Securing IEC 61850 communications

From protecting against eavesdropping to preparing for post-quantum threats

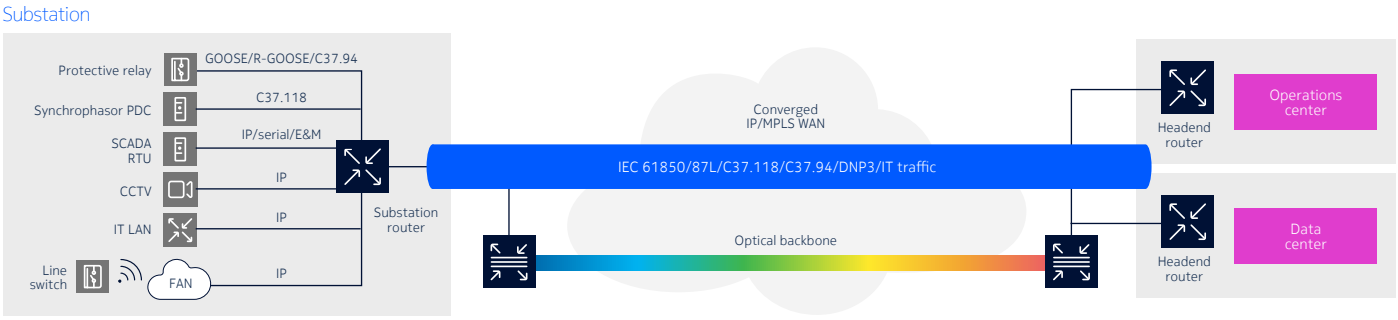
White paper

Contents

IEC 61850 communications in the new energy landscape

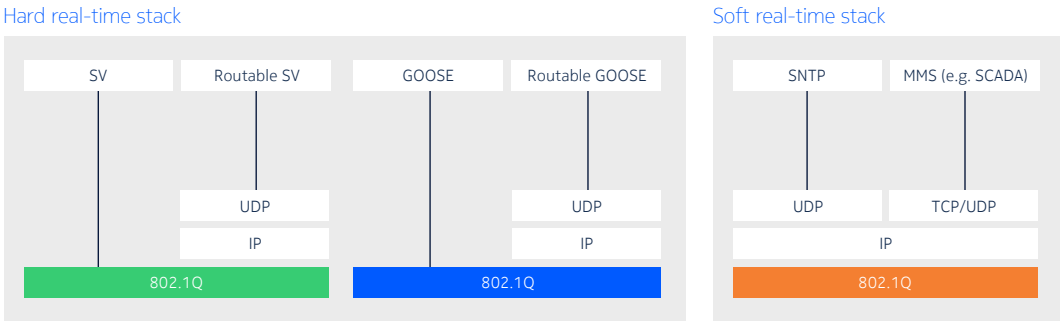
In response to the growing shift towards renewable energy resources, power utilities are undertaking a significant transformation of their power grids to embrace software-centric and data-driven operations. As part of this transformation, there is a notable rise in the adoption of IEC 61850 application systems for grid automation and monitoring that extends beyond substations. IEC 61850 communications are emerging as a critical component of grid communications over the mission-critical IP/MPLS wide area network (WAN), which connects intelligent electronic devices (IEDs) and edge compute in adjacent substations with the central management system in an operations center or a data center (Figure 1).

Figure 1. IEC 61850 communications in the IP/MPLS WAN



IEC 61850 communication comprises multiprotocol stacks (Figure 2). To enable the expansion of the protection and control application of the Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SV) protocols beyond substations to a wider area, IEC 61850-90-5 defines routable options for both protocols. These options facilitate the transport of GOOSE and SV messages in the WAN.

Figure 2. IEC 61850 communication stack



Sending 61850 communications over the WAN exposes the power grid system to various and constantly evolving cybersecurity threats. This paper explores the security threats and attack methods that can be encountered in the WAN. It also examines the critical need for power utilities to implement encryption as a key measure in a defense-in-depth security framework.

