Cyber-resilient networks for utilities

With increasing automation, the demands on the IT and OT infrastructure of power utilities are growing. A highly available and secure communication network is becoming mandatory for reliable operation. However, the high economic and social importance of energy suppliers also makes these networks a preferred target for cyberattacks. With new regulatory requirements such as the NIS2 and RCE directives, the European Community has responded to the escalating threat situation. The requirements for communication networks are described below and solutions for effective implementation are presented.

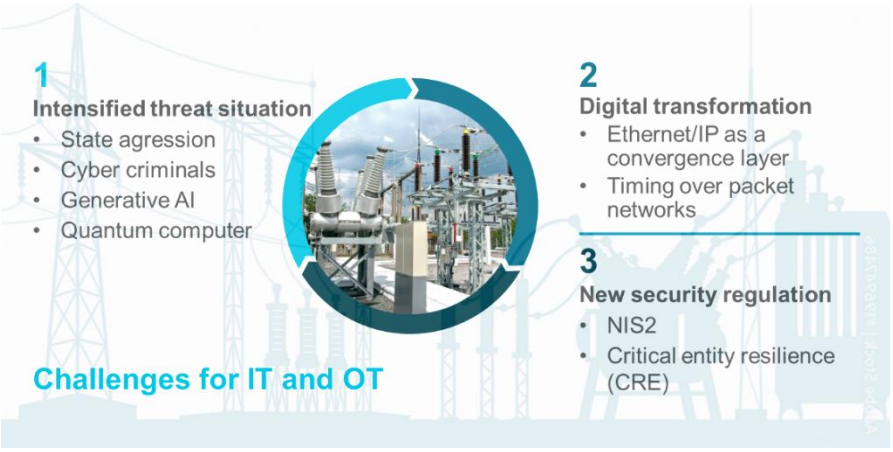
New requirements for IT and OT networks

Tougher threat situation

Growing threat: Operators of essential services, companies with high-security needs and governments are digitizing their processes and are therefore at risk from cyberattacks on their networks and IT/OT infrastructure. The current "Threat Landscape Report 2023" from ENISA and the "State of IT Security in Germany in 2023" from the BSI reveal a significant increase in malicious activities. In addition, artificial intelligence (AI) has expanded the arsenal of weapons used by cybercriminals.

Massive attacks: In May 2023, the Danish energy grid was threatened by coordinated attacks on 22 companies. The attackers were able to gain access to some of the industrial control systems. Some companies had to disconnect their operational systems from the grid. This was the largest cyberattack on critical facilities in Denmark and can be seen as a warning to operators of critical infrastructure in other EU countries.[1]

Quantum computers: Established public key cryptography is vulnerable to quantum computer attacks. Post-quantum cryptography (PQC) and quantum key distribution (QKD) offer possibilities for quantum-safe protection. However, the implementation of these new controls is a time-consuming process and should therefore be initiated immediately in order to reliably protect critical components and functions from future attacks by quantum computers.



[1] SectorCERT, The attack against Danish critical infrastructure, November 2023

Security regulations

Critical infrastructures: Energy suppliers are a crucial part of critical infrastructure systems and must meet regulatory requirements to ensure seamless operations. The deployment of management systems for information security (ISMS) and for business continuity (BCMS) are mandatory. Protective measures must be state of the art and attack detection systems are mandatory. In Germany, those requirements are based on the BSI Act, the BSI KritisV, the IT Security Act 2.0 and the Energiewirtschaftsgesetz (engl. Energy Industry Act).

New directives: In 2022, two directives – NIS2 and CER – were passed in the EU to strengthen critical infrastructure security. These directives have to be implemented as national law with all EU member states until October 2024. NIS2 lowers the thresholds for classifying companies. In the future, the supply chain will need to be included in the protection of the network. Encryption will also become mandatory. CER strengthens resilience to physical disruptions.

