Enhancing Network Resilience for Your Industrial Control Systems

An industrial control system (ICS) is one of the commonly seen automation systems in manufacturing applications. The purpose of deploying ICSs is to interconnect multiple industrial devices and machines to perform automated operations, with the goal of reducing manual effort and increasing operational efficiency. For example, a food and beverage factory can use ICSs to arrange the production schedule and procedures so that production lines can be operated as requested. As more industries evolve towards Industry 4.0, manufacturers are expecting more from ICSs. By connecting more field devices on an ICS network or even connecting multiple ICSs into one integrated network, manufacturers can collect field data and turn it into valuable information, which will allow them to optimize production efficiency and perform predictive maintenance. To make it a reality, it's important to develop a reliable and secure network infrastructure for an ICS to ensure field data can be delivered with accuracy and integrity, which will allow accurate data analysis to be performed.

Scenarios That Industrial Control System Engineers Frequently Encounter

To optimize production efficiency for manufacturing applications, system engineers are responsible for enabling connectivity for the increasing number of field devices that are being deployed into ICSs. This connectivity will allow factory operators to collect field data and analyze it. However, enabling this type of connectivity is easier said than done. Once the number of field devices connected to networks increase, system engineers frequently encounter three networking challenges.

First, a network design that is not capable of meeting the increased number of field devices on one network. When more field devices are deployed on existing networks, and no evaluation has been performed to ensure that the network can cope, system engineers often experience poor network performance such as bandwidth overload or broadcast storms, resulting in network latency or even packet loss. These scenarios are often very detrimental to operational processes.

Second, adding additional field devices into ICS networks increases the burden and complexity of daily operations. As the number of networking devices used to connect more field devices increases, system engineers must pay more attention to them. Without an efficient tool, it takes a significant amount of time and effort for system engineers to check the networking status on a regular basis.

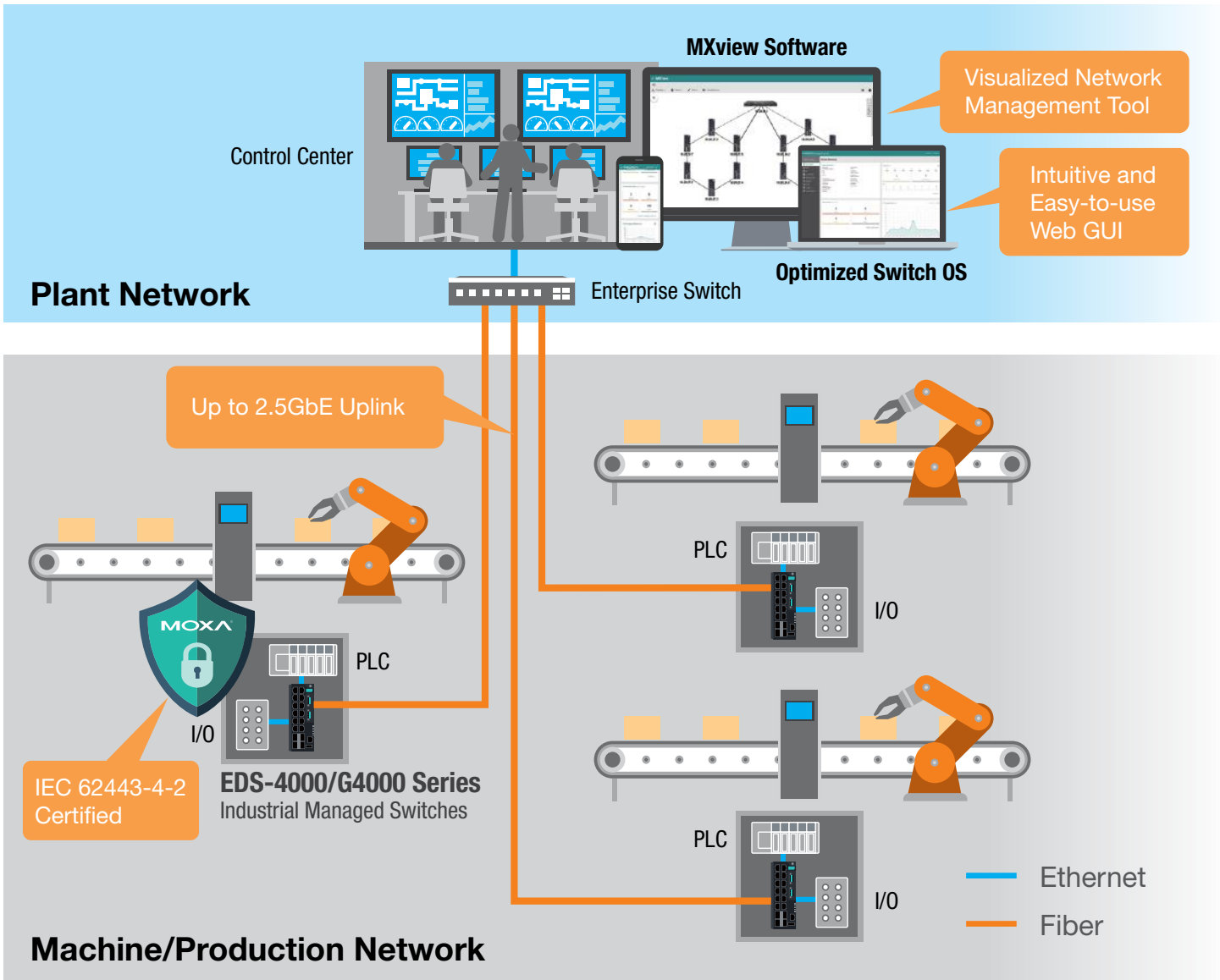
Third, as more field devices become connected, there is an increased chance that some devices will fall victim to a cyberattack, such as someone gaining unauthorized access. Without proper network protection in place, incorrect configurations or human error can easily lead to security breaches, resulting in unexpected system downtime and loss of revenue.

