Application Note Part 1

Simplifying Connectivity for Remote Monitoring

A resilient and reliable network that connects a large number of existing data sources from various systems is critical to ensure accurate data in order to realize remote monitoring

Remote monitoring gives you visibility and transparency of data that is often stored in decentralized silos, facilitating the overall monitoring of operations. Remote monitoring comes with many benefits for the manufacturing industry, from improving productivity to reduced downtime, to reducing operating costs.

With information readily available at managers' fingertips, they are able to address the highest production priorities in a timely manner. But without a resilient and reliable network, which connects sensors and other data-gathering devices on the shop floor, managers will adjust production planning based on unreliable data. Find out how the following two challenges to block your path to connect to remote monitoring.

Case in Brief:

Smarter Shop Floor with Real-time Cloud-based Monitoring

Tech Manufacturing, a long-time manufacturer of machine metal parts for aerospace clients, needed to raise production capacity and reduce lead time for their clients' largest and most urgent orders. Moxa helped Tech Manufacturing connect their legacy machines and devices to collect data and push it to the cloud. This time-saving and cost-saving remote monitoring solution is already reaping benefits for the customer with increased productivity as the real-time dashboard makes it easy to identify critical production issues. **Learn More**

![MOXA - Reliable Networks · Sincere Service]

Connecting Various Systems Causes Network Outage

As the IIoT continues to make inroads in manufacturing, we will see more and more machines and devices from different OT subsystems get connected to ensure that managers enjoy full transparency of their shop-floor operation. These subsystems include CNC control systems, conveyor belt control systems, AGV distribution systems, and inventory management systems. In older hierarchy-based network architectures, these systems used to run smoothly on their own. But as soon as they were connected to each other, networks either became unstable or failed due to slow responses, network interruption, or single point of failure, resulting in unreliable data and PLCs receiving incorrect responses.

A Cocktail-like Topology
Using different commercial and industrial network devices may impact the daily operation of long-term hardware when the network gets connected.

Unmanageable Interoperability
Using unmanaged Ethernet switches to connect machines in a single system directly is cost-effective; however, it will cause an unidentified network to act abnormal in an interconnected scenario.