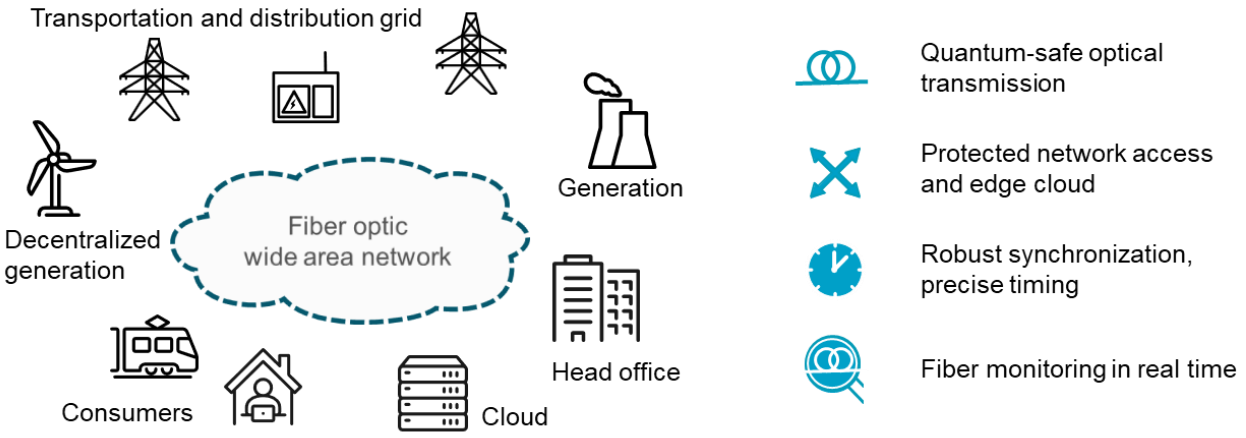
State of the art: When it comes to information security measures, the legal provisions are based on the current "state of the art." Particular attention should therefore be paid to those technology domains in which new protection technologies are becoming established, advancing the state of the art. In cryptography, traditional algorithms are being complemented by quantum-safe methods. Newer timing architectures protect against attacks on satellite-based timing. Virtualization of network functions enables agile and flexible adaptation to changing threat situations.

Digital transformation

IP/Ethernet connectivity: The introduction of new operational technologies and the transition to cloud-hosting will have an impact on the technologies used in the interconnection network. IP in conjunction with Ethernet creates a convergence layer that will be used by all future IT and OT applications. PDH and SDH systems, some of which are still in use, are becoming less relevant.

Precise timing: Automation places higher demands on time distribution in the network. According to IEC 61850, accuracy in the µs range will be necessary at substations in the future. Similar requirements are necessary for efficient replication of data in the cloud. The network must therefore be able to provide high-precision timing.

Edge cloud: Many applications can be hosted centrally in the cloud. However, time-critical functions and certain protective controls must be deployed at a remote site. Innovative edge cloud solutions are used for this purpose, which place special demands on cybersecurity.



Requirements for the wide area network

Implementing cyber-resilient networks

Quantum-safe optical transmission: Optical DWDM multi-channel technology provides the necessary bandwidth for an operator's entire traffic. Flexible add-drop multiplexers enable automated adaptation to new requirements. Capacity can be easily expanded by adding optical channels. Redundancy can be used to protect individual interfaces and wavelengths or complete fiber optic links and network elements. Our ConnectGuard™ security technology already offers quantum-safe protection. The FSP 3000 solution is the only BSI-approved encryption technology for optical connections on network Layer 1.

FSP 3000 optical transport

- Flexible, optical layer
- Quantum-safe encryption
- High availability

Protected network access and edge cloud: Ethernet technology is the dominant interface for connecting sites and properties. Our highly secure network access technology combines comprehensive monitoring functions with quantum-safe ConnectGuard™ encryption and local hosting of virtualized network functions. BSI-approved encryption secures data traffic and protects the integrated edge cloud from cyber-attacks. Virtualized network functions handle routing, monitoring of SCADA traffic and efficient use of the connection network through SD-WAN functionality. Our FSP 150-XG118Pro (CSH) offers unique flexibility, speed and security.

FSP 150 IP/Ethernet and NFV

- 1/10Gbit/s protected network access
- Integrated server for edge hosting
- Virtual routers, SCADA monitoring

Robust synchronization, precise timing: Today's requirements for precision, reliability and management can no longer be met with established time protocols such as NTP, IRIG-B. GNSS (Global Navigation Satellite System) receivers are a popular method of obtaining precise time information from satellites. These systems are very susceptible to jamming and spoofing. They should not be used as the primary source for synchronization and timing in utility grids. Our partner, Adtran Oscilloquartz, offers a comprehensive portfolio of utility solutions, including cesium atomic clocks, scalable grandmasters and optimized timing components.

Oszilloquartz timing Portfolio

- Scalable PTP grandmaster
- Cesium atomic clocks
- Multi-protocol: BITS, IRIG-B, PTP, NTP

Real-time fiber monitoring: Fiber breaks are unavoidable in a country with high levels of construction activity. Fast and targeted repair is crucial. By using Adtran ALM fiber monitoring, faults on the fiber can be detected and localized in real-time. Time-consuming troubleshooting is avoided. This enables connections to be put back into operation more quickly and, therefore, ensures high availability. ALM also detects when the fiber connection is being tapped, as the coupling device generates attenuation.

ALM fiber optic monitoring

- Real-time fiber monitoring
- Localization of fiber breaks
- Recognizing eavesdropping attempts