SPaRC

Secure Pathways for Resilient Communications



2026 Securing Grid Resilience Symposium: Key Lessons and Takeaways

U.S. DEPARTMENT of ENERGY | Office of Electricity

1. Introduction

The *Securing Grid Resilience Symposium*, hosted by Oak Ridge National Laboratory in collaboration with the U.S. Department of Energy (DOE) and the U.S. General Services Administration (GSA), was held in Washington, D.C. on February 10–11, 2026. The event brought together experts from utilities, industry, government, and national laboratories across the United States to examine evolving challenges and emerging opportunities in secure communications, timing, and synchronization for an increasingly modernized power grid.

Day 1 focused on the critical role of resilient timing and synchronization in supporting the reliability and operation of modernized power grids. It framed grid resilience as an urgent operational, security, and national infrastructure issue driven by rapid changes in the electric system. The speakers and participants emphasized that communication, timing, and synchronization are no longer background technical services. They are mission-critical capabilities for grid reliability, protection, control, situational awareness, recovery, cybersecurity, and future grid operations. The day focused heavily on timing and synchronization, particularly the grid's dependence on GPS, NTP, and other time sources. Speakers described the risks of GPS jamming and spoofing, network latency, cyber compromise, and the transition from legacy TDM/SONET architectures to IP-based communications. The discussion repeatedly returned to the need for resilient, utility-appropriate, interoperable alternatives that can work across a fragmented U.S. utility landscape.

Day 2 shifted from the timing-focused foundation of Day 1 toward operationalizing resilience through secure communications, OT modernization, utility requirements, and practical implementation. Speakers emphasized that grid resilience is not only a technical problem; it is a shared strategic responsibility across government, utilities, national laboratories, communications providers, vendors, regulators, and other critical infrastructure stakeholders. The day explored how communications architectures are evolving as utilities move toward IP-based networks, cloud and subscription models, intelligent endpoints, smart devices, distributed controls, and growing interdependencies with telecom, data centers, and other infrastructure sectors. Discussions focused on how to make these changes secure, observable, testable, affordable, and deployable for both large and small utilities.

2. Highlights of Day 1

The opening remarks established the central challenge: the U.S. electric grid is becoming more distributed, data-driven, and operationally complex. Load growth from AI and cloud data centers, electric vehicles, distributed energy resources, sensors, controls, and renewed interest in nuclear energy are changing the grid's operating environment. These changes require tighter coordination, faster response, more visibility, and stronger resilience than legacy systems were designed to provide.

DOE's Office of Electricity described timing, synchronization, and secure communications as interdependent. The Center for Alternative Synchronization and Timing, or CAST, was introduced as an ORNL-led effort focused on resilient grid timing solutions. The Secure Pathways for Resilient Communications, or SPaRC, was referenced as a complementary multi-lab effort focused on secure grid communications and modernization.

Several speakers emphasized that GPS is convenient and widely used, but it should not be treated as an unquestioned single point of failure. A DOE speaker used a navigation-system error as an analogy: an individual can ignore a faulty GPS route, but the grid cannot simply turn off timing when synchronized operation is required at millisecond or microsecond scales.

The first major discussion explored how grid communications, timing, cybersecurity, and national security overlap. The grid was described as critical infrastructure whose modernization depends on understanding both cyber entry points and operational consequences. The conversation included risks tied to IP-based systems, Zero Trust concepts, internet protocol migration, large electronic loads, AI, data centers, and the need to understand the full system rather than isolated technologies.

The CAST-focused panel explained that modern grid operations rely on accurate clocks across control centers, substations, measurement devices, protection systems, and grid-edge devices. Timing is used for stability monitoring, forensic reconstruction, synchrophasors, automated controls, and wide-area situational awareness. Panelists warned that GPS jamming/spoofing and NTP compromise can create operational risks that grow as the grid becomes more automated.
Panelists also discussed alternative and complementary timing methods, including terrestrial timing and time over fiber, Precision Time Protocol (PTP, IEEE 1588 standard), two-way satellite time transfer, local holdover clocks and robust Cesium clocks, commercial timing-as-a-service, and other approaches. A recurring point was that no single solution is sufficient everywhere; different utilities have different scale, geography, legacy equipment, budgets, fiber access, regulatory contexts, and operational needs.