IEC 61850 security considerations in the WAN

In addition to general grid communication protection requirement captured in NERC CIP-011-3[1] and CIP-012-1[2], the specifics of the main IEC 61850 cybersecurity threats are discussed in IEC 62351-6:2020[3] (Figure 3).

Figure 3. IEC 61850 communications security threats

The IEC 62351-6:2020 standard identifies the security threats and attack methods that need to be addressed. The security threats to IEC 61850 communications can be summarized as follows:

- Unauthorized disclosure of information, which breaches **confidentiality**
- Unauthorized modification of information, or tampering, which compromises **integrity**
- Unauthorized communications with intelligent electronic devices (IEDs) and management systems, which decreases **availability**

These three threats are often referred to as the CIA of cybersecurity. The common attack methods used to exploit these threats are:

Eavesdropping: Attackers intercept and listen to communications between two parties, for example, IEDs in two substations or an IED and a management system in the operations center or data center. This allows the attacker to collect system login credentials or sensitive operational information on critical grid cyber assets and use it to breach confidentiality.

Man in the middle (MITM): A more advanced attack than eavesdropping, where attackers not only intercept and listen to communications but also modify them and even masquerade as the legitimate party to send wrongful commands with inverted Boolean logic. For example, an attack that changes “close” to “open” in a GOOSE message destined to a protective relay can cause a power service disruption that compromises operational integrity and jeopardizes grid safety.

Denial of service (DoS): Another advanced attack, where attackers replay and flood information to overwhelm the compute resources in the IED or the management system, resulting in decreased service availability and degraded responsiveness to grid conditions.

1 CIP-011-3 — Cyber Security — Information Protection. North American Electric Reliability Corporation. Accessed 5 March 2024.

2 CIP-012-1 — Cyber Security — Communications between Control Centers. North American Electric Reliability Corporation. Accessed 4 March 2024.

3 IEC 62351-6:2020: Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850. International Electrotechnical Commission. Accessed 4 March 2024.

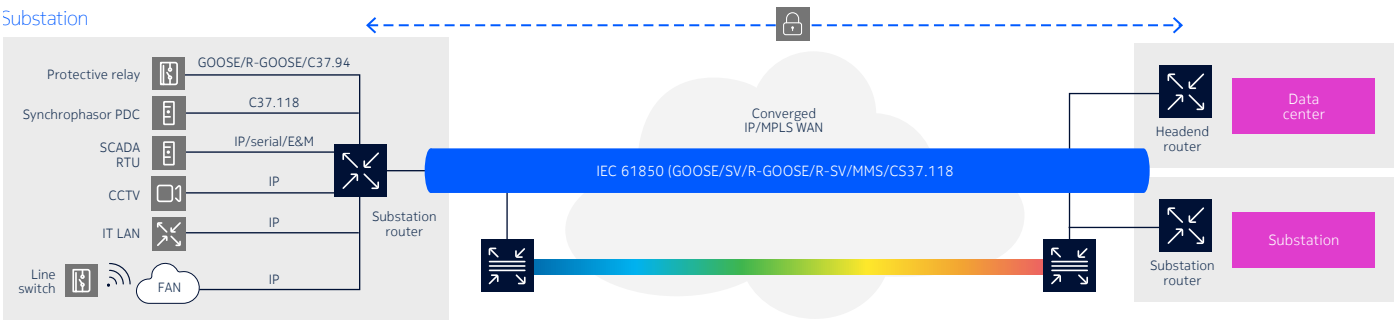
For example, flooding illicit traffic to the advanced distributed management system (ADMS) would compromise its ability to send commands to the load tap changer in the distribution systems to respond to an increase in air conditioning load during a heat wave.

