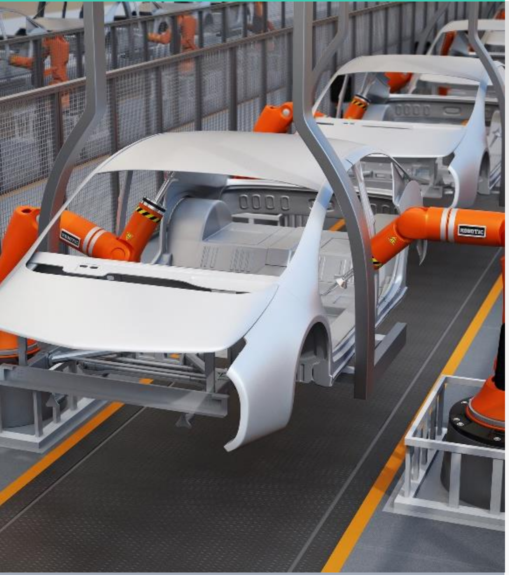
Factory Automation:
Assembly Lines



Location: South Asia

Case 1

Protect Assembly Lines From Cyberattacks

Introduction

- A global manufacturer suffered a large cyberattack and was forced to spend significant resources to get its plants back to normal. It caused not only a fall in profitability but also damage to its reputation.
- In order to achieve continuous industrial operations, the company needs its networks to be very resistant to disruptions and cyberattacks.
- To be able to prevent cyberattacks, its branch office in South Asia started to look for solutions that can enhance their operational resilience against cyberattacks.

Challenges

- Any new measures that are implemented must not interrupt existing operations.
- How to efficiently manage all devices and monitor all security incidents across 20 production and assembly lines.

MOXA®

Factory Automation: Assembly Lines

Expert Advice

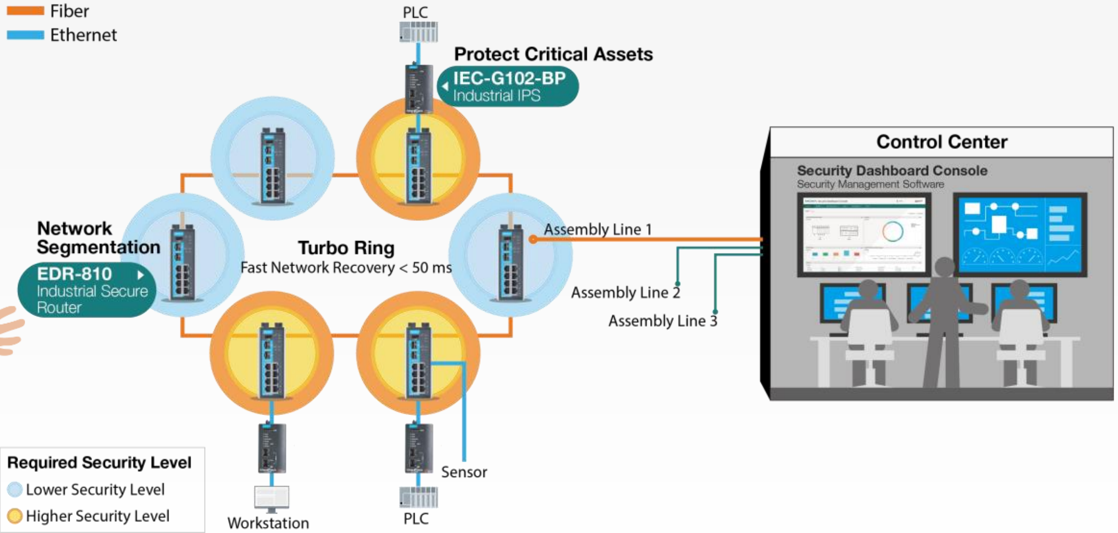
In order to protect networks and devices, a network design should ensure maximum network uptime and utilize a central management tool that can remotely configure and update all devices.

MOXA

Solution and Results

We suggest tackling the challenges from the perspectives of networking and network protection.

