MOXA®

[Challenge]

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

---

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.
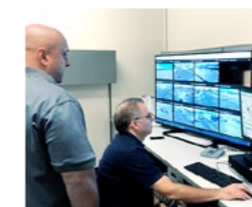
Moreover, with Moxa's network management software, they can monitor the entire city's network operation status and conduct a network security audit when necessary and quickly respond to incidents. In the past, the engineering team could only passively wait for the public to report traffic signal malfunctions 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."

What is a SMART CITY?

The City of Lancaster is using advanced techology data, and predictive intelligence to improve operations.

- Energy Management
- Traffic Monitoring
- Co-Locatable Infrastructure
- Citizen Access
- Wi-Fi
- Public Safety

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.