Recognizing the gravity of these cyberthreats, IEC has developed a comprehensive set of technical standards aimed at empowering utilities to use cryptographic technologies to mitigate potential attacks. Among these standards, two prominent cryptography approaches stand out:

1. Encryption using the Advanced Encryption Standard (AES), as outlined in IEC 62351-6:2020, serves to protect IEC 61850 communications.
2. Transport Layer Security (TLS) and Hash-based Message Authentication Code (HMAC), specified in IEC 62351-3:2023[4] and IEC 62351-5:2023,[5] respectively, are used together to secure telecontrol systems such as SCADA utilizing IEC 60870-5-104.[6]

The IEC 62351-6 standard also provides specific guidelines for applications that have a 3 ms delivery requirement. It recommends reliance on communication networks instead of the IEDs to ensure constant performance. Given that communications within substations are typically protected within the security perimeter, the focus shifts towards safeguarding data that transits the WAN. This requires the use of robust cryptography measures to maintain the CIA of grid operations data (Figure 4).

Figure 4. Encryption protecting IEC 61850 WAN communications



4 IEC 62351-3:2023: Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP. International Electrotechnical Commission. Accessed 5 March 2024.

5 IEC 62351-5:2023: Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives. International Electrotechnical Commission. Accessed 5 March 2024.

6 IEC 60870-5-104: Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles. International Electrotechnical Commission. Accessed 4 March 2024.

Cryptography for protecting IEC 61850 and other grid applications

Cryptography encompasses a suite of technologies that make use of various algorithmic techniques to secure communications and information transmitted over the network. There are three main categories of cryptography:

1. Hash functions: Hash algorithms such as MD5, SHA-1 and SHA-2 perform mathematical calculations on protocol messages and generate a unique fixed-length value for each input message. The process authenticates the received messages and prevents message tampering. However, hash functions do not ensure the confidentiality of the information.
2. Public key encryption: Public key encryption, also known as asymmetric key encryption or public key infrastructure (PKI), uses two distinct keys—a public key and a private key—to encrypt and decrypt messages. The recipient's public key is openly shared with the sender. The sender then uses it to encrypt messages destined for the recipient. Upon receiving a message, the recipient employs a closely guarded secret private key to decrypt it. Common encryption algorithms in this category include the Rivest–Shamir–Adleman (RSA) public key cryptosystem and Diffie–Hellman key exchange (along with its elliptic curve variant, ECDH), which are integral to widely adopted network security technologies such as TLS and HTTPS.

   These algorithms rely on mathematical operations such as large integer factorization or discrete logarithmic calculations. The security level provided by these algorithms solely depends on the extremely intense computational efforts required to solve them.
3. Symmetric key encryption: Symmetric key encryption uses one key for both encryption by the sender and decryption by the recipient (hence the "symmetric" label). Since it encrypts data in the communication session, it is often called the session association key (SAK) and is securely shared between the sender and receiver. Prevalent algorithms used for symmetric key encryption include AES-128, AES-192 and AES-256, with the number denoting the key length. The security strength provided depends on the length of the key and the entropy of the key generator, or key derivation function (KDF) in standard speak. This encryption process is compute-intensive, so most IEDs today only offer AES-128. Additionally, IEDs often lack access to the high-quality key generators necessary for generating keys with high entropy.

   To ensure secure transmission of the SAK across the network, it is necessary to encrypt the SAK with another secret key, called a key encryption key (KEK), during transport. A public key encryption algorithm is typically used for this purpose today.

These three cryptographic technologies have been playing a crucial role in securing communications in general and grid communications in particular. However, the advent of quantum computers upends the cryptography landscape.

Advancement of quantum computers

The complexity involved in solving the mathematical algorithms behind public key encryption has enabled current public key cryptography technology to provide effective protection for communications in the network. However, the rapid advancement of quantum computing presents a disruptive shift in the security landscape.[7] [8] [9]

Quantum computers use quantum bits (qubits) instead of classical bits when they perform calculations. Coupled with the right quantum algorithms, they can harness counterintuitive principles of quantum physics such as superposition and entanglement to perform super-efficient parallel calculations that are not possible with computers operating with classical bits. Bad actors with access to such quantum computers, also known as cryptographically relevant quantum computers (CRQCs), can break public key encryption schemes significantly faster than the most powerful classical computers.