- To ensure maximum network uptime, Moxa’s Turbo Ring features network recovery times within 50 ms.
- Moxa’s industrial Intrusion Prevention System (IPS) devices, EtherCatch, help monitor malicious network behavior.
- With MXview and Security Dashboard Console (SDC), customers can remotely and centrally manage all network devices and trace security incidents.



Factory Automation:
Production Lines

Location: China

Case 2

Build Future-proof Network Security

Introduction

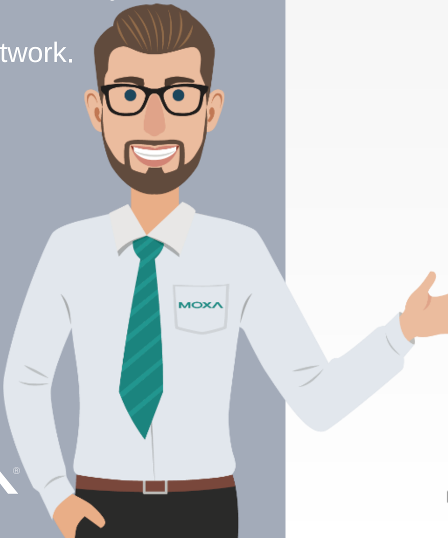
- A world-leading relay manufacturer in China is building new plants to upgrade its production lines to ensure they are ready for Industry 4.0 applications.
- In light of increasing ransomware attacks and government regulations, the company would like to build a solid foundation for its plant networks to get ready for the future.

Challenges

- The new plants are located across four buildings. There are 46 production lines and each line includes 60 devices. Due to the large-scale networks, the company needs a comprehensive and future-proof networking solution.
- The components produced by the company play an essential role within the global power generation supply chain. Any disruption to the production processes would harm its reputation and bottom lines. Therefore, the company considers network availability to be the priority for this project.

Expert Advice

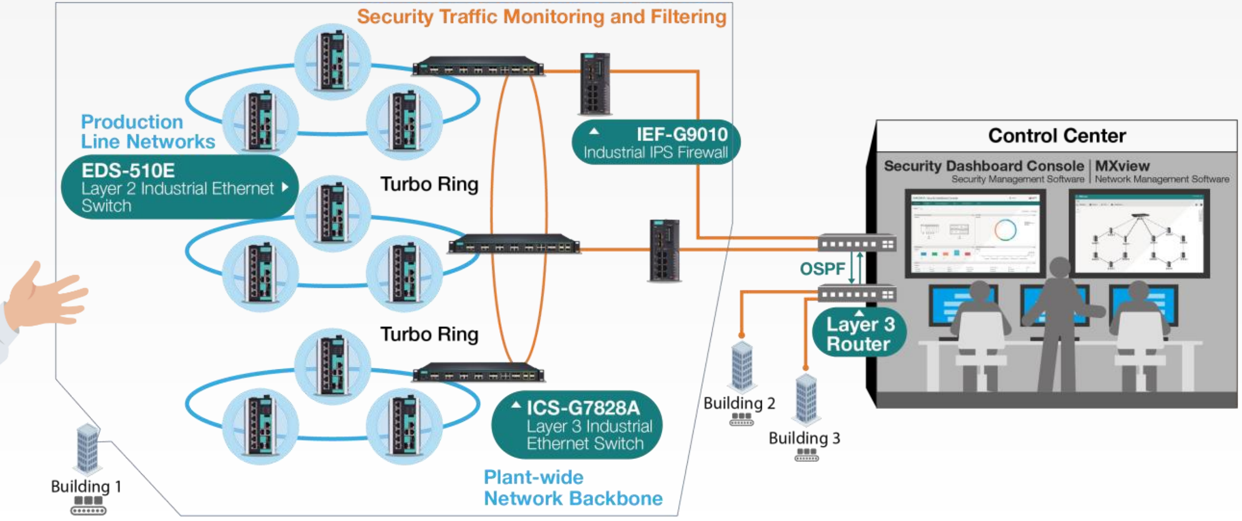
Understand your critical assets and divide them into zones based on your security policy so that you will have a better idea about how to balance the cost you can afford and the risk that you can accept even if you are managing a large-scale network.



