly system downtime. However, developing stable network and data connectivity that can support the transformation needs of today and tomorrow is a challenge for most automation businesses.

Customer's Voice:

"Although PEA is an electricity expert, we are not that familiar with critical network communication. In implementing and maintaining a digital substation communication system, we need an expert we know we can trust."

Pongsakorn Yuthagovit,

Assistant governor,
PEA (Electricity Authority)

Expert Tip:

Futureproof industrial automation depends heavily on seamless data transmission and data integration. A robust network foundation is a critical building block to enable future usability and stability. In sum, **Reliability** is the first major point of consideration when choosing network solutions to futureproof your communications.

Ruggedized devices are the cornerstone for stable communication in harsh environments. Industrial certifications are the benchmark for any network's performance and durability in certain demanding applications. For example, the NEMA TS2 certification proves devices can reliably operate in hazardous intelligent transportation system (ITS) environments. To make integration more straightforward, products with **multiple interfaces and high port density** can cater to different connectivity scenarios and simplify the network structure. Additionally, support for ring expansions can eliminate the need to modify the network topology when adding devices to an existing network, which is both risky and prone to errors. It's also important that network devices feature **redundancy mechanisms** to handle unexpected issues and avoid downtime. For example, redundant dual power inputs can eliminate power outage downtime while other network redundancy features can speed up network recovery and quickly get systems up and running again.

Choose network solutions that can be easily integrated.

Digital transformation is a slow and gradual process that requires durable and adaptable industrial network devices. Therefore, it's important to incorporate the necessary flexibility to support both current and future functional requirements. One of these is **bandwidth**. Choosing a product with higher bandwidth can support more devices and transmit more data as demands grow over time. Another important aspect is physical design. Cabinet space is usually quite limited. However, product size often differs depending on the number of ports, making it a headache for field engineers to plan cabinet space for more devices down the line. Networking devices with a **compact and uniform design** can turn a potential challenge into an opportunity when planning for future expansions.

Customer's Voice:

"The Moxa hardware solution brought full Gigabit speed all the way out to the edge—reaching every cabinet connected to the fiber infrastructure—futureproofing the network and providing the bandwidth necessary to support the data and video needs of today and tomorrow."

Traffic engineer,
City government

Moving forward, **time-sensitive networking (TSN)**, a new set of standards based on IEEE 802.1, prioritizes network traffic and guarantees real-time communication, which means time-sensitize data will be delivered to the right place at the right time. TSN can leverage standard Ethernet infrastructure to integrate industrial automation applications into a single, unified network. TSN has already been adopted for several mission-critical applications around the world, and it's expected to offer even more possibilities in future digitalized network environments. TSN can achieve deterministic communications across a variety of applications, including in-machine, machine-to-machine, or machine-to-supervisory. If you are interested in learning more about TSN implementations, check out our *success cases* covering Moxa's cooperation with industry pioneers to integrate TSN into several practical applications.

Futureproof your business with TSN technology to accelerate digital transformation and take full advantage of the possibilities offered by the Industrial Internet of Things and Industry 4.0.

[Challenge 2]:

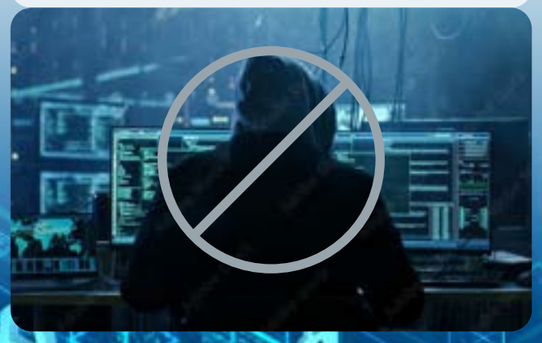
As IT/OT convergence continues to pick up momentum, closed OT systems are gradually shifting towards a more open architecture. However, this also exposes OT infrastructure to potential cyberthreats, becoming a target for hackers. Considering most production information of critical applications is confidential and often relevant to public safety, OT engineers are under pressure to keep their systems intelligent and secure at the same time. Cybersecurity is one of the major roadblocks that cause many organizations to hesitate going forward with digitalization, or in some cases, stop the process completely.