Insufficient Resilience
A star or daisy-chain network is easy to deploy; however, it cannot provide millisecond single-point-of-failure recovery.
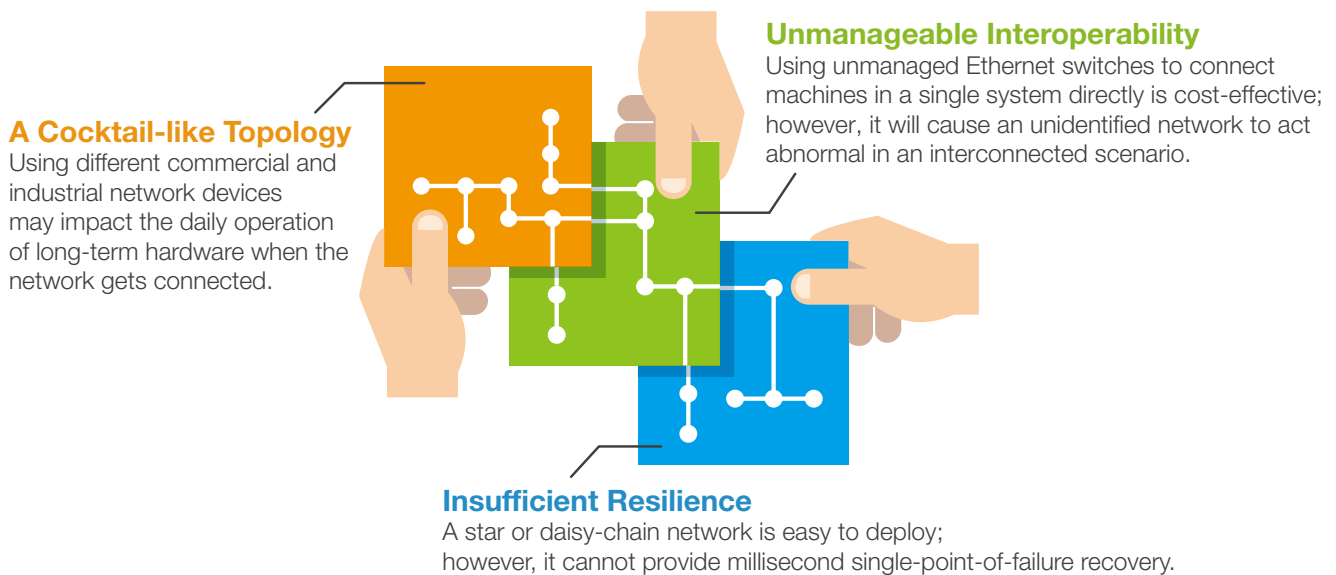
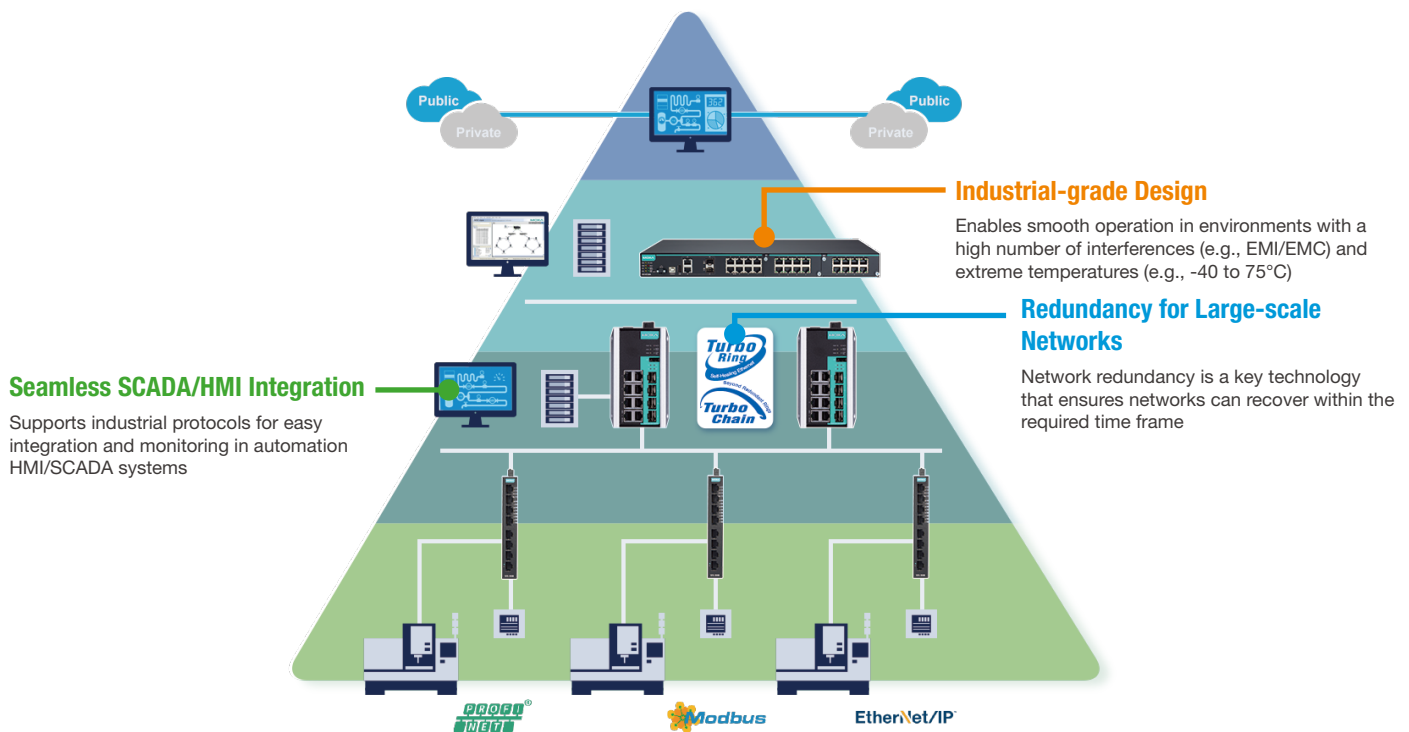Figure 1: Three issues that cause network outage