Solution and Results

If you are considering the possibility of expanding in the future, we suggest building the plant networks from the edge to the core.

- To ensure maximum network uptime, Moxa’s Turbo Ring supports network recovery times within 50 ms. In addition to network redundancy, Moxa’s switches offer robust security features to ramp up network security.
- Moxa’s industrial Intrusion Prevention System (IPS) firewalls, EtherFire, offer a high level of protection against cyberthreats from the core level network to the edge networks.
- With MXview and Security Dashboard Console (SDC), customers can remotely and centrally manage all network devices and trace security incidents.


Security Traffic Monitoring and Filtering
Production Line Networks
EDS-510E
Layer 2 Industrial Ethernet Switch
Turbo Ring
Turbo Ring
IEF-G9010
Industrial IPS Firewall
ICS-G7828A
Layer 3 Industrial Ethernet Switch
Plant-wide Network Backbone
Building 1
Building 2
Building 3
OSPF
Layer 3 Router
Control Center
Security Dashboard Console
Security Management Software
MXview
Network Management Software

Critical Power Monitoring:
Data Center

Location: U.S.A.

MOXA®

Case 3

Enhance Cybersecurity for a Data Center

Introduction

- A data center service provider located in the U.S.A. wants to increase their cybersecurity because data centers are frequently attacked, which has resulted in data loss and significant penalties over the past five years.
- It is now a corporate-level initiative because in addition to the server room being attacked, the power sources that supply the server rooms have communication interfaces that have also been identified as vulnerable to cyberattacks.

Challenges

- To manage security risks more efficiently, the corporation must perform a vulnerability scan monthly to prevent possible attacks and urge device manufacturers to take action immediately when a vulnerability is identified.
- Cyberthreats are not the only problem that IT departments face. OT devices in data centers such as switchgear, PDU, UPS etc., also have to be protected as the circuit breaker, relay, and meters all have communication interfaces. There could be thousands of these devices, which makes monitoring and updating firmware troublesome.

Critical Power Monitoring: Data Center

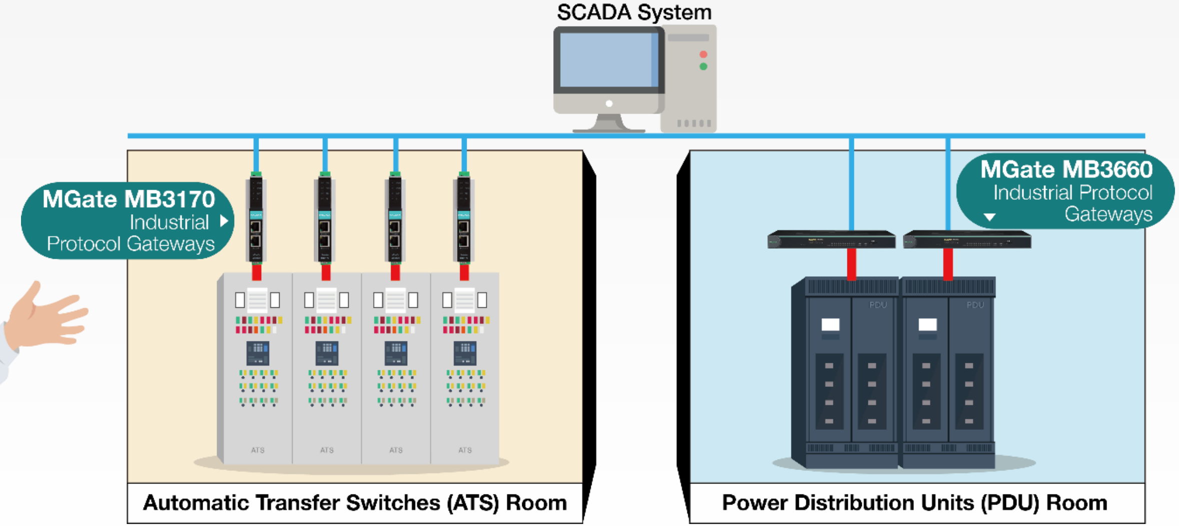
Expert Advice

A network security plan with proper device selection can greatly reduce the chances of being hacked and losing money or causing damage to your companies' reputation.