Two such quantum algorithms have existed for decades:

- Shor's algorithm enables efficient solving of the problems of integer factorization and discrete logarithms, effectively breaking the protection from RSA and Diffie–Hellman and its elliptic curve variant.
- Grover's algorithm provides a search method with quadratic acceleration for symmetric encryption keys compared to traditional exhaustive search methods, effectively halving its level of security, for example, reducing AES-128 security level to that of AES-64 only.

Emergence of quantum threats

National standards and security bodies have been closely tracking the evolution of quantum computing. They are now urging businesses, particularly those that operate critical infrastructure, to build up their readiness to defend against quantum threats.

Eavesdropping for harvest now, decrypt later (HNDL)

With the Shor and Grover algorithms, bad actors with access to a CRQC can potentially break public key encryption schemes significantly faster than they could with the most powerful classical computer. Even without immediate access to a CRQC today, they can collect and store encrypted grid communication data and messages for decryption later.

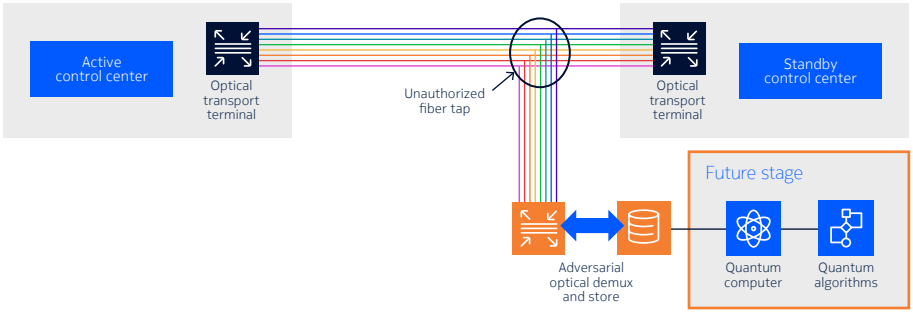
As shown in Figure 5, bad actors could tap into the fiber system between the active and standby control centers. They could then eavesdrop on communications and store all data. If utilities employ schemes such as TLS or Secure File Transfer Protocol (SFTP), the eavesdropped data remains safe today. However, if the bad actors have access to quantum computers in the future, they would be able to crack the encryption and decipher the data, gleaning information that they could exploit. This would allow them to gain a deep understanding of utility operations, identify weak spots and plan focused attacks on the grid.

7 Quantum-Readiness: Migration to Post-Quantum Cryptography. CISA, NSA and NIST. August 2023. Accessed 1 March 2024.

8 Position Paper on Quantum Key Distribution. French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces. Accessed 4 March 2024.

9 Rodriguez, Andrea G. A quantum cybersecurity agenda for Europe. European Policy Centre discussion paper. 17 July 2023. Accessed 4 March 2024.

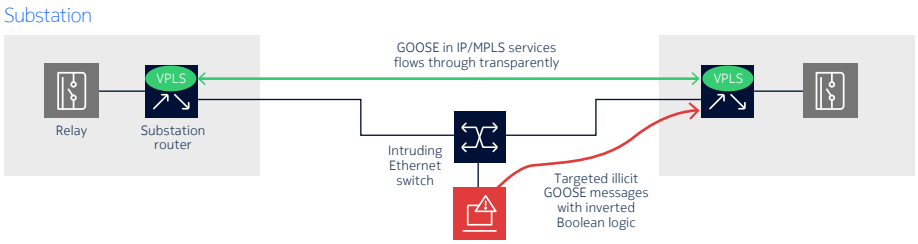
Figure 5. HNDL harvesting data traffic between active and standby control centers



Using a MITM attack to spoof commands and compromise PACS integrity

Communications between IEC 61850 IEDs play a pivotal role in IEC 61850-based protection, automation and control systems (PACS). Bad actors can construct illicit attack traffic that poses as legitimate control traffic to spoof wrongful commands with inverted Boolean logic or even take control of the IEDs to disrupt a circuit (Figure 6). Therefore, encryption is necessary. Some PACS IEDs can offer AES encryption with a shorter key such as AES 128 for GOOSE traffic and TLS for non-real-time traffic. However, these encryption schemes do not offer a strong level of security protection, leaving them vulnerable to post-quantum threats.

