WHITE PAPER

# How to Protect Substation Automation Systems From Cyberthreats

**King Wu**
*Software R&D Manager*
*Energy Sector*

MOXA®

## Executive Summary

Digitization has permeated nearly all aspects of daily life and the power grid is no exception. Today, sophisticated and highly complex digital systems are used to both monitor and control the power grid to ensure the safe and reliable supply of electricity. With the advance of the digital grid, it has become inevitable for critical infrastructure to be connected to a wide area network (WAN). With this high demand of connectivity, the vulnerability of these critical infrastructures, such as power substations would be key weaknesses to be exposed by hackers. If the power grid is successfully compromised by hackers, wide area blackouts and great economic losses may occur. This is why it is critical to protect the power grid and substation automation systems (SAS) from cyberthreats.

With respect to digital power grids, cybersecurity requirements may be defined as guidelines (e.g., NIST), standards (e.g., IEC 62443), or regulations (e.g., NERC-CIP) that cover many different aspects of organizational, operational, or process security.

## Cybersecurity and the Digital Power Grid

The NERC-CIP standards provide a cybersecurity framework to identify and secure critical assets that can impact the efficient and reliable supply of electricity through North America's bulk electric systems (BES), which are the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. When it comes to regulatory compliance, different regulatory regimes, jurisdictions, organizations, ownership, scales, and use cases may lead to different requirements, schedules, and risk management. As such, compliance could be costly and time-consuming for operators and related costs may eventually be transferred to end users, which hurt the wider community and economy.

For this reason, compliant-ready cybersecurity solutions that can bring power grid-related systems and applications up to standards and enhance overall security are sought after as they help reduce costs while ensuring reliable BES operations. Thanks to the availability of industrial networking equipment and platforms suitable for protecting the power grid, robust monitoring and protection of cyber systems can be performed more easily without having to design and implement a cybersecurity architecture from scratch.

Released on March 21, 2023



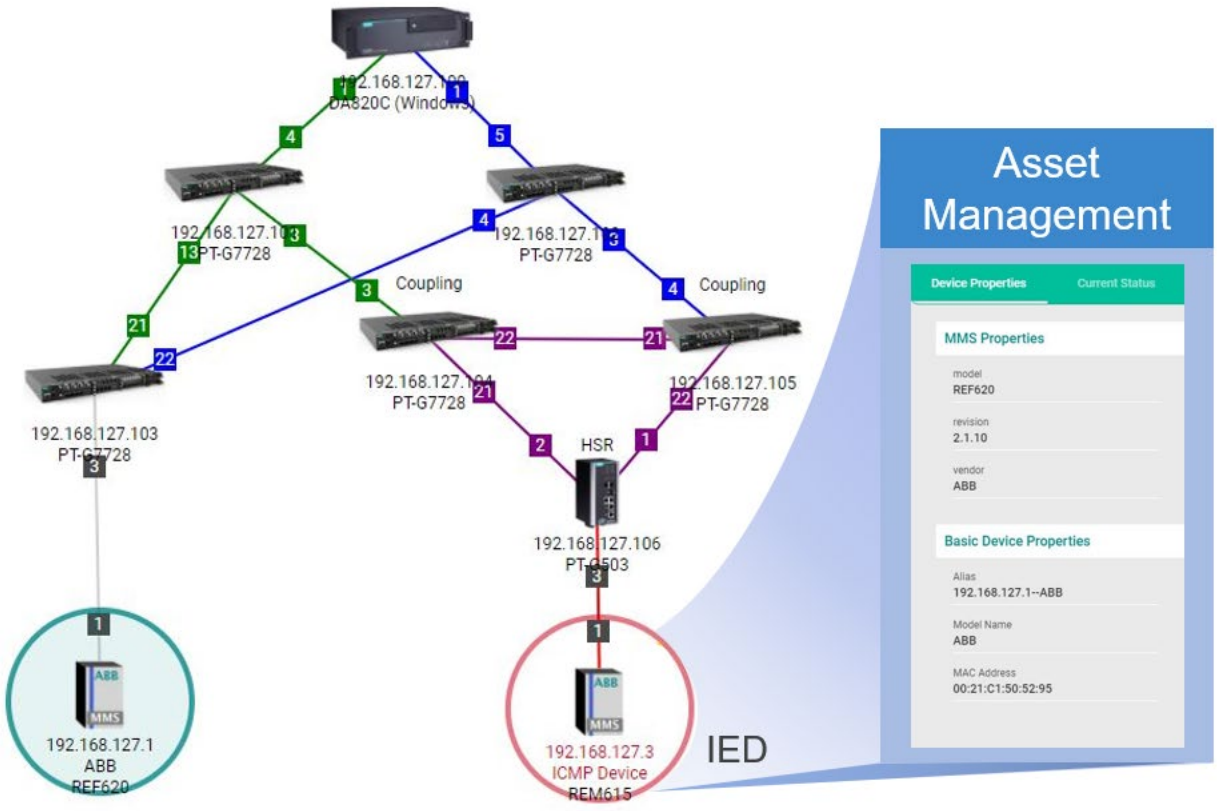
Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

