Defense in Depth:

Networking Security for Modern Energy Storage Systems

Product Highlights

BESS Integration

Firewall:
EDR-G9010 Series

- Developed according to the IEC 62443-4-1 and certified with the IEC 62443-4-2 industrial cybersecurity standards
- 10-port Gigabit all-in-one firewall/NAT/VPN/router/switch
- Industrial-grade Intrusion Prevention/Detection System (IPS/IDS)

Core Switch:
RKS-G4028 Series

- Meets a wide range of demands from Fast Ethernet to full Gigabit industrial networks (up to 28 Gigabit ports)
- Modular interfaces for flexible connector type combinations
- Support for IEEE 802.3bt PoE for up to 90 W output per port

Battery Container

Environmental Management Controller :
UC-2100 Series

- Arm Cortex-A8 600-1000 MHz
- Palm-sized form factor, 50 x 80 x 28 mm
- MXview One support for centralized
- monitoring of devices and computing status

Firewall Switch:
EDR-8010 Series

- Industrial-grade Intrusion Prevention/ Detection System (IPS/IDS)
- 8 FE + 2 Gigabit port all-in-one firewall/NAT/ VPN/router/switch
- Visualize OT security with the MXsecurity management software

Remote I/O :
ioLogik E1200 Series

- User-definable Modbus TCP Slave addressing
- Supports RESTful API for IIoT applications
- Supports EtherNet/IP Adapter

An energy company in Australia completed a significant energy project by building the country's initial large-scale Battery Energy Storage System (BESS) to improve market engagement and boost the integration of renewable energy. Yet, once the system was up and running, the company discovered that typical cybersecurity methods were not enough to handle the growing internal and external threats. Due to the crucial function of these systems in energy management and stability, the security issues related to BESS have grown more complex and critical. In general, BESS cybersecurity challenges fall into the following three categories:

Authorization Management and Access Control: BESS systems often lack strict network access control (NAC) and proper authorization management, leading to increased risks from unauthorized remote access and internal vulnerabilities. Moreover, if third-party contractors or maintenance workers are not effectively supervised, they may unintentionally create security weaknesses, elevating the system's risk level. It is crucial to enforce strict regulation of network access permissions to reduce these risks.

Device Security and System Updates: Industrial control devices in BESS often accumulate vulnerabilities over time due to challenges with maintenance, preventing timely firmware updates and security patches. Besides, allowing unverified or unmanaged devices to connect to the network can lead to potential cybersecurity vulnerabilities.

Network Complexity and Trust Management: In applications such as FSS, HVAC, BMS, PCS, EMS within BESS, there are significant data exchanges between devices, surpassing the connectivity complexities of traditional isolated industrial networks (air-gapped networks). Integrating cloud applications presents challenges in maintaining a secure network due to the ineffectiveness of traditional physical isolation against cyberthreats. Effective implementation of network security zone segmentations is crucial for advanced cybersecurity management strategies.

Recognizing these risks, the company decided to implement Moxa's **Defense-in-depth** strategy, which offers multi-layered protection to enhance the resilience and stability of their system.

System Requirements

To protect the smart energy storage system, the following cybersecurity measures are essential:

- Ensuring network access and authorization are properly managed and monitored.
- Controlling the impact scope during network attacks.
- Securing network resilience and device stability to handle abnormal behaviors or attacks.
- Providing real-time network and security monitoring for swift crisis management.
- Establishing a disaster recovery plan with regular equipment configuration maintenance and data backups.