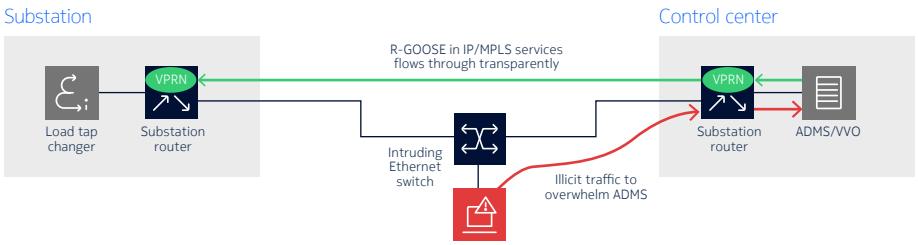
Figure 6. MITM attack targeting an IEC 61850 differential relay



Using a DoS attack to undermine the availability of an IEC 61850 application server

Denial-of-service (DoS) attacks aim to overwhelm the IEC 61850 application server so that it will lack the resources to execute the application logic to manage and control IEDs. For example, an ADMS with the Volt/VAR Optimization (VVO) application module can control IEDs such as load tap changers and voltage regulator and capacitor banks. If there is no encryption or the encryption is not strong enough to withstand a quantum threat, an adversary could inject massive illicit flows masquerading as normal data exchanges to congest the server link and overwhelm the application (Figure 7). This would significantly slow down the execution time of VVO logic to maintain proper voltage levels. It could, for example, hinder a utility's ability to support increasing air conditioning loads during a heat wave .

Figure 7. DoS attack undermining the availability of the VVO application



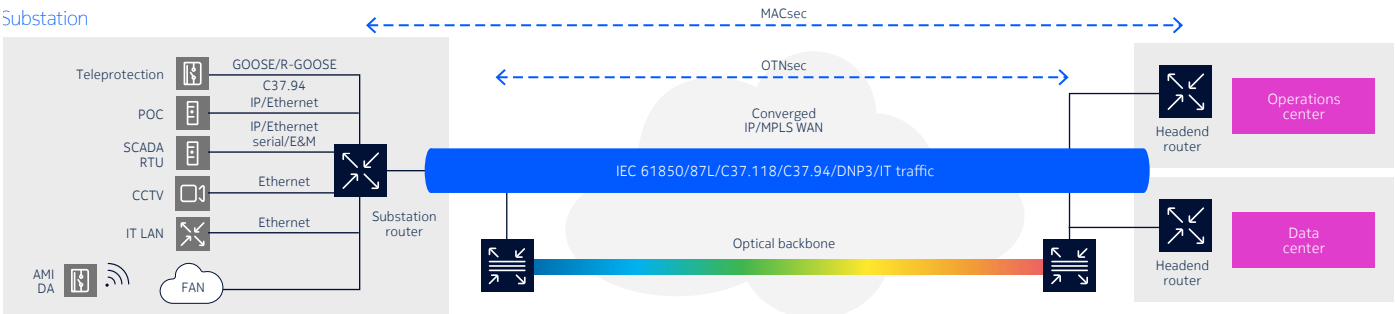
Developing a multilayer defense-in-depth blueprint

IEC 61850 requires a multilayer communications infrastructure that supports multiprotocol message exchange among numerous IEDs and application servers. To safeguard these communications, utilities need to develop a robust multilayer defense-in-depth network security framework with a suite of security technologies that encompasses encryption, firewalls, access control lists and network segmentation.

For encryption, it is important to use symmetric key encryption with a session key length of at least 256 bits to ensure an effective defense against quantum attacks. As explained earlier, the quadratic acceleration search by Grover's algorithm highlights this necessity because it reduces AES-128 encryption to the AES-64 level, which is not sufficient. AES-256 encryption is essential to maintain a security level equivalent to AES-128. Ensuring that the SAK distribution channel is quantum-safe is of paramount importance. Moreover, the KDF must possess a high entropy of 256 bits or greater to be more resistant to brute-force attacks.