Customer's Voice:

"Edible oil refinery customers are extremely cautious about cybersecurity since the details of their production process is the company's own secret recipe; the information is highly confidential, and no one would risk exposing such valuable information to public networks."

Jeffery Wong,

Senior business unit manager,
YNY Technology (Manufacture)



Expert Tip:

Adopting digital technologies in automation environments can introduce potential cybersecurity risks which in turn can significantly disrupt operations. **Secure Networking** designed for OT engineers can simplify network security deployment, ensuring both network protection and availability when transitioning to a converged infrastructure.

Availability is a vital goal for any OT network, with some critical infrastructure needing to be available 24/7, all year round. However, every year hundreds of businesses experience some type of security breach. In many cases these breaches can be very costly and damaging to their operations and reputation. To most OT engineers, cybersecurity is complex, unfamiliar territory. To mitigate cybersecurity risks on the road to digital transformation, combining purpose-built OT networks and cybersecurity measures can minimize any potential threat to your operations.

Secure networking with defense-in-depth protection is the answer.

Defense-in-depth protection provides a suitable solution for OT engineers. A good defense starts with solid building blocks to create a secure network infrastructure. Select **security-hardened devices** that have passed international security certifications, or feature security functions based on internationally recognized standards. The IEC 62443 standard is one of the most prevalent cybersecurity standards adopted worldwide. This standard outlines a defense-in-depth approach and provides fundamental requirements at the component level, providing a common language for asset owners, system integrators, and component providers. Standardized criteria make it a lot easier to procure and integrate network devices. For wireless networks, the WPA security standard employs robust authentication and encryption algorithms to protect sensitive data in mission-critical network environments.

Next, you will need a second layer of protection to **guard your network** from attacks through segmentation and threat prevention. Some common security control technologies include deep packet inspection (DPI) and firewalls. With these technologies you can build a layered defense to protect your network from malicious activity or contain breaches to isolated zones to minimize damage.

Customer's Voice:

"To protect the communications between the power plant controller and the PCS and BMS containers, Moxa's industrial secure routers build the security boundary, and its Modbus DPI function safeguards the Modbus communication in between the systems."

Designer and manufacturer of energy storage systems, France

Lastly, it's important to always **be up to date on the status of your network.** Good visibility gives you a better understanding of your network's status, from high-level systems all the way to end devices. Dedicated security management tools can further help OT engineers keep track of the security status of their network. When it comes to remote operations, having a secure communication channel backed with strong safety measures lets you enjoy all the benefits of digital technology without the headaches.

[Challenge 3]:

When the number of connected devices increases from a few dozen to several hundred or more, it becomes increasingly harder to manually manage such complex networks with minimum downtime. Not to mention, some applications have special characteristics that complicate matters even more, such as the invisible Wi-Fi connections of moving robots in factories. Managing such evolving networks while trying to maximize uptime can be a daunting task.