Solution and Results

To reduce the chances of being hacked and suffering financial losses, any network node should have embedded security functions to ramp up device security.

- Moxa's MGate MB3170 and MB3660 protocol gateways were designed based on the IEC 62443 standard, ensuring cybersecurity is embedded within the device.
- Frequently perform vulnerability scans to ensure the latest patch can be obtained by users for critical applications that can be subjected to cyberattacks.
- Moxa's MXconfig has an easy-to-use GUI and our MCC, which is a CLI tool that simplifies performing configurations, makes it easier for both OT and IT users to make mass firmware updates.



Power & Energy:
Energy Storage

Location: U.S.A.

MOXA

Case 4

Enhance Remote Connection Security for a Li-ion ESS

Introduction

- A grid-level energy storage system (ESS) builder developed their ESS using Li-ion batteries. The batteries could be used multiple times before needing to be replaced and there was good energy storage for multiple battery sizes.
- There are safety concerns about Li-ion batteries. When the battery is coming to the end of its lifecycle, it requires constant monitoring to avoid a catastrophic accident such as catching fire or exploding.

Challenges

- How to monitor the state of the batteries in the ESS in real time and have an early warning system to prevent the batteries from overheating and failing or even causing a fire.
- As an ESS is commonly used with power grids, it is often targeted by hackers. It is important that system integrators carefully select communication devices that have higher levels of security protection such as HTTPS with TLSv1.2 to mitigate these risks.
- An ESS is often located in remote areas, which increases maintenance tasks, especially in the event of an unexpected failure.

Power & Energy:
Energy Storage

Expert Advice

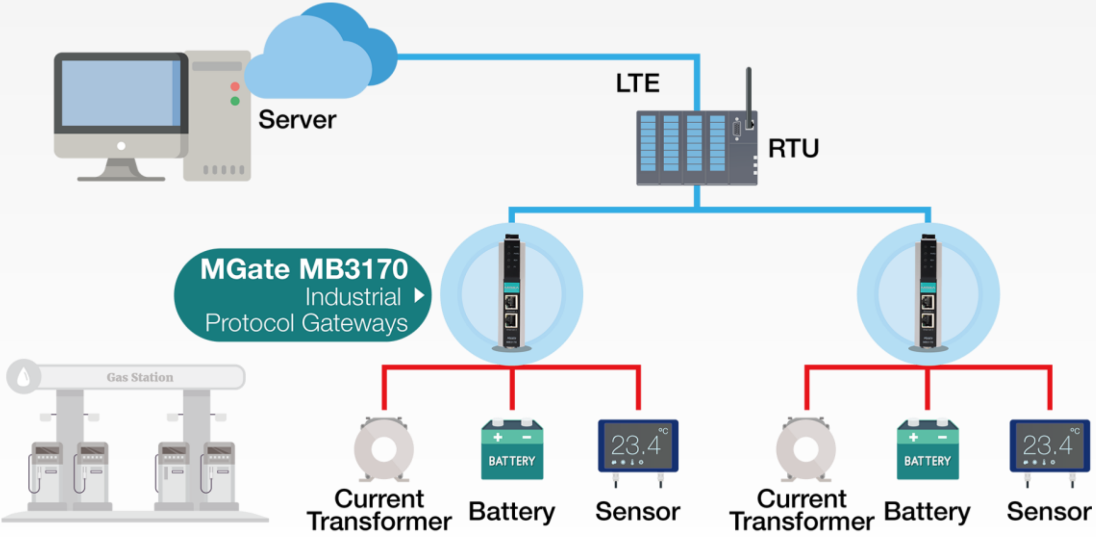
Remote communication requires a secure protocol such as HTTPS or SNMPv3 to enhance your connectivity security when using public networks.

MOXA

Solution and Results

To develop seamless and secure communications between an ESS and the control center, we suggest a reliable edge connectivity solution deployed in between.

- MGate MB3170 protocol gateways facilitated communications between Modbus serial-based batteries and Ethernet-based RTUs.
- Security features such as HTTPS, SNMPv3 management, and Accessible IP Addresses to ensure the communication and access of the device is securely protected, reducing the risk and making remote communications more reliable.