Layer 1 OTNsec and layer 2 MACsec can fulfill these criteria and offer quantum-safe protection for IEC 61850 and other grid application communications. They can protect multiprotocol traffic that includes GOOSE, SV and other non-IEC 61850 grid communications such as C37.94 between differential relays, IEC 60870-5-101/104[10] between SCADA servers and remote terminal units (RTUs) and other IT applications such as CCTV video. Layer 1 OTNsec safeguards communications in the optical transport core and the high bandwidth links between operations centers and data centers. Substation routers can extend this protection to the substation edge by utilizing MACsec as specified in IEEE 802.1AE to protect all communications coming out of substations (Figure 8).

Figure 8. Quantum-safe IEC 61850 communications blueprint



10 IEC 60870-5-101: Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks. International Electrotechnical Commission. Accessed 4 March 2024.

It’s time for action

This paper has addressed the risks of IEC 61850 communications beyond the security perimeter of substations. In the absence of a strong encryption safeguard capable of withstanding quantum threats, adversaries can eavesdrop on communications and execute advanced attacks such as command spoofing to manipulate IEDs and launch DoS assaults on core grid management systems. Now that CRQCs have become a looming specter, utilities must raise the encryption key length to 256 bits to ensure that they can effectively thwart quantum attacks.

In response to this critical threat landscape, this paper has advocated a multilayer defense-in-depth security framework that harnesses layer 1 OTNsec and layer 2 MACsec to fortify the data and communication security of IEC 61850 and other grid communications. It has also highlighted the importance of using AES-256 encryption together with a KDF with entropy of 256 bits or higher to resist quantum attacks.

While standards bodies, including the National Institute of Science and Technology (NIST), are working to finalize post-quantum cryptography (PQC) standards, it will be some years before IEDs and servers widely implement these application-level encryption algorithms to complement AES encryption in the network. Therefore, it is important for utilities to start proactively planning a resilient and flexible grid security blueprint for quantum-safe readiness. To learn more about strategies and solutions for securing networks against quantum attacks, visit the Nokia quantum-safe networks web page.

Nokia has a broad grid communications product portfolio that spans IP/MPLS, data center fabrics, packet optical DWDM and microwave transport, passive optical networks as well as 4G/LTE and 5G networks. With a long history of working with utilities complemented by a full suite of professional services that includes audit, design and engineering practices, Nokia has the unique experience and expertise to support utilities as they continue on their digitalization journey. To learn more about Nokia grid communications solutions, visit the Nokia power utilities web page.

Abbreviations

ADMS	advanced distribution management system
AES	Advanced Encryption Standard
CCTV	closed-circuit television
CIA	confidentiality, integrity, availability
CIP	Critical Infrastructure Protection
CRQC	cryptographically relevant quantum computer
DoS	denial of service
DWDM	dense wavelength-division multiplexing
GOOSE	Generic Object Oriented Substation Event
HNDL	harvest now, decrypt later
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	local area network
KEK	key encryption key
LTE	Long-Term Evolution
MACsec	Media Access Control security
MITM	man in the middle
MMS	Manufacturing Message Specification
MPLS	multiprotocol label switching
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OTNsec	Secure Optical Transport Network
PACS	protection, automation and control system
PDC	primary domain controller
PKI	public key infrastructure
PSK	pre-shared keys
PQC	post-quantum cryptography
RSA	Rivest–Shamir–Adleman
RTU	remote terminal unit

SAK	session association key
SCADA	supervisory control and data acquisition
SFTP	Secure File Transfer Protocol
SNTP	Simple Network Time Protocol
SV	Sampled Values
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VAR	volt-ampere reactive
UDP	User Datagram Protocol
VVO	Volt-VAR optimization
WAN	wide area network

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 874652 (March) CID213941