Boosting Cybersecurity for Your Substation Automation Systems With Secure IEC 61850 Gateways

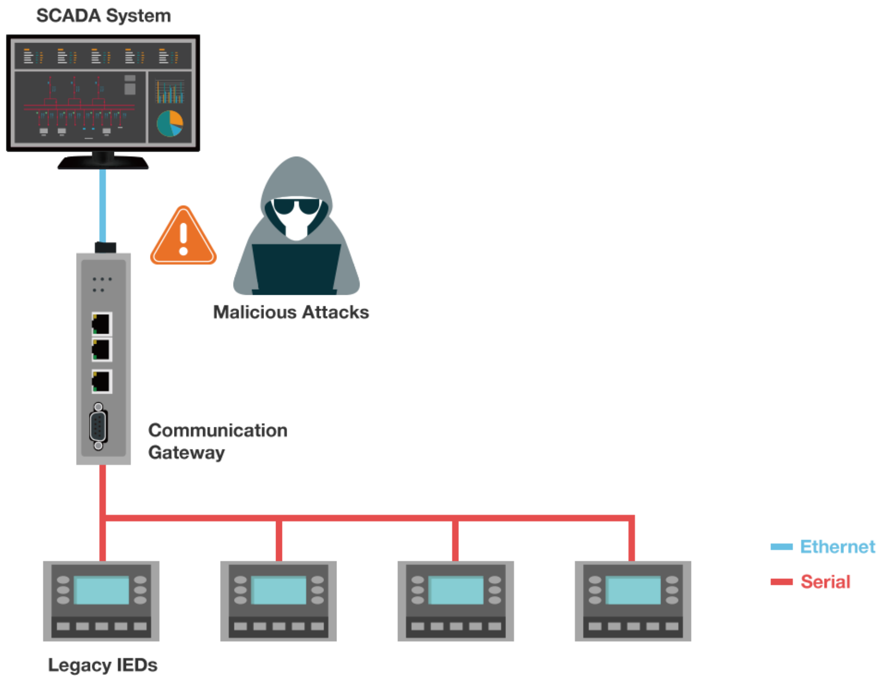
Because of a significant surge in distributed energy resources (DERs) and energy storage systems, along with the upward trend of unmanned substations, power grids have become a lot more complex. So far, DERs are having the biggest impact on power grids because of their intermittent energy production. At times, they generate too much power; other times, their output is too low. These fluctuations make the grid unreliable.

For this reason, engineers in substation control centers find it increasingly difficult to manage the dispatch of power in real time. To address these instabilities in power grids, digital substations, which provide stability and flexibility regarding power supply, increasingly play an important role in power transmissions. However, converting all substations to digital at once is not so straightforward because of limited budgets to retrofit the large number of serial-based legacy devices.

Communication gateways can help overcome these concerns as they help serial-based intelligent electronic devices (IEDs) communicate with Ethernet-based networks. They are also a cost-effective solution compared to computing platforms. With the serial-to-Ethernet problem solved, however, another issue raises its head: cyberattacks always pose enormous threats to Ethernet-based networks, putting cybersecurity in retrofit power substations at the forefront.

The Importance of Cybersecurity for Substation Automation Systems

Substation protection and control systems manage critical power operations through communication protocols. In substation retrofitting projects, communication gateways act as data concentrators, managing the large numbers of legacy IEDs. Despite their significantly important role, communication gateways rarely incorporate adequate security measures. Therefore, a high risk exists that malicious attackers can easily access legacy IEDs through these gateways to cause system downtime, power outages, and damage to critical equipment, resulting in huge financial losses. What’s even worse, people’s lives can also be in danger.



The IEC 62443 standard has become one of the most popular cybersecurity standards for industrial automation and control systems. For specified critical power automation systems, also consider a specified power standard such as IEC 62351. When incorporating the acknowledged technologies of both standards, it's essential for operators to consider methods that can protect your critical data and track your network security status.