Why Moxa

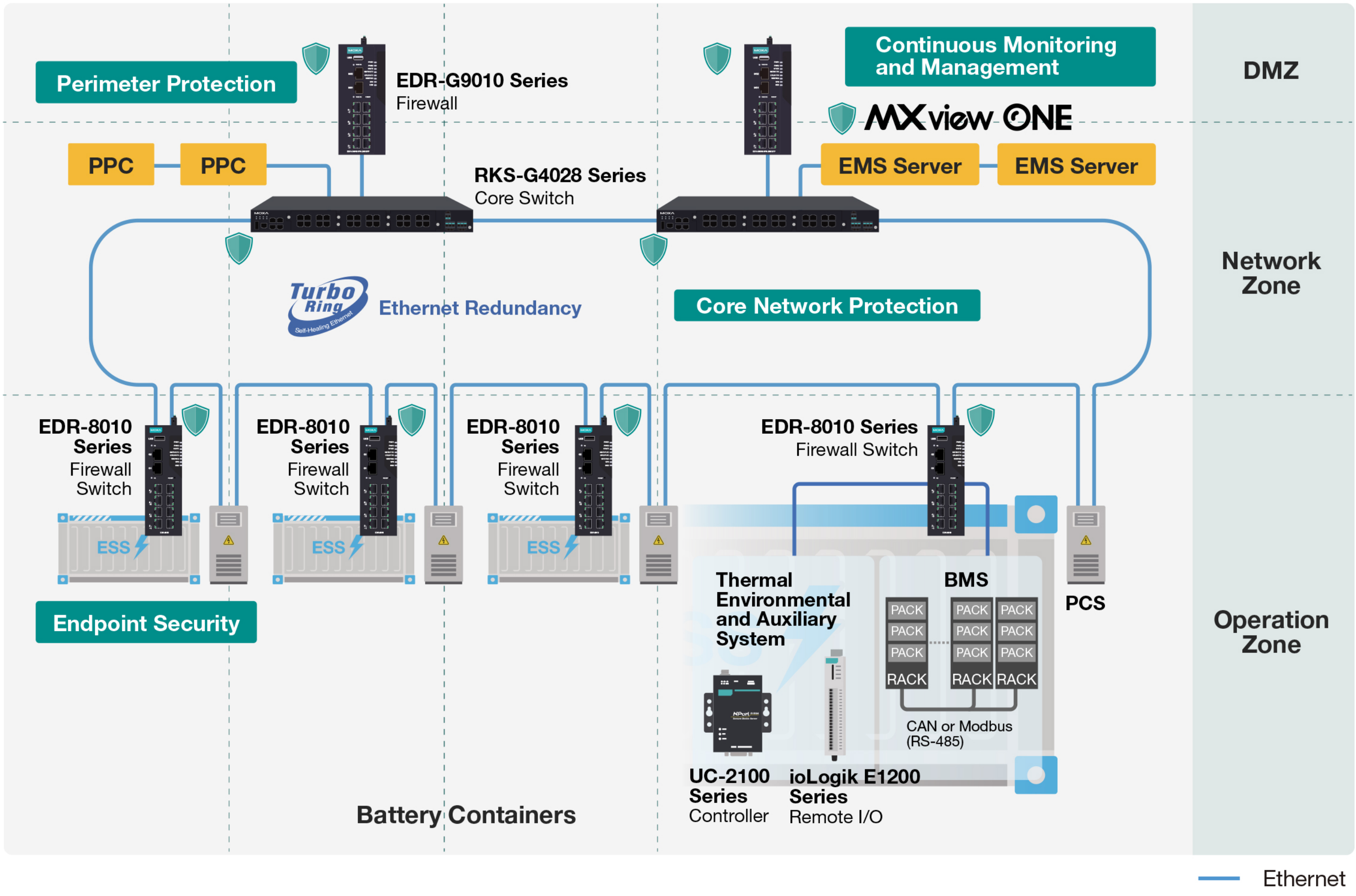
Moxa is one of the first companies worldwide to receive IEC-62443-4-1 certification, demonstrating a deep understanding of the unique cybersecurity needs in industrial environments. Moxa helps BESS partners establish strong networking security through Defense-in-depth solutions, aiding in effectively addressing both internal and external risks.

- **Perimeter Protection:** Moxa's EDR Series firewall switches are equipped with Intrusion Detection and Prevention (IDS/IPS) capabilities to block external attacks. Additionally, the EDR Series can perform logical segmentation, restricting communication between different network zones to minimize the attack surface. Network segmentation and cyberthreat defense are key components in strengthening perimeter security, ensuring that potential vulnerabilities are contained and managed effectively.
- **Core Network and Endpoint Protection:** Moxa's industrial-grade switches offer authentication and authorization functions, ensuring only authorized devices and users can access the network. With port mirroring technology, real-time network traffic monitoring allows early detection of anomalies. Additionally, preventing unauthorized connections between critical controllers in BESS, PCS, and other key components is crucial to maintaining network integrity and security. Moxa's endpoint security solutions include firmware updates, virus protection, and intrusion detection, ensuring stable operation of endpoint devices. Integrating core network security and endpoint measures creates a unified defense strategy for the whole infrastructure.
- **Continuous Monitoring and Management:** Moxa's network management software provides centralized network configuration, monitoring, and troubleshooting, with log analysis and anomaly detection to identify potential threats proactively.

Moxa's comprehensive solution delivers multi-layered networking security protection for energy storage systems, securing the perimeter, core network, and endpoint devices, ensuring customers are well-prepared for future challenges.

System Diagram

Moxa's BESS Defense-in-depth Strategy


Perimeter Protection
EDR-G9010 Series
Firewall
Continuous Monitoring and Management
MXview ONE
DMZ
PPC
PPC
EMS Server
EMS Server
RKS-G4028 Series
Core Switch
Network Zone
Turbo Ring
Self-Healing Ethernet
Ethernet Redundancy
Core Network Protection
EDR-8010 Series
Firewall Switch
EDR-8010 Series
Firewall Switch
EDR-8010 Series
Firewall Switch
EDR-8010 Series
Firewall Switch
ESS
ESS
ESS
Thermal Environmental and Auxiliary System
BMS
PACK
RACK
CAN or Modbus (RS-485)
PCS
Operation Zone
Endpoint Security
UC-2100 Series
Controller
ioLogik E1200 Series
Remote I/O
Battery Containers
Ethernet