On closer inspection, these network problems are attributed to three issues:

- **A cocktail-like topology:** With regards to a cocktail-like topology, different machines and systems might use different commercial and industrial network devices (e.g., Ethernet switches), as they were built at different stages. Subsequently, an OT environment contains many interfaces that may impact the daily operation of long-term hardware with regard to electromagnetic compliance (EMC), surge, and many more when the network gets connected.

- **Unmanageable interoperability:** Subsystems employing different OT protocols usually use unmanaged Ethernet switches to connect machines in a single system directly. In an interconnected scenario, each connected node in a port should not only be manageable, but it should also support different OT protocols to be visible in SCADA systems, thus ensuring interoperability and communication with each other in the network.

- **Insufficient resilience:** A resilient network is rooted in a network design that emphasizes redundancy. A traditional star or daisy-chain network is easy to deploy and maintain; however, it cannot provide millisecond single-point-of-failure recovery when connecting multiple factory subsystems together. Another common issue is insufficient bandwidth, as it will make network connections unstable, especially multiple systems running on the same network. Bandwidth becomes inadequate as data transmissions increase in an interconnected IIoT-based network.

MOXA®
Reliable Networks ▲ Sincere Service

We Can Simplify Your Network Solution for Various Systems?

Moxa's managed industrial Ethernet switches provide simplified networking solutions for your cross-platform systems to transmit all the data between plant-floor equipment and SCADA/MES systems or cloud platforms.

Industrial-grade Design

Enables smooth operation in environments with a high number of interferences (e.g., EMI/EMC) and extreme temperatures (e.g., -40 to 75°C)

Redundancy for Large-scale Networks

Network redundancy is a key technology that ensures networks can recover within the required time frame

Seamless SCADA/HMI Integration

Supports industrial protocols for easy integration and monitoring in automation HMI/SCADA systems

Industrial-grade Design

An industrial-grade design enables smooth operation in environments with a high number of interferences (e.g., EMI/EMC) and extreme temperatures (e.g., -40 to 75°C). To illustrate its successful application, an industry-leading automotive component supplier in China now uses Moxa's industrial Ethernet switches, so that they can prevent packet loss, caused by a high number of environment interferences and extreme temperatures, which the customer's previous commercial-grade solution could not withstood.

Seamless SCADA/HMI Integration

Moxa's managed industrial Ethernet switches can seamlessly integrate devices to SCADA/HMI systems and support the mainstream industrial proprietary OT protocols, such as Modbus and EtherNet/IP. For example, the network of a solutions provider of automated material handling systems in the USA, which used unmanaged switches to integrate its Ethernet/IP PLC with its existing SCADA system, experienced jitter as more and more devices were connected to the network. Moxa's managed switch supports EtherNet/IP protocols to enable IGMP snooping, which controls multicast traffic so that jitter is eliminated.

MOXA®
Reliable Networks ▲ Sincere Service

# Redundancy and High Bandwidth for Large-scale Networks

Redundant Ethernet technology has been adopted rapidly due to its enhanced reliability. Moxa's redundancy technologies provide an efficient way to build a reliable and flexible network to ensure high availability and support unlimited redundant network expansion to protect networks against transmission failures.