Industrial Control System Engineers' Expectations

To reduce obstacles when deploying numerous field devices on ICS networks, system engineers are looking for advanced networking solutions that can efficiently deliver data with accuracy and integrity. Nowadays, system engineers need high-performance networking solutions to ensure smooth data transmission for the increasing amount of field data found on one network. In addition, networking solutions that are secure by design can also reduce security concerns when more field devices are connected to networks. Last but not least, intuitive user interfaces for networking devices can make daily operations easier for system engineers.

Get the Most Out of Industrial Control Systems With Futureproof Networks

To meet system engineers' expectations as well as enhance network resilience, it's recommended to develop a futureproof network infrastructure with high performance, security features, and enhanced usability to maximize network uptime. As a company with proven industrial networking expertise, Moxa has helped our customers in the manufacturing industry to build futureproof network infrastructure that achieves optimized production efficiency for their manufacturing applications. For manufacturing innovators who are building a futureproof network to get the most out of their ICSs, our solutions can offer them three main benefits.



Benefit 1: Superior Network Performance Delivers Smooth Data Transmissions

Ensuring smooth data transmissions for an increasing number of connected field devices can be challenging. Innovators within the manufacturing sector might encounter unexpected packet loss when more field devices are connected to their ICS networks. To solve this problem, we suggest enhancing network performance to ensure there is sufficient bandwidth as well as traffic control functions. In order to do this, first build your ICS networks to support Gigabit transmission and use link aggregation functions to maximize throughput. This way, you can provide sufficient bandwidth for the increasing amount of data that is being transmitted across your ICS networks. Then, adopt traffic control functions to ensure your data can be delivered as requested. One important thing to remember is that advanced functions that can help avoid traffic storms and prioritize data transmissions will be beneficial. Our high-performance managed switches support 2.5GbE bandwidth and advanced traffic control functions to help manufacturing innovators build a futureproof network for ICSs, paving the way to realize optimized production efficiency.

When your networks need to connect more field devices, you need better network performance, which includes larger bandwidth and more advanced traffic control functions to ensure smooth data transmissions.

Benefit 2: Enhance Network Security to Reduce Cybersecurity Risks

As the number of field devices being connected to networks increases, so does the chance of a cyberattack. Therefore, many manufacturing innovators are starting to pay more attention to the importance of cybersecurity. We suggest they follow international security standards to strengthen network security for their ICSs. The IEC 62443 standard is one of the most widely used security standards that was designed for industrial automation and control systems. By adopting the security guidelines, it can significantly enhance the security of your ICSs. Our networking devices were developed based on the IEC 62443-4-1 secure product development lifecycle guidelines and aim to act as a secure building block for your ICS network infrastructure. Furthermore, our networking devices are equipped with security features to enhance the overall security of the network, which significantly reduces cybersecurity risks.

The most effective and industry-proven method to enhance cybersecurity for your connected ICSs is to implement security standards such as IEC 62443. The security standards include guidelines that provide clear instructions for how you can protect your networks and reduce cybersecurity risks.

Benefit 3: Simplify Network Management to Increase Operational Efficiency

Operating ICSs that include numerous connected field devices increases the complexity of network connections. To reduce the burden of operating the network, we suggest innovators within the manufacturing sector choose networking devices that come with intuitive user interfaces. Our networking devices have a built-in user-friendly web GUI that allows you to easily monitor the networking device status and quickly modify connection settings if necessary. In addition, our networking devices also support an easy-to-use management tool that simplifies network management from the initial installation all the way to daily maintenance of the ICS networks.

Managing ICS networks can be a real challenge without the right tools. Ensuring your networking devices support an intuitive user interface and easy-to-use network management software will tremendously improve the efficiency of your daily operations.

See What a Manufacturing Innovator Has to Say

> With the main objectives of converging our IT and OT systems, achieving a secure and efficient network architecture that adheres to IEC 62443 standards, and building a production monitoring and analytics platform to drive data-driven decisions, we have truly hit the bullseye. And it would not have been possible without the Moxa EDS-G4000 series network switches.

Matt Eberly
Manager, Automation & Electrical Engineering
Minerva Dairy

Conclusion

To make yourself more competitive within the manufacturing industry, it's essential to build a futureproof network to enhance network resilience for your ICSs. Our EDS-4000/G4000 Series managed switches are a game-changing networking solution. Our switches are equipped with up to 2.5GbE bandwidth and link aggregation functions to maximize network bandwidth for ICS networks. To make it easier for you to control your traffic flow and deliver data as requested, our advanced functions such as traffic storm control, ingress data limit, and QoS can all help. To enhance network security, our EDS-4000/G4000 Series managed switches are certified with IEC 62443-4-2 standards, providing security features such as VLAN, IEEE 802.1X, port security, and ACL to reduce the risk of unauthorized access to your ICS networks. Efficient network operations are essential. Our EDS-4000/G4000 Series not only features an intuitive web GUI but also comes with our MXview network management tool to help you visualize the network status, even on a large-scale network. Visit our microsite to learn more about what our Ethernet switches can do for your industrial applications.

EDS-4000/G4000 Series
Industrial Managed Switches