Cyberattacks on industrial automation and control systems are real and increasing in frequency, leading to large financial losses.

HITACHI
Inspire the Next

Deliver peace of mind

RTU cybersecurity solutions

Hitachi Energy

RTU cybersecurity solutions

deliver peace of mind.

A major European transmission system operator's network is now secure from cyber threats. Cyberattacks on industrial automation and control systems are real and increasing in frequency, leading to large financial losses.

Cyberattacks on industrial automation and control systems are real and increasing in frequency, leading to large financial losses. Cybersecurity has become an issue with the introduction of Ethernet based communication protocols into industrial automation and control systems.

Connections to and from external networks (remote access, office intranet) with industrial automation and control systems have opened these systems to the possibility of misuse and cyberattacks. Each "connection point" should now also be considered a potential "hacker point".

01

Hitachi Energy secures substation communications and data integrity with advanced new cybersecurity features for a major European TSO.

Customer challenges

Hitachi Energy's customer is one of Europe's main transmission system operators (TSO) and responsible for developing and managing high-voltage and very high-voltage electrical transmissions throughout its country. At the same time they are also the majority owner of the country's high-voltage transmission grid.

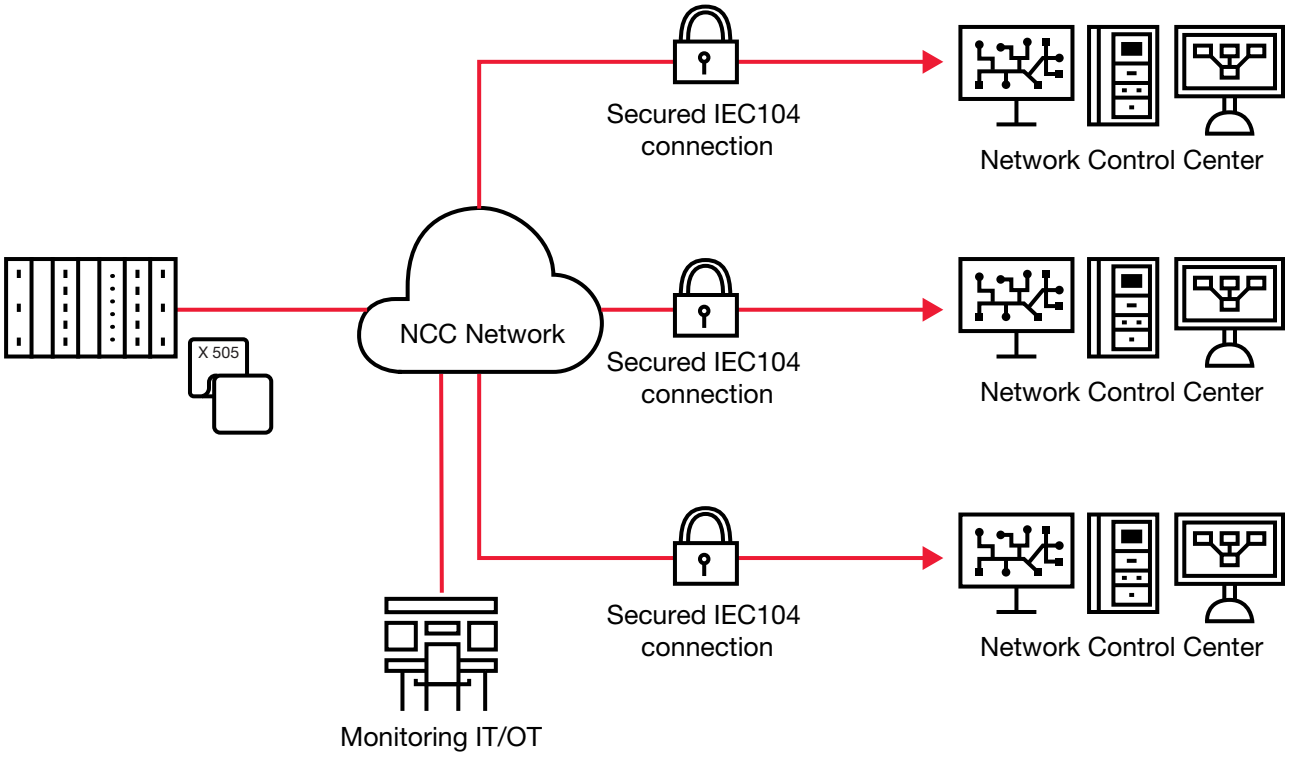
As a TSO, the company manages the flow of electricity over more than 70,000-kms of high-voltage line, which requires a high degree of standardization in the operation of the network's substations. As the previous standardization was already more than 10 years old, it was mandatory to update it with the latest cybersecurity features to protect the electrical grid.

To ensure security, customer was already using user account management, audit trail, security logging (syslog) and https support. The most important extensions to enhance security were to implement IEC 60870-5-104 secure communication based on the IEC 62351-3 standard and Simple Network Management Protocol version 3 (SNMPv3), which provides advanced new security features.

Secure control communications

The customer asked Hitachi Energy to provide secure communications with the control center as previously communication was done without any security level. Because the customer was part of a standardization committee, it was clear from the beginning they wanted to use standardized security protocols.

A part of the customer's specification was IEC 60870-5-104 communication protocol combined with TLS encryption based on the IEC 62351-3 standard. The advantage of this kind of communication is the end-to-end encryption between RTUs and the network control centers. This implementation provides data integrity, supported by digital certificates (X.509) and mandatory mutual authentication of client and server.



Device supervision

The customer had divided the responsibility between the network operation and the operation of the RTUs and the SCADA system. Because it was vital for network operators to know the status of all equipment in the network, the RTU was requested to provide this information to the network device monitoring tool.

SNMP protocol is the de facto standard for network device monitoring in IT/OT. The supported SNMPv3 protocol defines a secure version of SNMP. SNMPv3 provides customer confidentiality by encrypting packets, message integrity and authentication by verifying the source. Because of the high number of IP devices in the network, manual maintenance of devices is not possible, therefore integration of RTUs in the network management tool is needed.

The operator of the network monitoring system benefits from SNMP, as it allows graphical analysis of the data for the actual status and a longer period of time, and thus differentiates from other available remote control protocols for a SCADA system to communicate with the control system.

Customer benefits

To fulfill the customer's standardization and security process, Hitachi Energy provided the latest software version with features including standardized security functionality. The solution helps the customer increase its level of cybersecurity to the most up-to-date available on the market.

Hitachi Energy RTUs are continuously responding to the needs of power utilities and industries for products that can provide the highest levels of cybersecurity, including user access control, security logging, hardware hardening, device monitoring and secure communication based on standards.

Hitachi Energy's solution will protect customer's electrical grid and provide peace of mind in the decade ahead.

02

Secure IEC 60870-5-104 connection based on IEC 62351-3 TLS provides end-to-end encryption between RTU and Network control centers

Hitachi Energy
de-rtu-sales-support@hitachienergy.com
www.hitachienergy.com/rtu

4CAE000426