Turbo Ring
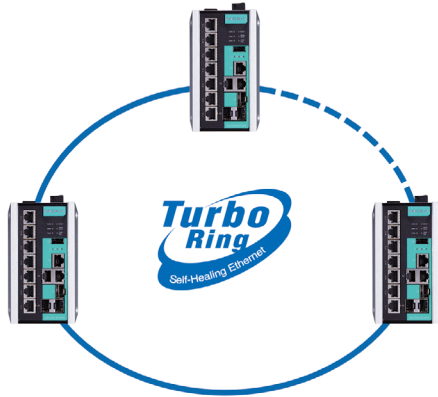
Ring topology is a very popular and cost-efficient way to build a network and is recognized within the industry as being one of the most effective solutions to avoid network downtime. Moxa's Turbo Ring technology allows networks to recover within 20 ms* on a network with up to 250 nodes. (*Note: 10G/1G Ethernet recovery time < 50 ms)

Turbo Chain
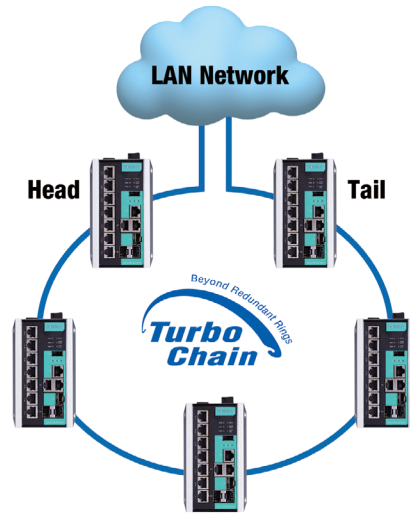
Moxa's Turbo Chain is a very flexible redundancy technology that offers unlimited redundant network expansion and is designed for use on widely distributed networks. Turbo Chain outperforms traditional ring topologies by providing superior flexibility, unrestricted expansion, and simplified configuration that allows network operators to reduce deployment costs when connecting separate redundant rings together.

Our Solutions:

- Moxa's industrial Ethernet switches are designed with -40 to 75°C wide operating temperatures and are EMI/EMC certified.
- Layer 2 Smart Switches support EtherNet/IP, PROFINET, and Modbus TCP industrial protocols for easy integration and monitoring in automation HMI/SCADA systems
- Advanced Managed Switches provide real-time and visualized central network management through MXview and cybersecurity features based on IEC 62443-4-2.
- Layer 3 Managed Switches offer bandwidth of up to 10G for large-scale networks to bridge various IT and OT systems.

Invisible Large Networks Cause Unreliable Network

Traditionally on the shop floor, machines and other equipment involved in processes such as assembling, processing, and packaging were visible in SCADA systems while but networking devices and other related equipment were invisible to operation managers. As a large variety of systems are deployed in different manufacturing sites on a large scale in the age of the IIoT and Industry 4.0, their invisibility is not a good thing in modern-day manufacturing. There is always the increased risk of network failure that can lead to catastrophic events during production. As networking equipment is an integral part of any smart manufacturing process, it is critical to make them visible and manageable, especially in large-scale applications. These challenges are vital to address:
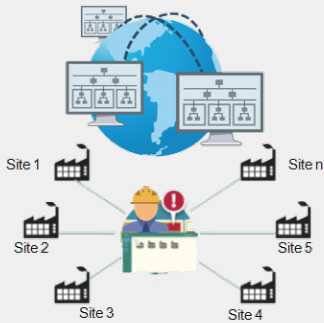

Managing the Interconnectivity of Thousands of Devices and Machines

Traditionally, different systems were cascaded into a large network to facilitate data collection and system management of machinery and equipment. In other words, networks only consisted of a dozen or so devices. But in the era of the IIoT, the same network might house up to hundreds or even thousands of devices. Inevitably, such large-scale deployments of devices come with a slew of challenges in managing a network, such as being updated in real time on the connection status of all the network devices.
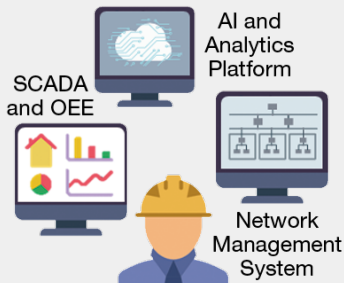
Operating Multiple Systems and Software Separately Causes Complexity

