Protect PLCs & SCADA Systems

Enhance Industrial Cybersecurity for Oil and Gas Pipeline Monitoring

A leading company in the oil and gas industry wanted to enhance the security of their pipeline monitoring solution by upgrading their existing serial-based communication infrastructure to Ethernet-based networks.

Location: U.S.A
Application: Oil & Gas Pipeline Monitoring

Pro Tips

- Deploy industrial managed Ethernet switches that feature enhanced security functions based on the IEC 62443 standard

Moxa Products

MXview
Industrial Network Management Software

EDS-510E
Industrial Managed Ethernet Switches

Challenges

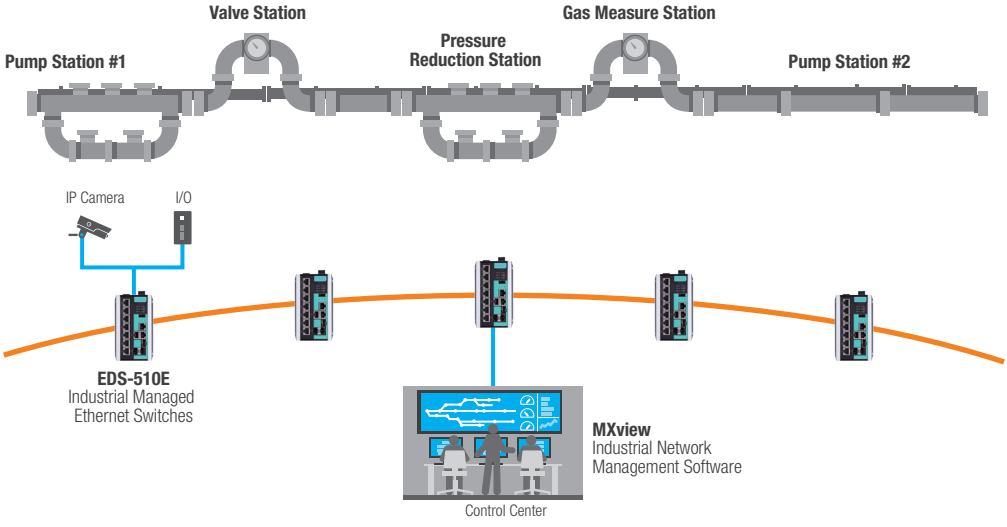
High-capacity oil and gas pipelines are very volatile and often span thousands of kilometers. The pump stations along the pipeline are equipped with analyzers and PLCs. The company found it challenging to maintain a stable network connection between the stations and the remote SCADA system because the PLCs and I/O devices lacked security features. In order to enhance industrial cybersecurity, the company started by strengthening its security policy to ensure that it was based on the IEC 62443 standard, which requires each networking device to be equipped with enhanced security features.

Moxa's Solution

Moxa's recommendation was to upgrade the industrial networks at the field sites with industrial managed Ethernet switches because they have enhanced security functions that fully comply with the company's security policy.

Device Protection

- Provides enhanced industrial cybersecurity based on the IEC 62443 standard
- Provides real-time and visualized central network management via MXview network management software



Protect Factory Networks

Visualize the Security Status of Large-scale Factory Networks

Location: U.S.A
Application: Factory Automation

A manufacturer of automotive parts in the U.S.A. wanted to digitalize their production processes. However, the industrial control networks were built a long time ago and expanded overtime to meet increased production capacity requirements. It became a challenge for the company to effectively manage all of the devices.