The Puerto Rico grid recovery and modernization experience was repeatedly used as an example of how moving from legacy TDM/SONET to IP-based networking can unintentionally reduce visibility and timing capabilities if those functions are not deliberately re-engineered. This became a broader caution about modernization: replacing legacy technology with newer network architectures can create new operational dependencies unless timing, observability, and security are designed in from the beginning.

Utilities and practitioners stressed that cost, ownership, interoperability, and governance are as important as technical feasibility. The U.S. grid includes thousands of utilities, spanning large investor-owned utilities, municipal systems, cooperatives, regional operators, federal power marketing administrations, and smaller rural providers. Solutions must be right-sized and operationally sustainable, not just technically impressive.

The second panel broadened the discussion to how precision timing supports advanced measurements and situational awareness. Utility, NIST, and academic perspectives highlighted the importance of synchronized measurements for understanding grid dynamics, oscillations, renewable integration, and wide-area events. The discussion connected timing accuracy to better decision-making, better analytics, and better resilience.

3. Highlights of Day 2

The opening remarks summarized Day 1's main theme: secure communications, trusted timing, and synchronization are essential enablers of the modern grid. Speakers emphasized that Day 2 would focus on moving from risk identification to operational solutions, including how DOE and the national labs can help utilities understand what success looks like, where gaps remain, and how collaboration can accelerate progress.

The opening fireside chat with DOE and Oak Ridge leadership framed communications as an undervalued but essential requirement for future reliability. As grid hardware becomes more intelligent, controls more distributed, software more complex, and analytics more data-intensive, the ability to exchange information securely and predictably becomes central to operations. Communications requirements such as latency, throughput, jitter, availability, security, governance, and data ownership were presented as planning-level concerns rather than afterthoughts.

Speakers distinguished communications security from traditional cybersecurity. Cybersecurity often focuses on protecting data and endpoints, while secure grid communications require an end-to-end view of the infrastructure, providers, protocols, data owners, operational dependencies, and governance structures that allow grid data to move safely and reliably.

The discussion connected communications resilience to NERC, FERC, resource adequacy, system planning, and operational risk. Speakers noted that timing and synchronization are not always explicitly captured in regulatory or planning frameworks, even though they increasingly affect reliability, data alignment, situational awareness, and operational coordination.
The first major panel focused on OT communications architecture and emerging risk. Panelists described a move toward millions of smart endpoints, cloud and subscription models, advanced distribution systems, virtual power producers, large loads, and increasingly complex stakeholder relationships. They warned that adversaries are increasingly interested in denial, degradation, and disruption of critical services, giving communications resilience direct consumer, public safety, and national security implications.

Utility practitioners discussed real-world modernization constraints. Many utilities operate long-lived legacy systems, mixed generations of equipment, limited staff, limited budgets, and communication networks that may include leased services, private fiber, microwave, radio, LTE, and shared municipal or carrier infrastructure. The panel repeatedly

emphasized that utilities cannot simply "rip and replace" their communications and OT environments.

Zero Trust was discussed in the context of OT and utility operations. Speakers cautioned that enterprise-grade security concepts must be adapted carefully to mission requirements. OT systems prioritize reliability, determinism, safety, and operational continuity. The discussion stressed that visibility, asset awareness, segmentation, monitoring, and trust decisions must be built around operational consequences, not just enterprise IT assumptions.

The panels highlighted the need to understand what is actually on utility networks. Asset inventory, network management, baselining, anomaly detection, and knowledge of normal communications behavior were described as prerequisites for resilience. If a utility does not know what devices are present, what they should communicate with, and what normal behavior looks like, it cannot reliably detect new risks or respond when failures occur.

The final panel emphasized testing, validation, and practical tools. SPaRC was described as a program that helps make communications pathways, dependencies, and failure modes visible. National lab participants described work to test devices, networks, and architectures to failure or near-failure before deployment on the grid. This was framed as essential because many technologies appear to work in ideal settings but behave differently under realistic grid conditions.

The discussion also returned to fiber and communications infrastructure. Panelists noted that utilities, municipalities, departments of transportation, telecom providers, and other entities may all have fiber assets that could support more resilient grid communications if better coordination and sharing models are developed. At the same time, speakers stressed that fiber is not always available, and utilities need practical alternatives such as microwave, LTE, leased services, and hybrid architectures.

DOE and SPaRC participants described a developing decision-support architecture tool intended to help utilities evaluate communications options based on grid services, available local media, technology choices, and service requirements. The tool is intended to be descriptive rather than prescriptive: it gives utilities a starting point, helps them understand tradeoffs, and helps non-telecom specialists communicate requirements to carriers or providers.