Power and Energy:
Energy Storage

Case 5

Safeguard the Energy Storage System

Location: France

Introduction

- Following the trend of decarbonizing the global economy, a grid-level energy storage system (ESS) builder is expanding its ESS capacity for renewable energy.
- Its mission is to provide a reliable and affordable ESS, as this is key for grid operators to be able to balance power demand and supply during peak and off-peak times.
- Thus, the reliability of the power grid through flexible power storage capacities, especially batteries, becomes essential.

Challenges

- The energy management system (EMS) monitors operations of the ESS in real time. It aggregates the data collected from the power conversion system (PCS) and battery management system (BMS) containers. The entire network needs to be protected from unauthorized access and any unexpected activity that may disrupt operations.
- The security mechanisms need to be designed when containers are being manufactured in the plants to ensure the whole system can be efficiently deployed to the farm and grid.
- As an ESS is often located in remote harsh environments, it is challenging to ensure reliability and security.

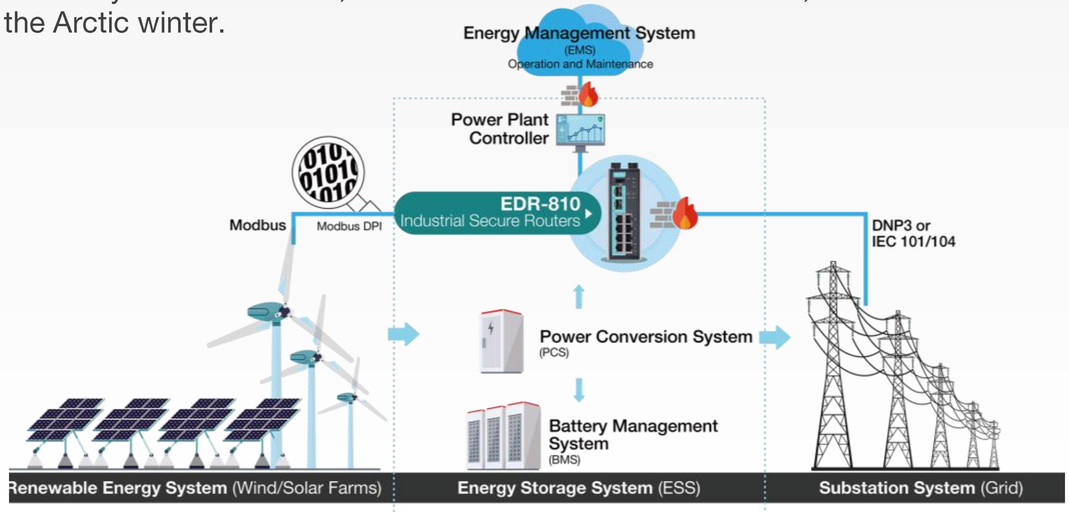
Expert Advice

Embrace the defense-in-depth concept and leverage deep packet inspection technology to perfect vertical and horizontal network protection and ensure continuous operations.

Solution and Results

To protect the communications between the power plant controller and the PCS and BMS containers, we suggest stateful firewalls with Modbus deep packet inspection (DPI) deployed in between.

- The EDR-810 industrial secure routers build the security boundary, and its Modbus DPI function safeguards the Modbus communication in between the systems.
- With an all-in-one firewall/NAT/VPN/switch and network redundancy functions, the EDR-810 can help system integrators design the network architecture and expand connections more efficiently.
- The EDR-810 was built to operate reliably on the harshest uncrewed remote solar/wind farms in dry and hot deserts, brutal offshore weather conditions, and even in the middle of the Arctic winter.


Energy Management System
(EMS)
Operation and Maintenance
Power Plant Controller
010
0101
010
Modbus
Modbus DPI
EDR-810
Industrial Secure Routers
DNP3 or
IEC 101/104
Power Conversion System
(PCS)
Battery Management System
(BMS)
Renewable Energy System (Wind/Solar Farms)
Energy Storage System (ESS)
Substation System (Grid)