Challenges

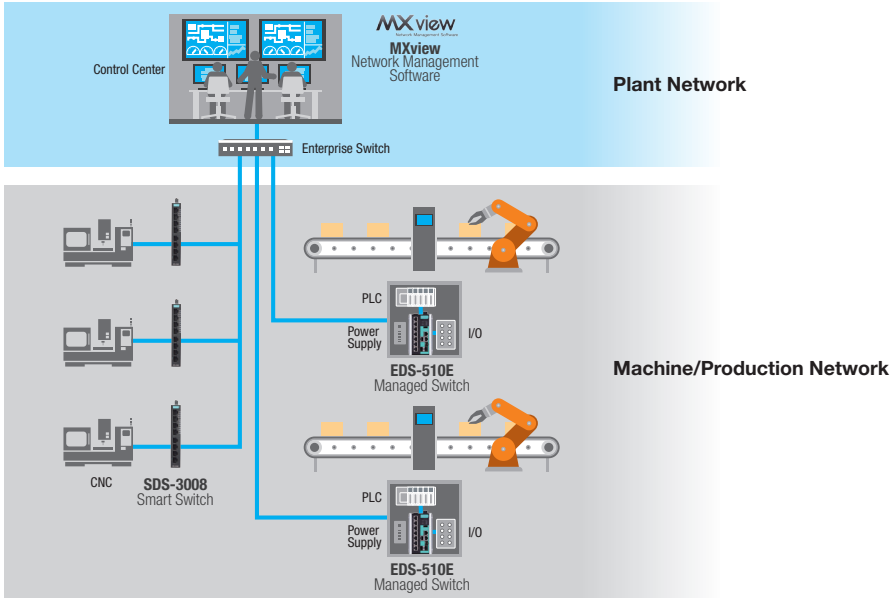
The field devices run on the EtherNet/IP protocol for control unification and data acquisition. As this plant required a large-scale network infrastructure, it was very difficult for the plant manager to monitor all devices and visualize the network topologies. In addition, in order to achieve digitization, the networks had to be interconnected from the field site all the way to the ERP and even to the cloud. It is essential to have good cybersecurity measures in place to allow this transformation to occur, and importantly, without compromising production efficiency.

Moxa's Solution

Moxa helped the company upgrade its networks with industrial managed Ethernet switches so that they support EtherNet/IP multicast filtering and advanced security functions. In addition, the company utilized our MXview network management software for real-time monitoring and visualization of the industrial control networks.

Device Protection

- Supports EtherNet/IP protocol and IGMP Snooping to manage multi-cast traffic and reduce jitter
- Offers real-time and visualized central network management with security status at a glance
- Provides industrial cybersecurity features referencing the IEC 62443 standard



Pro Tips

- The combination of managed switches and network management software is the ideal solution to provide advanced security features and real-time monitoring while also meeting the EtherNet/IP multicast traffic filtering requirements.

Moxa Products

EDS-510E
Industrial Managed Ethernet Switches

MXview
Industrial Network Management Software

SDS-3008
Industrial smart Ethernet switch

Protect Factory Networks

Enhance Industrial Cybersecurity by Segmenting Factory Networks

Within a steel plant in Taiwan, there are different processing areas and production lines. The plant manager wanted to isolate and separate data transmissions between the production lines to prevent unexpected behavior from affecting other production lines.

Location: Taiwan
Application: Factory Automation

Pro Tips

- Deploying a secure router with a firewall and switch functionality allows the network to be segmented and for data filtering to be performed. In addition, NAT can be utilized to simplify management of IP addresses.

Moxa Products

EDR-G903
Industrial Secure Router with Firewall/NAT/VPN

EDR-810
Industrial Secure Router with Switch/Firewa/NAT/VPN

Challenges

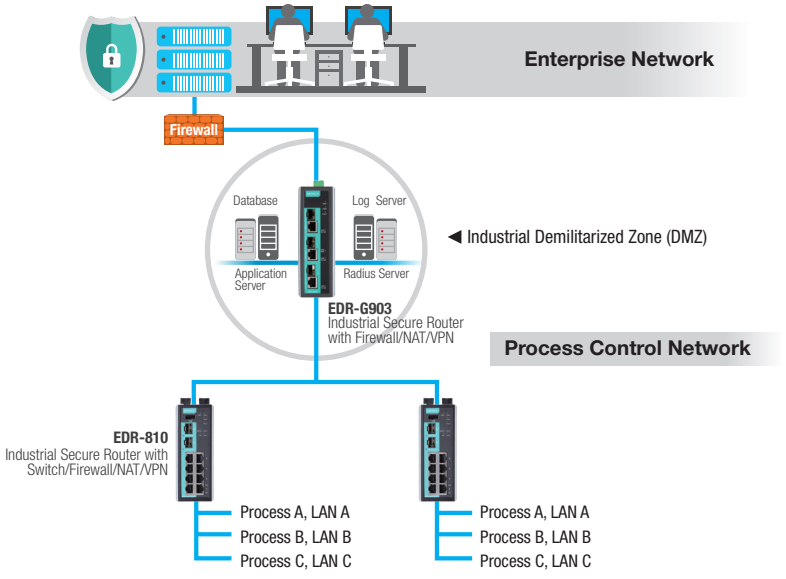
When connecting the enterprise network to the control networks, the plant manager was required to comply with IT policies in order to mitigate any potential risks. One of the most challenging tasks for the plant manager was to manage all of the IP addresses. Furthermore, in order to enhance the industrial cybersecurity of the network, the plant needed a network design that secured the data transmission from the enterprise network to the control networks.