The event closed with next steps: organizers plan to send a participant survey, publish a summary-of-findings report, and continue building a broader community around secure communications, timing, synchronization, energy security, homeland security, and national security.

4. Symposium Findings

- The grid is moving faster than traditional communications assumptions. Large electronic loads, DERs, inverter-based resources, data centers, distributed controls, and edge devices are pushing the grid toward machine-speed operation.

- Communications and timing must be engineered as part of grid reliability. They cannot be treated as procurement afterthoughts or carrier-provided conveniences.
- The United States has a fragmentation challenge. Thousands of utilities, multiple business models, and different state and regulatory structures make a uniform national strategy difficult.
- Local and relative synchronization may be as important as absolute time. Many grid applications need coherent alignment across devices and substations, with traceability to official time where needed.
- Multi-vendor monitoring is a gap. Utilities need a small number of operational views that show timing health, path changes, latency, jitter, drift, and device anomalies.
- Cloud and subscription models introduce new fragility. They can accelerate deployment but also create tethered dependencies and failure modes that must be understood before operational reliance.
- Workforce is part of the architecture. The sector needs people who understand both telecom/networking and power-system operations.

5. Key Takeaways

- Timing and synchronization are mission critical. They now determine whether distributed measurements, controls, protection signals, and event records are coherent and trustworthy.
- Timing and synchronization are becoming operational dependencies, not invisible support functions.
- GPS and NTP are useful but vulnerable; the grid needs layered, resilient timing architectures.
- GPS remains valuable but is not sufficient by itself. Jamming, spoofing, data spoofing, antenna failures, and recovery complexity require alternate paths and local holdover.
- CAST is focused on testing and validating alternative synchronization and timing solutions using realistic grid equipment and field-relevant scenarios.
- CAST is positioned to help utilities more rapidly adopt resilient timing and synchronization solutions that are right sized to their budget, service area, and risk posture.
- SPaRC complements CAST by addressing secure grid communications, monitoring, baselines, visibility, and modernization of communications infrastructure.
- SPaRC is positioned to help utilities understand secure communications pathways, requirements, baselines, and architecture options.
- Data centers, AI workloads, distributed resources, and large electronic loads are increasing the importance of timing, visibility, and secure communications.
- Interoperability across utility boundaries is a major challenge because the U.S. grid is a network of many networks.
- Education and practical demonstrations are needed to show why precision timing matters before a crisis makes the need obvious.

- Collaboration across DOE, national labs, DHS, NIST, utilities, vendors, academia, and regulators is essential.
- Communications resilience is a core grid reliability issue, not a back-office IT concern.
- Secure grid communications require an end-to-end view across infrastructure, providers, protocols, data owners, and operational dependencies.
- OT security is not enterprise IT security. Protection and control systems require deterministic, recoverable, segmented, and purpose-built approaches.
- OT modernization must be mission-driven; IT/OT convergence is not simply a technology decision.
- Visibility is the first control. Utilities cannot secure, recover, or operate what they cannot see: assets, routes, ports, timing sources, latency, jitter, drift, and dependencies.
- Utilities need visibility into assets, traffic patterns, dependencies, and failure modes before they can meaningfully secure or modernize their networks.
- Zero Trust principles can be valuable, but they must be adapted to OT requirements for safety, determinism, uptime, and operational continuity.
- Small utilities and resource-constrained organizations need practical, affordable, right-sized solutions.
- Fiber is highly valuable for precision timing and communications, but not universally available or affordable; utilities need flexible architecture options.
- Fiber is a powerful enabler, but resilience planning must include hybrid options and realistic local constraints.
- The technical problem is solvable; the deployment problem is harder. Governance, ownership, rate recovery, utility fragmentation, third-party dependencies, and workforce gaps are the limiting factors.
- Testing technologies to failure or near-failure is critical before deploying them into grid environments.
- Ongoing engagement, shared language, and collaboration across sectors are necessary to turn the workshop discussion into deployable solutions.

6. Audience Concerns

- Regulation and incentives: The audience repeatedly asked what would force action: mandatory rules, a major event, or a more constructive incentive model. The strongest synthesis is to avoid waiting for an event by embedding timing/comms risk into existing reliability, cyber, and planning processes.
- Small-utility access: The question was not only what technology works, but how a small co-op or municipal utility can know what it needs, afford it, and operate it. Shared reference clocks, association-led services, planning tools, and practical playbooks are essential.
- IT/OT convergence: Participants challenged simplistic convergence narratives. The better framing is control-network vs. enterprise-network. OT may use IP and IT-like

tools, but it must preserve deterministic behavior, recoverability, and purpose-built segmentation.

