Cybersecurity in low-voltage power distribution

From the field level to the cloud
siemens.com/lowvoltage/digitalization

Digitalization has many advantages, but it also heightens the risk of financial loss due to increased professional cyberattacks. In the case of infrastructures like power grids, there's even a threat of supply bottlenecks. Because the threat is especially high on the low-voltage level, Siemens has developed a comprehensive cybersecurity approach to ensure the protection and secure operation of the relevant components and plants.

Comprehensive protection from cyber threats is provided by the defense-in-depth concept, which Siemens also recommends. This is a higher-level, all-encompassing information security concept that ensures plant security, network security, and system integrity.

One important element of this concept is direct contact with the field level. For IoT-capable components, connectivity to the Internet means that they need to meet the same high cybersecurity standards as other connected systems. Only then can they guarantee the operational reliability of a company or building over the long term. Security features integrated directly into devices have to be part of every comprehensive cybersecurity concept. Specific starting points include the systematic management of vulnerabilities throughout a component's entire lifecycle, account management, write-access restrictions, and signed firmware.

Cybersecurity is the foundation for secure operations

As a rule, Siemens uses only signed firmware in its communication-capable products. This means that only software produced by Siemens can be installed and operated on a given IoT device, which prevents third parties from modifying the firmware.

The installation of updates is a critical procedure because third parties can theoretically upload malware code with manipulated updates. Signed Siemens firmware prevents this. An attempt to tamper with the code automatically causes the signature to change. The device then recognizes that the update is untrustworthy and prevents its installation. In many devices, password protection can also be used to prevent unauthorized modification of the configuration. In addition, the configuration of an IP address filter ensures that only specific IP addresses recognized by the user will be allowed to communicate with the devices.

SIEMENS

Security implemented on all levels

One example of how consistent, end-to-end cybersecurity can be implemented from the field level to the cloud is the 3WA air circuit breaker. Security features integrated in the device itself protect the circuit breaker from manipulation attempts. For example, the PROFINET IO/Modbus TCP module COM190 has parameter-write and remote-switching protection integrated right in the hardware. This means that when hardware write protection is activated, no parameters can be changed, whereas when remote switching protection is activated, devices can't be switched on or off via a communication path. Both features are always activated as a factory default and must be manually – meaning deliberately – switched off on the communication module itself. If the 3WA air circuit breaker is installed in an access-restricted service room, the parameter-write and remote-switching protection becomes an insurmountable obstacle for unauthorized third parties attempting access, because protection can only be deactivated locally at the circuit breaker.

Depending on the applications where the 3WA air circuit breaker is used, it can be useful to switch them on or off remotely via the communication interface. The COM190 communication module with remote switching protection ensures that remote switching is possible only if the operator provides for it. Deactivating remote switching protection involves bridging two terminals. Like parameter-write protection, remote-switching protection is activated as a factory default and has to be intentionally bridged when needed.

Remote switching is activated via a separate channel – for example, a programmable controller (PLC) – as needed and is then blocked. The remote switching itself is performed by another application, like an energy management system. As a result, remote switching can only occur via two independent paths, which makes unauthorized switching by hackers or malware much more difficult.

Bluetooth access is carefully safeguarded

The Bluetooth functionality of the 3WA air circuit breaker allows it to be accessed via the SENTRON powerconfig mobile app. Comprehensive security precautions like encryption are applied. The Bluetooth interface is also deactivated by factory default and has to be switched on via the display of the ETU600 electronic trip unit. After use, the Bluetooth interface must be switched off in order to prevent improper access. To pair with the 3WA air circuit breaker, a one-time PIN is used that's assigned by Siemens. It's newly generated for each 3WA air circuit breaker and loaded onto the units during production. After the initial pairing, the operator need to change this PIN.

The 7KN Powercenter 3000 IoT data platform can be implemented as a gateway to the cloud. It collects information on energy values from lower-level, communication-capable devices. This data is subsequently visualized and evaluated via cloud-based applications (for example, MindSphere). Communication via a single gateway that's protected by safety features guarantees data security. Use of the 7KN Powercenter 3000 safety features is made possible, for example, by utilizing the 3WA air circuit breaker's Modbus TCP whitelist and entering the 7KN Powercenter 3000 in the list of approved IP addresses.

SENTRON powerconfig software commissions and parametrizes the 3WA air circuit breakers. Access can be restricted using the Modbus TCP whitelist and by parameter-write protection on the COM190 communication module.

Cybersecurity always matched to the latest threats

By taking these measures, Siemens has laid the foundation for cybersecure products. Because the threats are continuously changing and evolving, Siemens is also constantly engaged in developing new security technologies that reduce risks. Communication-capable devices help make operating in Industrie 4.0 more efficient, and they also save resources. The number of applications based on communication is steadily increasing. A powerful cybersecurity concept supported by security features installed in the devices ensures that operators can safely use these applications and enjoy all the benefits.

Published by
Siemens AG

Smart Infrastructure
Electrical Products
Siemensstrasse 10
93055 Regensburg
German

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article No. SIEP-B10219-00-7600
TH S22-220463 DA 0123

SIEMENS