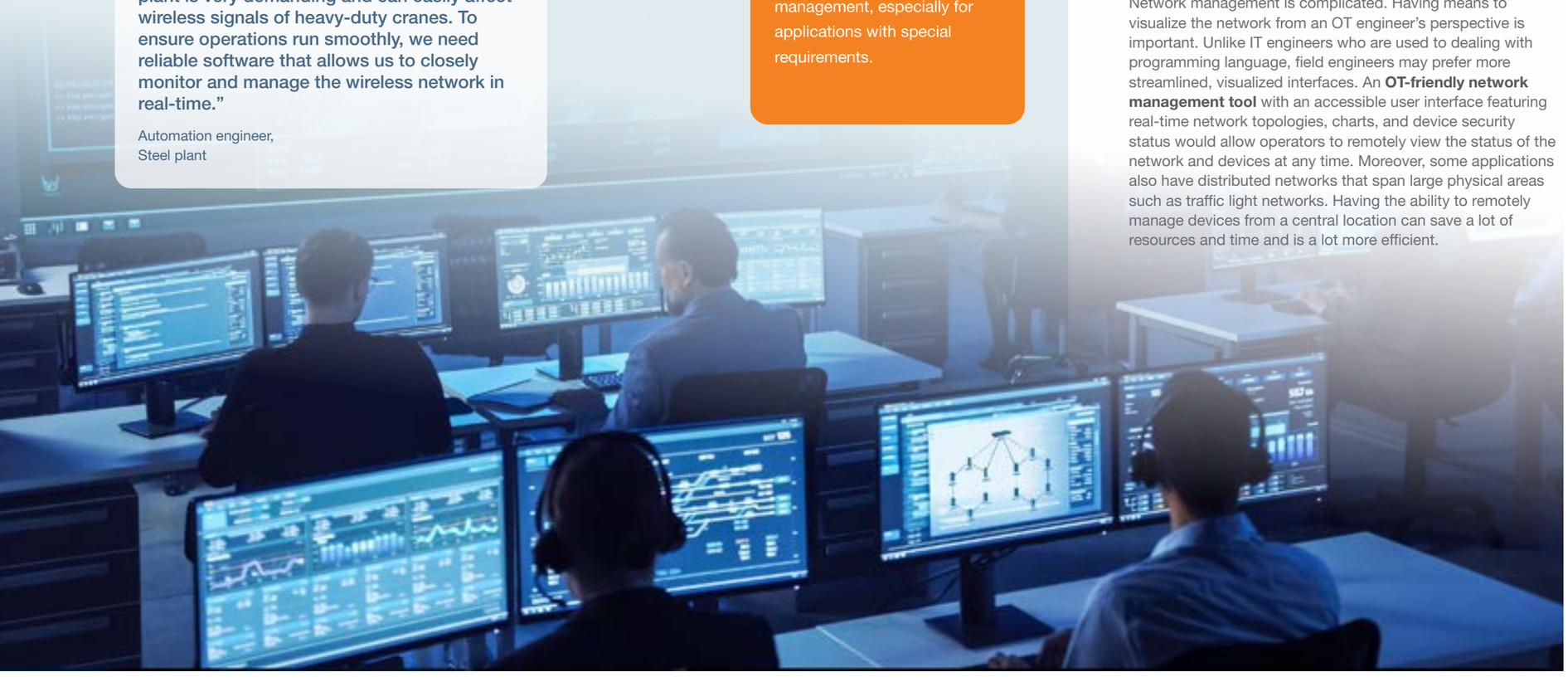
Customer's Voice:

"The operating environment inside the steel plant is very demanding and can easily affect wireless signals of heavy-duty cranes. To ensure operations run smoothly, we need reliable software that allows us to closely monitor and manage the wireless network in real-time."

Automation engineer,
Steel plant

Expert Tip:

Networks and devices are becoming more interconnected and the scale of networks keeps growing. Having clear network visualization is essential to efficiently configure devices and maintain systems on a large scale. **Simplified management** tailored to OT users can help facilitate network configuration and management, especially for applications with special requirements.



Transitioning to digital unified networks means that OT network infrastructure will inevitably grow in scale and become increasingly complex and interconnected. A single point of failure could significantly affect the entire OT infrastructure and even IT networking systems. Therefore, ensuring maximum uptime is critical to keep business running smoothly. Having different network devices running on a single, **unified operating system** can significantly simplify network configuration and management. Meanwhile, a **holistic monitoring approach** allows you to quickly respond to issues and maximize network uptime.

Visibility is the basis for simplified OT network management.

Network management is complicated. Having means to visualize the network from an OT engineer's perspective is important. Unlike IT engineers who are used to dealing with programming language, field engineers may prefer more streamlined, visualized interfaces. An **OT-friendly network management tool** with an accessible user interface featuring real-time network topologies, charts, and device security status would allow operators to remotely view the status of the network and devices at any time. Moreover, some applications also have distributed networks that span large physical areas such as traffic light networks. Having the ability to remotely manage devices from a central location can save a lot of resources and time and is a lot more efficient.

Customer's Voice:

"With Moxa industrial network management software, we can now easily identify where issues occur, drastically reducing the time required to resolve power supply problems. This streamlined system helps prevent shutdowns and reduces restoration time when they occur."