- Official-time traceability and national timing: Utilities can build internal timing islands, but inter-utility events, islanding/reconnection, and forensics require traceability to official time. The difficulty is less the clock and more the physical, contractual, and governance path to distribute it.
- Who owns the risk: Utilities, telecom providers, vendors, cloud providers, regulators, federal agencies, and customers all touch the risk surface. The answer is not a single owner; it is explicit responsibility mapping and shared operational language.

7. Actionable Next Steps

- Classify timing requirements by application: absolute time, relative synchronization, precision, holdover, traceability, recovery time, and acceptable degraded mode.
- Create a utility communications and timing dependency inventory: GPS receivers, NTP sources, PTP domains, fiber/microwave/cellular/leased links, routing paths, cloud dependencies, remote access points, timing consumers, and critical applications.
- Establish baselines: normal ports, routes, traffic volumes, latency bands, jitter, timing drift, device neighbors, and expected communication pairs.
- Close or control unnecessary pathways: unused ports, default routes, unmanaged remote access, undocumented modems, and unmanaged timing sources.
- Develop a communications/timing failure-mode library: loss of GPS, GPS spoofing, NTP compromise, route change, mirror port insertion, fiber cut, PTP degradation, cellular outage, cloud service loss, and vendor service degradation.
- Test degraded communications behavior before deployment: do not accept vendor assumptions that bandwidth and connectivity are always present.
- Use DOE/lab testbeds for pre-field validation, especially for multi-vendor timing, relay/control communications, digital substation behavior, and cross-distance timing distribution.
- Prepare executive and regulator-facing business cases that quantify reliability, safety, outage, public-good, and national-security benefits of communications and timing investments.
- Define OT-appropriate Zero Trust: segment, fingerprint, baseline, monitor, and recover gracefully before layering in tools that may add fragility.
- Keep the SPaRC/CAST dialogue active with utilities, vendors, regulators, labs, and federal agencies so timing and communications needs are represented in broader PNT and infrastructure conversations.

8. Questions the 2027 Securing Grid Resilience Symposium Should Answer

- What grid applications require microsecond synchronization, and which only require millisecond timestamping?

- How long can critical devices successfully operate in “holdover state” after loss of GPS or external timing?
- What are the minimum viable timing and communications architectures for a small co-op or municipal utility?
- How should a utility monitor communications and timing security and health across multiple vendors and transport media?
- What failure modes should every communications architecture be tested against?
- How should secure communications requirements be written into procurement and carrier contracts?
- Where do voluntary guidance, NERC/FERC reliability structures, PUC incentives, and federal leadership intersect?
- What should be demonstrated live before utilities are asked to deploy broadly?

9. Conclusion

Day 1 successfully established the strategic and technical foundation for the event. The strongest message was that the grid's future reliability will depend on capabilities that have often been treated as secondary: timing, synchronization, communications visibility, and secure operational networking. Participants repeatedly emphasized that modernization must be mission-driven and utility-informed. The day closed by positioning Day 2 to build on this foundation with a deeper focus on communications security, OT modernization, and practical resilience requirements.

Day 2 effectively translated the strategic concerns from Day 1 into operational and implementation-focused discussions. The strongest theme was that resilience depends on understanding the actual operating environment: assets, networks, ownership, dependencies, failure modes, regulatory context, and mission impact. The event closed with a clear call to sustain the community, expand participation, share findings, and continue developing tools and guidance that utilities can use in real-world modernization decisions.

The 2027 Securing Grid Resilience Symposium should be designed as a deployment event, moving beyond a focus on awareness. While this event succeeded in surfacing the strategic importance of timing and secure communications and in identifying the questions that matter most, the next step is to translate those questions into architectures, tests, requirements, and shared deployment models that utilities can use.









The US Department of Energy's SPaRC (Secure Pathways for Resilient Communications) program is leading grid communications research and development through a National Multi-Lab testbed, established to design, test, evaluate, and benchmark next-generation secure communications architectures and technologies. A secure communications system protects the end-to-end physical pathway that transports data from origin to destination. Key SPaRC activities include the Grid Communications Test Bed, Next-Generation Communication Experiments, and Education & Technical assistance. For more information see: https://securecomms.ornl.gov/