Secure Communications

Interoperability in the Power Grid

September 2023

Prepared by:
U.S. DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY

Part of a series of white papers on
electric grid communications.

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY

Introduction: What are the interoperability challenges related to secure communications in the power grid today?

As a geographically dispersed and segmented system, the electric power grid requires continual cooperation from interdependent stakeholders—including utility owners and operators, communications providers, power customers, and regulatory entities—to maintain the balance of electric supply and demand. In a landscape characterized by increasingly diverse and interactive distributed energy resources (DERs) at the grid edge, the traditional bulk-power and distribution systems remain essential to reliability. Rapid changes to business interactions and physical interconnections among diverse stakeholders can overtax the original design and construction of these systems. Ensuring system reliability requires a secure, end-to-end communications pathway capable of handling the information requirements of the modern grid, linking stakeholders across the generation sector, the transmission system, the distribution system, and the grid edge. Implementing this communications interoperability necessitates addressing several important challenges:

Secure Communications
A secure communications system protects the end-to-end physical pathway that transports data from origin to destination. That pathway may involve different transmission methods, such as optical fiber, copper wire, and microwave; transport diverse data, including grid state information and control messaging; and use a variety of analog and digital formats. Securing this end-to-end communications pathway—which is essential for reliable grid operations—involves preventing unauthorized access and monitoring traffic to identify anomalous activity without compromising the confidentiality, integrity, or availability of the data. Communications security methods complement cybersecurity approaches used to protect data at origin and destination.

- Increasingly diverse entity ownership, including independent power producers at the bulk level, investor-owned DERs on the distribution system, and customer-owned infrastructure at the grid edge.
- Incomplete standardization of tools and approaches at the edge and on the distribution system—such as DER management systems, advanced distribution management systems, and prioritization schemas—to enable interoperability and security.
- Decentralized, market-driven evolution of grid architecture compared with traditional, centralized planning and operation.
- Varied and inconsistent regulation, particularly on the distribution system and at the grid edge.
- Prioritization of communications investments in a cost-sensitive decision environment.

This white paper discusses the current state of secure communications interoperability in the electric power grid and delineates some of these challenges.

What is the current technical landscape for secure communications interoperability on the power grid?

Traditional electric grid communications interoperability began when bulk-power generation required connection to load centers via the transmission system.[1] The bulk-power generation and transmission systems have different internal communications needs and must also interoperate (often, between different owners). Generators use a localized industrial control system (ICS) with their own distributed control systems and

[1] Office of Electric Delivery and Energy Reliability, "United States Electricity Industry Primer," U.S. Department of Energy, July 2015.

operational technology (OT) assets, such as programmable logic controllers, sensors, actuators, and human-machine interfaces. Generators typically connect to the broader power grid via one or more redundant wide-area network links, which carry control instructions from operators and telemetry back to control centers. In contrast, the transmission system is a geographically dispersed ICS composed of assets covering entire states or regions and centralized control centers using supervisory control and data acquisition systems (SCADAs). They also contain energy management systems to regulate power flows, automate generator controls, control/monitor breakers, perform state estimation, and other functions—all of which rely heavily on interoperable, secure communication.

As distribution systems grew in complexity, interoperable communications evolved into distribution management systems (DMSs) to maintain reliability for the consumer. The DMS encompasses a range of systems and components, including outage management systems, geographical information systems, advanced metering infrastructure, and controls for protective relays. These components both consume a variety of data streams and relay data back to the distribution control center. The deployment of DERs on the distribution grid has now added the complexity of having two asset owners, with different priorities, which must communicate to support visibility, planning, and control. Unlike bulk-power or distribution systems with a legacy of interoperability, the new frontier of systems at the grid edge has no predecessor interoperability requirements.

The landscape is also changing faster than traditional infrastructure planning and upgrade cycles can support. In transforming to support new requirements and technologies, communications pathways must still leverage and support existing systems and the protocols that support them (see box at right), which have been engineered for transfer of important information like real-time voltage and current data with minimal processing and delay to enable timely operational decision-making at grid control centers. Because of the importance of communications speed and availability, legacy protocols used in the grid typically do not have encryption or logic protection—a circumstance in direct tension with the need to secure data flows, which is increasingly critical for grid operation.