As the complexity of the entire management of a network increases, pressure mounts on network engineers to acquire new skills and tools to deal with new demands. For example, engineers have to learn new network management software. Furthermore, if IT people manage the network, then it is most likely that their usual management tools do not support industrial switches, making their implementation difficult.
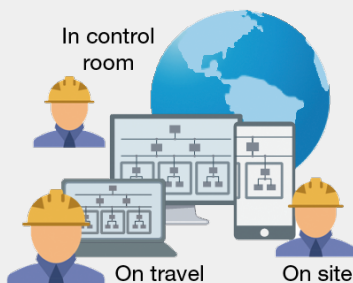
Accessing Network Management From Multiple Sites and Locations

Operating multiple systems and software separately, managers need to use management software to see the status of the devices on the network. For factories operating 24 hours a day, dealing with network issues after hours or during business trips can be a huge headache as they cannot monitor the relevant data remotely.


MOXA®
Reliable Networks ▲ Sincere Service

We Can Simplify Your Network Management of Large-scale Deployments?

Moxa's MXview is an industrial network management solution that helps visualize the network for operational engineers to make monitoring and management of networking devices easy.

- **Scalability:** MXview supports different network management scenarios. It can monitor up to 20,000 nodes in a single factory or monitor up to 2,000 nodes in 10 separate factories.
- **The flexibility of integrating OT and IT:** Through MXview, the network status information is converted to OPC protocol and integrated into SCADA software. Or, the network status information can be integrated into the online SCADA software as a web widget. Another alternative is RESTful API support, allowing IT people to easily integrate network management into existing system applications.
- **Accessibility:** Administrators can use any browser from any platform to remotely monitor network status—no need to install new client software. Furthermore, Moxa has an MXviewToGo app (iOS and Android) that proactively notifies users of any network communication exceptions.

Virtual Device Panel
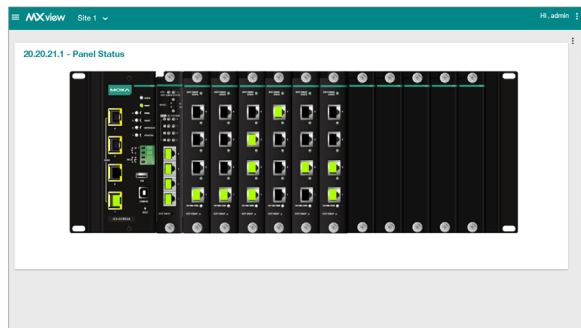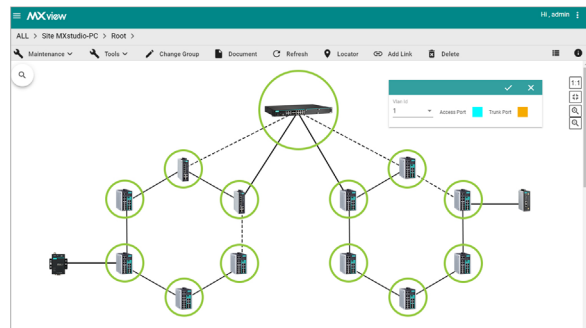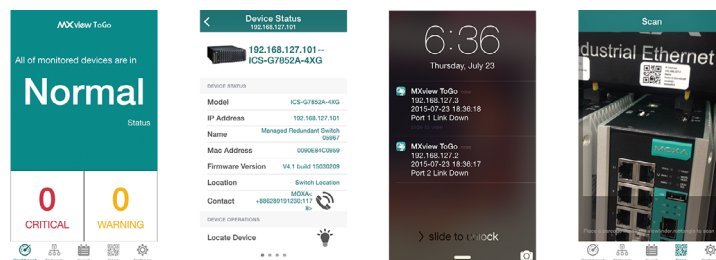
VLAN Visualization

Figure 2: Visualizing network devices

Figure 3: Mobile APP for remote monitoring