Engineer,
Electricity Authority

Considering some applications may have special requirements, a **purpose-built management module tailored for specific networking environments** can strengthen functional reliability. For example, the quality of the wireless connections between Wi-Fi devices often determines the efficiency of autonomous mobile robots (AMR) in an automated factory. Given that Wi-Fi links are invisible and dynamic, being able to make real-time snapshots of the wireless network to locate robots and spot potential issues can significantly improve automation efficiency.

Applying Digital Transformation in Industrial Applications

— Focusing on Intelligent Transportation Systems (ITS)

Expanding urbanization, and the resulting increase in traffic congestion and carbon emissions, are driving the importance of ITS. Not to mention, ITS is a key component for developing smart cities and smart transportation. A recent survey* showed that the global ITS market size is expected to reach USD 42.80 billion by 2028, expanding at a CAGR of 9.34% between 2021 and 2028. As more and more transportation infrastructure systems are becoming interconnected, reliable data communication will be essential.

Keep the following three considerations in mind to help you avoid unexpected roadblocks as you transition to a fully digitalized network.

Reliability:

Most traffic network devices are deployed in harsh outdoor environments, making industrial durability a key requirement. The network backbone needs to be able to support transmissions of large volumes of data between roadside equipment and the traffic control center, including road condition, traffic signal, and video surveillance data. Building your network around high bandwidth, high performance, and expandability can help prepare you for more device additions in the future. Since smooth transportation relies on a consistent stream of traffic data, the entire network also needs to be resilient and sufficiently redundant to ensure that data is continuously transmitted.

Security:

According to Cybertalk.org, between June 2020 and June 2021, the transportation industry witnessed a 186 % increase in weekly ransomware attacks*. If successful, these attacks can heavily disrupt city traffic and lead to serious injury or worse. Combining network and OT security disciplines and capabilities can help you manage reliability and risk more efficiently. Because a lot of traffic network devices are installed outside and are vulnerable to tampering, secure hardware can ensure network safety at the edge. In addition, it's also important to have threat prevention mechanisms, segmented IT and OT networks, and have secure network management capabilities. Having these safety measures in place can help block malicious traffic, mitigate damage in the event of a breach, and proactively perform the necessary actions when spotting abnormalities while monitoring the network.

Simplified Management:

To manage these interconnected, distributed network devices efficiently, being able to configure, monitor, and diagnose the traffic network from a central location can save a lot of time and resources. When field engineers install new network devices, operational engineers no longer need to drive miles away to configure the device on-site. Instead, the devices can now be easily set up from a remote control center. If there is an issue, instead of sending out engineers in the blazing sun or during a stormy night to inspect physical devices cabinet by cabinet, a user-friendly and intuitive network management system can help engineers understand the network status remotely and enable them to take the necessary actions.

** Market research report of intelligent transportation system (2021-2028), Fortune Business Insights*

MOXA®

Case Study

Building Futureproof Traffic Infrastructure for a Safer and More Efficient City

Forward-thinking cities like the City of Lancaster, USA, recognize the importance of using advanced networking technology to enhance interconnectivity to build a new Advanced Traffic Management System (ATMS) solution. More than 140 traffic cabinets needed to be connected to the fiber network and ATMS, so all traffic cabinets and remote assets could be managed from one central location. This provides the city with real-time data and predictive intelligence to improve operations, such as allowing operators to adapt to traffic incidents and congestion.

They used a number of Moxa's switches to build the network infrastructure that brought full Gigabit speed all the way out to the edge, futureproofing the network to support the data and video needs of today and tomorrow. The city government was very satisfied with their reliability and ruggedness. Mitch Megas, Lancaster City transportation engineer, remembers vividly that one of their cabinets was energized with high voltage from an Edison line, and the only component in the cabinet that was still functioning was the Moxa switch.

Moreover, with Moxa's network management software, they can monitor the entire city's network operation status and conduct a network security audit when necessary and quickly respond to incidents. In the past, the engineering team could only passively wait for the public to report traffic signal malfunctions before they could schedule repairs. Now they can react immediately as soon as something is malfunctioning. This not only makes their job easier, but also increases maintenance and operational efficiency."