Encrypt Your Critical Data to Reduce Cyberattacks

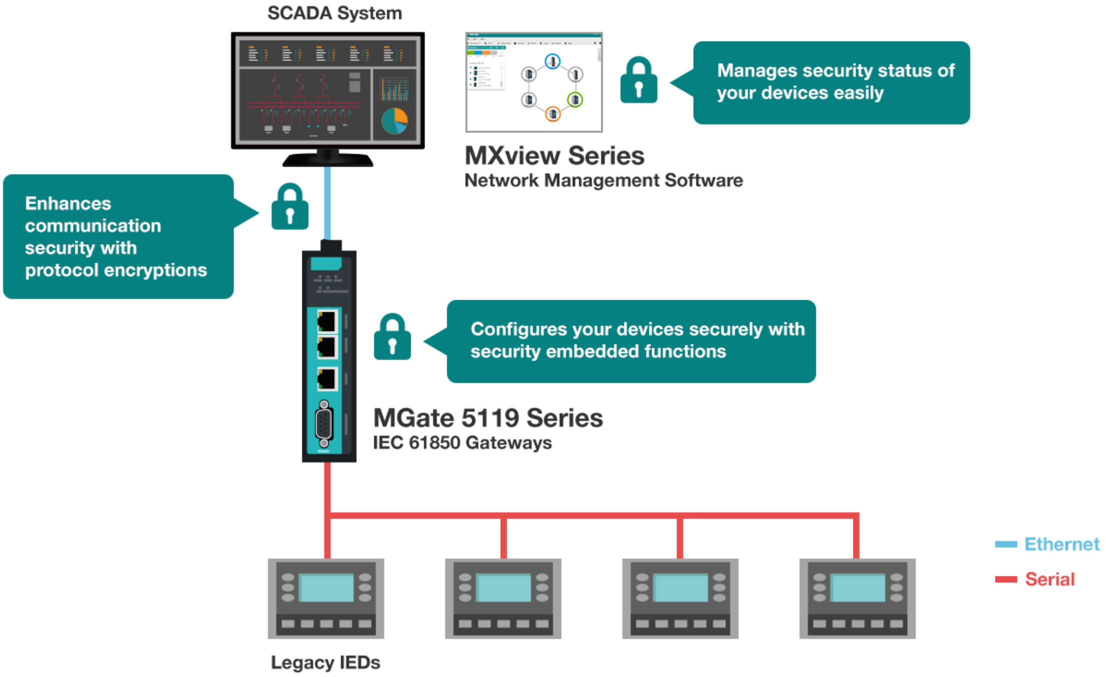
Once hackers invade your substation networks, they can easily capture data and learn a lot about your network communication behavior. What's more, they can easily cause havoc by sending a wrong command to control the IEDs. To counteract these types of malicious activities, your communication gateways must encrypt data for communication protocols such as DNP3 TCP and IEC 61850 MMS.

Monitoring the Security Status of Networks and Malicious Behavior

For monitoring and controlling IEDs in refurbished substations, it is critical to make the network infrastructure more secure. The status of network devices, such as switches, IEDs, and communication gateways must always be monitored. For example, if the links of an Ethernet port of a network device are down or malicious behavior is detected, the gateway will send an alarm message to the information system immediately. When the information system receives the alarm, engineers can handle this problem in a timely manner.

Your Secure IEC 61850 Substation Gateways

We designed our MGate 5119 Series IEC 61850 gateways to secure your devices from configuration to daily maintenance. They also enhance your communication security, ramping up network security for your retrofitted substations.


SCADA System
MXview Series
Network Management Software
Manages security status of your devices easily
Enhances communication security with protocol encryptions
Configures your devices securely with security embedded functions
MGate 5119 Series
IEC 61850 Gateways
Ethernet
Serial
Legacy IEDs

Configure Your Devices Securely With Security Embedded Functions

Your substations are exposed to potential threats once they connect to networks. Thus, all networking nodes need to be protected from intruders. Based on IEC 62443 and NERC CIP guidelines, our MGate 5119 Series IEC 61850 gateways provide multiple security functions to ensure your device is secure in the initial configuration process.

- Password-cracking defense: Using default passwords for convenience is not an option anymore. Our IEC 61850 gateways have a password policy that encourages you to use stronger passwords to avoid unwanted access.
- Sniffer and data breaches protection: Using plain text for your device configuration can be dangerous. Our IEC 61850 gateways provide SSL/TLS to encrypt your critical data during configuration process.
- Configuration file and program tampering resistance: When you export your configuration files for backup, our IEC 61850 gateways will encrypt the file to enhance file’s integrity.
- DDoS defense with built-in detection capabilities of suspicious activities: DDoS

attacks are usually carried out by occupying your network bandwidth or attacking the resources of your networking devices. Our IEC 61850 gateways help you detect abnormal packets and alert you for instant responds.

Enhance Communication Security With Protocol Encryptions

If your data communications are not encrypted, then hackers can capture the plain text data easily. From the plain text data, hackers can figure out how to control your IEDs and subsequently send out a fake control command to them, which could endanger your substation operation. Our MGate 5119 Series IEC 61850 gateways support TLS v1.2, which secures data transmission between communication gateways and a power SCADA system, using standard communication protocols such as IEC 61850 MMS and DNP3 TCP.

Manage Security Status of Your Devices Easily

Security is not a onetime event, but a journey that requires you to constantly monitor device security status in daily operations. Our MGate 5119 Series IEC 61850 gateways support MXview network management software, which provides intuitive network topology to help users easily check device status. Moreover, you can monitor user-defined security events and bring violations to the administrator’s attention. This way, engineers can easily check and ensure our IEC 61850 gateways operate at the accepted security level.

In addition to enhancing your communication security, our MGate 5119 Series IEC 61850 gateways also come with handy functions that make configuration and troubleshooting efficient for you. Our industrial-grade design also ensures operational reliability for your critical applications in substation retrofits projects.