intertrust®

Executive brief

Platform

New cyber-attack and data security challenges for the TSO

Flexibility and reserve capacity opportunities in energy

Transmission system operators (TSOs) globally are facing significant challenges due to increased volatility caused by the energy, mobility, and heating transition. This has led to various initiatives to integrate smaller energy systems into the planning and grid optimization process over time. For example, Redispatch 3.0 in Germany, where decentral energy asset load is coordinated with consumer demand to avoid grid bottlenecks. TSOs are also planning to develop various regional or national energy flexibility platforms, such as EQUIGY. These platforms will create market opportunities for new reserve balancing products.

Flexibility platforms enable smaller energy producers, users of energy, aggregators, and more (PV, batteries, heat pumps, EVs, etc.) to participate in reserve capacity and flexible distributed energy markets.

To operate in reserve capacity markets, three criteria must be met:

1. Create and establish a market-oriented price-finding mechanism for existing and new reserve products
2. Establish a secure and transparent (technical) connection of assets and loads
3. Ensure a secure communication of commands and a secure connection between assets and energy markets

A secure and tamper-resistant flexibility platform creates significant value for the energy system by creating optimization opportunities for grid operators and monetization opportunities for energy asset owners.

The integration of flexible energy assets can be established directly or via third-party aggregators. In both cases, the security and trust of data provided and commands pushed to assets is of utmost importance for the reliability of the entire system.

The TSO attack surface increases exponentially

Opening the flexibility and reserve market and connecting a very large number of decentralized energy assets also comes with risks: it dramatically increases the attack surface for malicious activities and cybercrime.

The current security approaches like air-gapping fall short because they have proven to be insecure and are impossible to maintain. The manipulation and tampering of data streams in the energy system can cause significant damage to equipment, and people, nullify any basic security infrastructure, and potentially inflict total supply blackouts.

Security focused practices must be developed and implemented in parallel to technical advancements and business oriented schemes. While the speed of innovation in tech provides higher levels of protection, the big challenge comes from the speed in which malicious actors learn and adapt.

Blockchain is only part of a comprehensive cybersecurity framework

Access to energy assets like heat pumps, EV chargers, EVs, machines, buildings, and infrastructure is required to manage energy flexibility, but that creates exposure to sophisticated cyber-attacks and data security risks for hardware and software.

The protection and identity of all information generated by these assets and its edge sensors is of utmost importance. Particularly, as data traverses its entire lifecycle and value chain across software and hardware like SCADA, gateways, clouds, etc., information security and trust is essential.

Blockchain technologies are a great first step for data security, because they render data immutable, but blockchains do not provide inherent protection against malicious data coming from internal and external data sources.

If erroneous or malicious data enters the blockchain, it will be stored immutably, which can lead to the propagation of incorrect information. Blockchain does not directly address the security of individual endpoints or devices that interact with the blockchain network.

The security of the devices and systems connected to the blockchain network remains crucial to prevent unauthorized access or attacks.

Not all data can be stored directly on the blockchain. Integrating 'off-chain data' sources and ensuring the security of data exchanges between the blockchain and external systems can pose challenges that need to be addressed separately. Ultimately, blockchains only protect data at rest. Secure systems require that data integrity and authenticity is also maintained in transit and during data processing.

A high level view of the total risk

TSOs are most critical entities responsible for the operation, maintenance, and development of high-voltage electricity transmission networks.

The role is crucial at the national, and in some cases, international level, connecting vast regions with reliable electricity. Isn't it time to build a cybersecurity framework worthy of the complex physical and cloud infrastructure?

TSOs must implement robust cyber technologies to safeguard against attacks and ensure the integrity and reliability of the transmission network.

One such cutting edge technology is Intertrust's Explicit Private Network – 'XPN', which adds an unprecedented level of security by protecting the data itself and not the transmission lines. Let's delve into more details.

Protecting energy data systems

Protecting data or critical infrastructure against cyber-attacks is a dynamic race, not a static process.

Combining security technologies is a popular approach for hardening defense mechanisms and increasing the tamper resistance of critical systems.

In addition to providing a high level of security and protection, security systems need to be flexible, adaptable, and responsive. The system must allow for adjustments and improvements whenever necessary.

Preventing malicious actors from manipulating data and damaging the energy system requires adjustments to existing data security strategies.

Heterogeneous technologies, like storage or cloud services from different vendors or different communication protocols must be supported. Vendor lock-in, or dependency on one security provider should be avoided.

The system should support zero-trust environments, such as the internet, for easy and cost-efficient device-to-cloud and cloud-to-device communication, as well as remote data accessibility. Persistent protection requires a common trust model with security controls that are maintained all the time.

XPN meets all new security requirements and shifts the paradigm of data security and interoperability in the OT/IT convergence.

The XPN technology fulfills the unique security requirements for today's TSO. It delivers unprecedented security in evolving energy markets.

XPN is a protocol which is based on a small and easy to integrate software client securing and authenticating data end-to-end, at the source (data at rest) and when the data is being processed.

XPN provides a much higher level of tamper resistance compared to only securing the communication link (protecting data in transit) or relying on session-based approaches like VPN or TLS.

XPN works bidirectionally and securely transmits commands back to systems or devices. It tunnels through different networks and does not rely on standard network security but instead generates a true secure system for data. XPN solves the data security problem of OT/IT convergence and ensures that AI does not get poisoned with bad data.

Get started with XPN

To launch TSO data security with XPN is simple and takes 4 steps: The feasibility phase starts by 1. clustering energy assets from a data security perspective; 2. selecting a limited number of assets for the specific security assessment; 3. identifying existing data security gaps; 4. derive a target security specification based on XPN.

XPN will then be implemented in a limited number of assets and tested under lab conditions, followed by field and robustness testing.

XPN meets all new security requirements and shifts the paradigm of data security and interoperability in the OT/IT convergence.

The XPN technology operates flawlessly with the data exchange and data analysis mechanisms from the Intertrust Platform.

The Intertrust Platform works independently from other systems, but also integrates with incumbent systems, and with standard business intelligence tools, providing business analysts, data scientists, applications, and third-party stakeholders with granular access to the data they need, in a compliant and auditable way.

Secure access to data reduces time-to-AI and provides information that are needed for developing market opportunities for new reserve balancing products.

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035