Moxa's Solution

To protect the enterprise and control networks, Moxa recommended the plant manager to deploy a secure router with dual WAN ports because it establishes an industrial demilitarized zone (DMZ), which prohibits both sides of the network from communicating directly with each other. In addition, Moxa suggested using secure routers that come equipped with a firewall to segment networks and perform network address translation to simplify the management of IP addresses.

Secure Network Infrastructure

- Supports industrial Layer 2 switches and has a firewall to segment networks and filter traffic
- Supports NAT for IP address mapping and management
- Supports routing between different network subnets
- An industrial-grade design to ensure greater reliability for critical applications



Easy and Secure Remote Access for Improved Machinery Services

Maximizing network uptime enhances machine productivity. Therefore, a leading manufacturer of mechanical power presses needed to provide a timelier and more efficient after-sales service to its customers around the globe in order to ensure improved machine performance and effective troubleshooting.

Location: Taiwan
Application: Factory Automation

Pro Tips

- Deploying out-of-bound LTE cellular connection for isolated protection from local networks and fully-integrated secure connection with end-to-end data-encryption can fulfill IT security requirements and secure remote access needs at the same time

Moxa Products

Moxa Remote Connect Suite
Remote Connection Management Platform for Secure Remote Access

Challenges

At first, the machine builder adopted Windows-based Remote Desktop Control (RDC) technology, but there were significant security risks and additional costs that the machine builder wanted to avoid. Windows-based RDC requires a Windows-operated computer to be installed at the factory. However, the Windows-based computer is susceptible to security risks and the possibility of cyberattacks increases even more when the computer connects to the Internet. To preempt security risks, the machine builder needs to adopt complex IT-related firewall equipment, which is time-consuming and hard to manage.

Moxa's Solution

Among remote connection solutions, Moxa's MRC solution stands out for a number of reasons: end-to-end and fully-integrated security, ease-of-use, cloud-based flexibility, and proven reliability in harsh factory conditions. Only three components—MRC gateway, a cloud server, and client software— are needed to build the cloud-based remote access connection.

Secure Network Infrastructure

- Fully-integrated secure connection with end-to-end data-encryption
- Cloud-based interconnections and security management for service scalability
- With one click, engineers with no IT expertise can access remote machines without having to perform complex firewall settings or IP management

Securing Interconnected Traffic Signal Communications

Henrico County, U.S.A., wanted to upgrade existing closed-loop traffic signaling control systems to a distributed traffic management system that was compliant with NEMA TS2. From the central command center, operators can access traffic signals at remote traffic control locations for real-time monitoring and react quicker to emergencies.

Location: Henrico County, U.S.A.
Application: Intelligent Transportation

Pro Tips

- Deploying a secure router with a firewall, VPN, and switch will encrypt data transmission and provide redundancy networks for higher reliability.

Moxa Products

EDR-810
Industrial Secure Router with Switch/Firewall/NAT/VPN

Challenges

This advanced traffic control network will be deployed across a public network and will require highly reliable connections and cybersecurity protection, such as a VPN and firewall, to ensure the integrity of system communications. In order for the traffic controllers to transmit the data smoothly to the traffic operation center, the system integrator utilized the existing ISP public network, which required modems for communication. However, the traffic control network is vulnerable to security threats, which means a VPN and firewall are essential to ensure secure data communications.

Moxa's Solution

Moxa's recommendation was to install EDR-810 secure routers in the roadside cabinet located at each intersection for data communication and data security. The EDR-810 Series supports VPN and firewall capabilities, which provides secure remote access and protects critical field devices.

Secure Network Infrastructure

- Supports 20 Mbps VPN bandwidth for VPN tunneling between field cabinets and the central traffic operation center
- 2 Gigabit fiber ports with RSTP and Turbo Ring technology for future expansions that requires optic fiber ring topology