Customer's Voice:

"With the support of digital network infrastructure, the city government reduced the need for human intervention by 67% and eased personal workloads."

City of Lancaster, USA

Paving the Way for Futureproof Transportation

Our futureproof network solutions provide you with a reliable foundation to upgrade your transportation systems, turning ideas and opportunities into real advantages and benefits.

ITS applications typically need higher bandwidth, such as multi-Gigabit uplinks to support the large volumes of video data. Meanwhile, the rising trend of automated vehicles is expected to raise data demands even more. Moxa's **EDS-4000 Series**, a set of security-hardened managed Ethernet switches compliant with the IEC 62443-4-2 standard, is designed to provide futureproof capabilities for the next decade. These switches are fast Ethernet switches with the option for four Gigabit SFP uplink ports, and support 90 W IEEE 802.3bt PoE ports to power devices such as outdoor PTZ cameras. The Turbo Ring and Turbo Chain technologies offer fast network redundancy to make sure your operations are always up and running. Meanwhile, scheduled operating system upgrades along with well-defined vulnerability responses and management enhance availability and security for dynamic transportation markets.

In addition, the EDS-4000 Series supports centralized network device configuration and management through Moxa's industrial network management software, **MXview,** to streamline configurations and reduce the workload of traffic operators. Lastly, when combined with the **EDR-G9010 Series** secure routers, traffic operators can worry less about cyberattacks on their critical network and focus more on developing smart transportation.

— Focusing on Power Substations

Substations are an integral component of distributed power grids. Their controlling and coordinating function are vitally important to the stability of the overall power system. However, the power industry is now facing the emergence of new trends and challenges including the integration of more renewable energy sources and increasing electricity demand. Digitalized substations are becoming a necessity to accommodate and balance these new dynamics and to achieve operational resilience. To successfully transform substations, optimizing the flexibility and availability of the underlying critical network communication is paramount.

Since power substations are critical infrastructure, keep the following three considerations in mind when implementing digitalization.

Reliability:

For substation communications, availability and reliability are crucial. Any kind of packet loss is unacceptable. Since network devices at substations are often deployed in very harsh operating environments, they must be rugged enough to withstand extreme temperatures and high electromagnetic interference. Equally important to ensure network availability are robust redundancy mechanisms to avoid interruptions and minimize recovery times. Network devices that support the IEEE 1588 Precision Time Protocol (PTP) are also an invaluable component of substation network reliability. Precise time synchronization makes sure substation devices inside merging units have accurate clocks, giving operators pinpoint control and letting them respond to any problems immediately.

Security:

Cybersecurity has been recognized as a critical issue for substations. With the line between IT and OT fading rapidly, a properly segmented network helps protect critical network communications. This involves setting up the right router and switch configuration, and managing safety mechanisms including firewall rules, access control, and authorization and authentication policies.

Remote access to substation networks is a common but vulnerable way for operators to monitor and maintain a widely distributed power grid. To protect utilities from cyber threats and breaches, a secure form of remote access such as IEC 61850 certified VPN solutions allows operators to safely monitor the intelligent electrical devices (IEDs) in each remote substation. Combining secure-hardened devices and secure network management capabilities can create holistic defense-in-depth network protection to keep critical industrial networks safe.

Simplified Management:

Digital substation systems need to operate 24 hours a day, all year around. To improve network management and operations while avoiding unnecessary outages, real-time monitoring is of utmost importance. The ability to visualize physical network topologies on-screen offers major advantages, especially when there is an issue. It can help operators quickly identify the source of the problem and respond immediately, significantly reducing recovery times.

MOXA®

Case Study

Power Up Economic Growth for a Smart City in Thailand

The city of Pattaya, Thailand, was chosen for the pilot test of a Provincial Electricity Authority (PEA) program to transform cities throughout Thailand into smart cities, in part to provide the electricity needed to power economic growth. Backed by the PEA, the project aimed to transform the city's power grid by moving from manual processes for identifying power delivery issues to an automated one that minimizes the occurrence and duration of power outages using smart grid technology. The PEA partnered with Italthai Engineering, the leading engineering contractor in Thailand, and Moxa to implement this overhaul.