Example Grid Communications Protocols and Their Uses on the Grid

- Distributed Network Protocol 3 (DNP3): SCADA interoperability
- Modbus: general ICS messaging
- Generic Object-Oriented System Event (GOOSE): event data within substation networks
- Inter-Control Center Communications Protocol (ICCP): power flow information between large utilities, balancing areas, and independent system operators
- Precision Time Protocol (PTP): precise network time distribution for grid synchronization
- Vendor-specific protocols: communications within proprietary systems

This state of evolution raises several key communications interoperability questions:

- Are current protocols capable of supporting the communications requirements of the next generation grid architecture?
- If needed, how will any new protocols interoperate with existing, deployed systems?
- How will adequate communications security be implemented on both new and existing systems while maintaining interoperability?

What are the key non-technical challenges to developing a secure, interoperable grid communications system?

The questions posed in the previous section are largely technical, but the regulatory and economic landscape in which the grid operates will also influence the path to building a secure, interoperable grid communications network.

The bulk-power system is subject to regulation and requirements to maintain reliable operation. For grid communications networks, this oversight manifests as the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) requirements, which cover control centers, many generation facilities, and transmission substations. NERC CIP sets the regulatory requirements for traditional system categorization, security, controls, incident response, etc. However, NERC CIP requirements are limited in scope: They define the electronic security perimeter[2] and communications between control centers[3] but exclude, for example, communications with entities outside the normal substation "fence." These limitations leave a security hole in the grid end-to-end communications path. The distribution system, investor-owned DERs, and grid edge fall into this large hole.

Most distribution systems do not fall directly under federal regulatory bodies but are accountable to state regulatory authorities, which can have different approaches to achieving grid reliability. Absent clear regulatory directives, utility companies decide how to implement their security posture, leading to inconsistent approaches. Regardless of the ultimate decision authority—state regulators or utilities themselves—the implementation costs of cyber and communications security can be a challenge to prioritize against other grid investments.

DERs connected to the distribution system are not typically owned by utility companies, but rather by outside investment companies. These DERs are subject to requirements of any federal incentive programs they are using, applicable industry standards, and distribution utility interconnection policies. These requirements might not include robust security, and additional investment in secure communications does not necessarily align with investor goals of minimizing installation cost and maximizing power sold to the utility.

Grid-edge systems use the same type of OT protocols as distribution and bulk-power systems, although they stay internal to the subsystem's network. Connections to external networks for data transmission include communication with the manufacturer for firmware updates, system monitoring and control, and provision of user services. Some mature standards, such as IEEE 1547[4] and 2030.5,[5] apply to the OT systems, as do common IT security standards for data transmission over the internet. However, implementation of these security standards is driven by consumer market demands and cost minimization.

Considering this regulatory and economic environment, several key questions confront the development of interoperable, secure, end-to-end communications on the grid:

- Implementation costs impose friction on robust implementation of communications security at all levels of decision-making—the regulator, the utility, the investor-owner, and the customer-owner—and at all layers of the grid, from the edge to the bulk-power system. How can we overcome this challenge?
- Grid-edge systems are increasingly critical to grid operations and have high disruptive potential. Given

[2] North American Electric Reliability Corporation, "Cyber Security - Electronic Security Perimeter(s)," 2013.
[3] North American Electric Reliability Corporation, "Cyber Security - Communications between Control Centers," 2020.
[4] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," IEEE Std 1547-2018.
[5] "IEEE Standard for Smart Energy Profile Application Protocol," IEEE Std 2030.5-2018.

their decentralized, market-driven development trajectory, how can their secure interoperability with centrally planned distribution and bulk-power systems be ensured?
- How do we implement interoperable, secure grid communications systems in this patchworked landscape of regulatory and economic conditions?
- Are existing standards evolving sufficiently to facilitate the enhancement of traditional cybersecurity requirements by interoperable secure communications in this complex, multi-stakeholder environment?

Conclusions

Secure and reliable power delivery requires interoperable, secure communications from the grid edge through the distribution system to the bulk-power system. The increasing quantity and diversity of assets within the distribution system and the grid edge must drive conversations among utilities, DER vendors, regulators, and other stakeholders on integrating these flexible assets and their data with the bulk-power system. The goal of this white paper is to motivate such a discussion around interoperable secure communications frameworks to facilitate integrated coordination and control of grid assets. The paper is part of an effort by the Department of Energy's Office of Electricity to bring stakeholders together to discover gaps, identify needs, and explore how secure communications can enable new capabilities for the electric system of the 21st century.

Please consider participating in a series of Department of Energy-sponsored webinars, workshops, and conferences in 2024 and beyond to drive consensus toward an innovative, cost-effective, and secure solution for grid communications.