**How to contact Moxa**
Tel: 1-714-528-6777
Fax: 1-714-528-6778

- **Improve Asset Visibility With System Visualization**

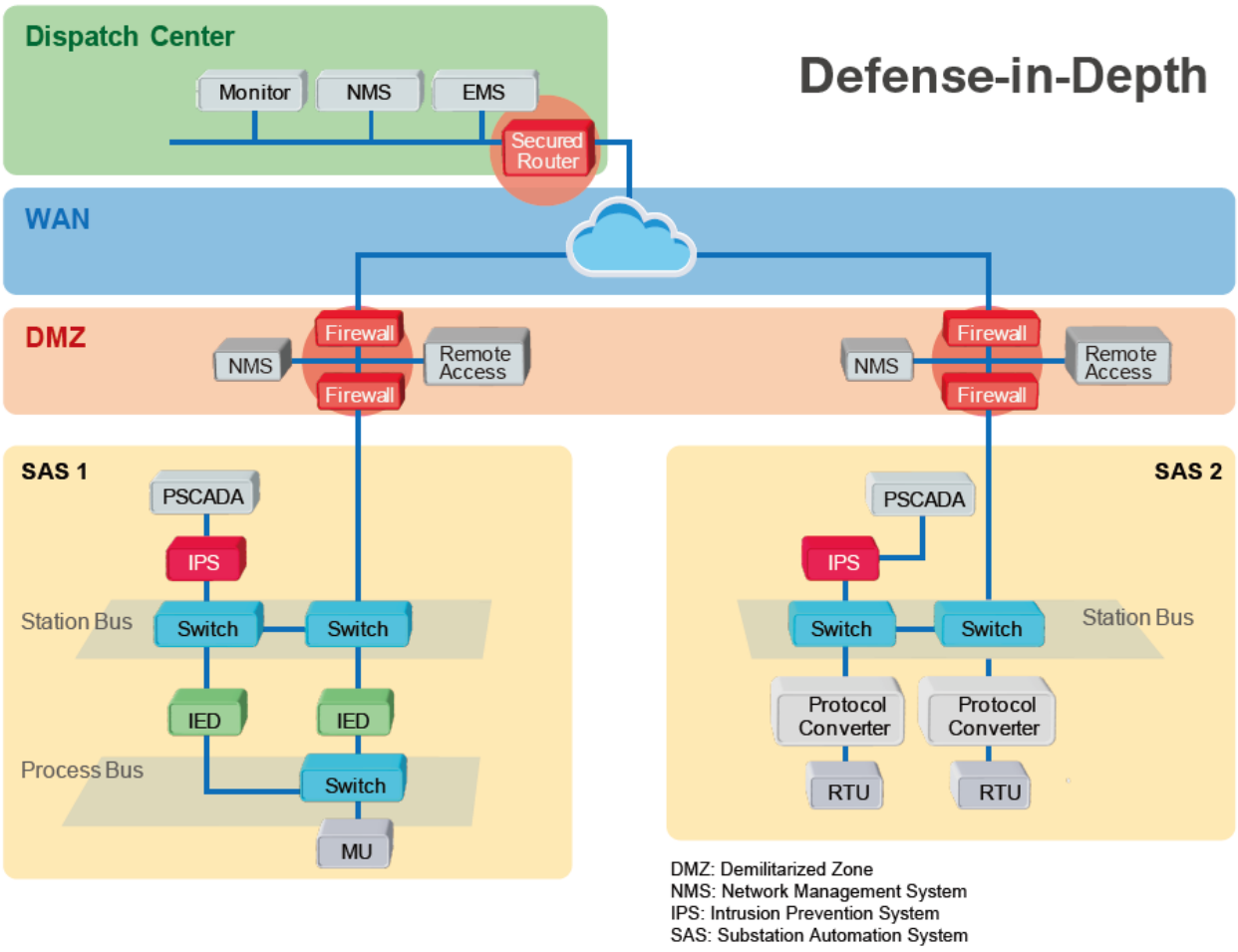
Protection becomes easier when the operator knows what is there to protect. Complex IT and OT configurations, as in the case of power substation automation, consist of hardware and software components and OT equipment that come from multiple suppliers and use different operating systems or communication protocols. From the security standpoint, the setting is less than ideal because making every component secure necessitates having a holistic view of the system and knowing where the assets' vulnerabilities, if any, are. Thus, risk mitigation measures (such as network segmentation or system monitoring, discussed later in this whitepaper) can be implemented when there is clarity on the system setup, component attributes and behaviors, and data-transmission patterns.