A crucial element of smart grids are smart substations. To ensure a smooth transition to smart power infrastructure, Moxa provided expertise and assistance with designing the topology to help the PEA move from an outdated, 30-year-old system with a wide variety of equipment brands, models, and types to a system with a simplified and standardized design. The new smart infrastructure enabled substations to operate automatically and achieve real-time communication. Moreover, with Moxa's network management software, operators were able to easily identify issues and respond quickly, drastically reducing the time required to address power supply problems. The new upgraded systems helped prevent shutdowns and shorten recovery times whenever issues occurred. The best practices developed during this pilot project can now be used by the PEA to achieve the same level of success when deploying similar upgrades in other pilot cities.

Energizing Substations With Digital Networks

Our futureproof network solutions provide you with a reliable foundation to retrofit or build new digital substation systems, maximizing operational efficiency and minimizing outages.

Digital substations depend heavily on seamless communication between devices to achieve substation automation. Moxa's **RKS-G4000 Series** industrial rackmount switches can handle large numbers of links and operate reliably in harsh conditions. These IEC 61850-3 and IEEE 1613 certified switches provide robust protection against a variety of environmental hazards such as electromagnetic interference (EMI) to ensure critical packets are reliably transmitted. The hardware-based IEEE 1588 PTP features for high-precision time synchronization ensure the accuracy of the communication. Meanwhile, the intuitive user interface and integration with Moxa's industrial network management software gives operators full network visibility and simplifies management.

Facing rising concerns over security threats, the RKS-G4000 Series has passed the IEC 62443-4-2 international security standard, providing protection for the critical Ethernet network from the device-level up. Integrating our **EDR-G9010 Series** industrial secure routers into your critical networks adds an additional security boundary to create a first line network defense. These secure routers support Deep Packet Inspection (DPI) which examines the data portion of network packets for various power-specific protocols. They also act as an IEC 61850 certified VPN firewall to create a multilayered defense for its multiple Gigabit connections. With these combined features, operators can achieve long-term functional reliability for their Ethernet network and make full use of the digital substation technology.

Conclusion:

Get Ready to Futureproof Your Networks

Digital transformation is a striving goal for any industry looking to achieve operational resilience. Seamless and real-time data communication is the cornerstone of IT/OT convergence, allowing data to flow smoothly between on-site end devices and the control center to guarantee uninterrupted operations. We are witnessing how industrial networks are evolving in this new direction. In response, we are redefining what it means to futureproof networks. We hope the tips provided in this guidebook will help you smoothen your network operations and **futureproof your business.**

Your Trusted Partner in Automation

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

Moxa Americas

USA

Toll Free: 1-888-MOXA-USA
Tel: +1-714-528-6777
Fax: +1-714-528-6778
usa@moxa.com

Brazil

Tel: +55-11-95261-6545
brazil@moxa.com

Moxa Europe

Tel: +49-89-413-25-73-0
europe@moxa.com

Moxa Asia-Pacific and Taiwan

Asia/Taiwan

Tel: +886-2-8919-1230
Fax: +886-2-8522-8623
asia@moxa.com
taiwan@moxa.com

India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045
india@moxa.com

Russia

Tel: +7-495-287-0929
Fax: +7-495-269-0929
russia@moxa.com

Korea

Tel: +82-2-6268-4048
Fax: +82-2-6268-4044
korea@moxa.com

Japan

Tel: +81-3-6721-5670
Fax: +81-3-6721-5671
japan@moxa.com

Moxa China

Shanghai

Tel: +86-21-5258-9955
Fax: +86-21-5258-5505
china@moxa.com

Beijing

Tel: +86-10-5976-6123/24/25/26
Fax: +86-10-5976-6122
china@moxa.com

Shenzhen

Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
china@moxa.com

© 2022 Moxa Inc. All rights reserved.
The MOXA logo is a registered trademark of Moxa Inc. All other logos appearing in this document are the intellectual property of the respective company, product, or organization associated with the logo.