When power system engineers choose a cybersecurity device, perhaps the software platform from the device supplier is just as important as the device itself. To improve asset visibility, a platform featuring system visualization that includes network topology and listing the inventory of IEC 61850 devices can offer engineers useful information on how best to protect the system from cyberthreats and manage it for optimal performance.



- **Implement Network Segmentation**

Cyberattacks, unfortunately, remain a fact of life. As substation automation systems will face the challenge at some point, it is a best practice to reduce a system's exposure to external cyberthreats by fencing off part of the system, that is network segmentation. There are two major benefits to network segmentation. First, network segmentation prevents one micro control system, such as a bay, from disturbing others, for instance, during a failure. Second, as data is stored in different network segments, it minimizes access to sensitive data should system security be unfortunately compromised and mitigates the loss and damage to the system. Moreover, segmentation can also help implement the least privilege principle (or the need-to-know basis), as it limits access to users who do not need the data to do their work.




Network segmentation can be achieved using a number of techniques and technologies depending on the network's architecture and configuration. For example, within a local area network (LAN), users can apply Virtual LAN (VLAN) technology to segregate a micro control system or adopt Layer-3 switches or routers to segregate an IP network. Network segmentation, when implemented properly, is an effective tool to enhance protection from unauthorized access and untrusted networks.

- **Build Next-Generation Perimeter Protection**

The security perimeter, which is capable of monitoring and managing access points, is the primary defense of the power cyber system. Installing access point protection devices protects the assets within the identified perimeter. Today, the increasing popularity of the next-generation firewall (NGFW) speaks volumes for the effectiveness of its advanced security features. NGFW supports deep packet inspection (DPI) or intrusion protection system (IPS) to proactively block abnormal communication patterns. As such, NGFW helps enhance security regarding remote access to critical control, beefing up overall security. Preferably, the NGFW interface of choice is intuitively designed and user-friendly, allowing OT operators with no or little IT background to turn on proactive protection for BES cyber systems.

- **Keep System Security Management Up to Date**

Developing a sound security policy, implementing the policy with practical procedures, and applying adequate security technologies are the three pillars of a secure system. Even with state-of-the-art protection devices, technology alone is inadequate if there are loopholes in the security policy or its implementation.

By adopting best practices for secure network design and solutions, digital power grids can effectively strengthen their cybersecurity. The following table summarizes the main purpose for several key NERC-CIP requirements that impact power grid cybersecurity and provides several solutions that can help you satisfy these requirements.

| Requirement | Purpose | Moxa Solution |
|---|---|---|
| CIP-002-5.1a BES Cyber System Categorization | To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cybersecurity requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. | MXview Power (network management tool): Identify cyber assets |
| CIP-005-6 Electronic Security Perimeter(s) | To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. | MXview Power (network management tool): Monitor cyber assets<br>EDR-G9010 (secure router): Support IPS on EAP<br>Moxa Remote Connect (MRC): Secure remote access |
| CIP-007-6 System Security Management | To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). | Moxa switches and routers with service/physical port management<br>MXsecurity: Security event management<br>EDR-G9010 (secure router): Malicious code prevention |
| CIP-008-6 Incident Reporting and Response Planning | To mitigate the risk to the reliable operation of the BES as the result of a Cybersecurity Incident by specifying incident response requirements. | Moxa PSIRT: Security incident response plan |
| CIP-009-6 Recovery Plans for BES Cyber Systems | To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. | MXview Power (network management tool): Configuration management |

## Summary

Substation automation systems are integral to BES security and the entire power grid. As new cybersecurity regulations and guidelines are being introduced under NERC's CIP program, utilities will be mandated to ensure that substation automation systems comply with regulations and are capable of tackling cyberthreats. Even utilities outside of North America can refer to these guidelines to shore up their own domestic power grid security. Best practices such as improving critical assets visibility, implementing network segmentation, building robust perimeter protection, and enhancing system security management will help make systems more secure.