SPaRC

Secure Pathways for Resilient Communications

# Best Practices for Grid Communications

# 1. Introduction

Our nation's electric grid is transitioning from a centralized, producer-controlled network to a distributed, consumer-interactive model that is often referred to as the smart grid. A fully functioning smart grid will feature ubiquitous sensors throughout the transmission and distribution grid while continuing to balance electric supply (generation) with consumer demand (load). These sensors will need to collect and share data with consistent and well-defined latency, higher bandwidth, and two-way communications to transport information between grid utilities and consumers (or prosumers) through distributed or cloud-based computing necessary to make that data actionable. Secure communications are critical to achieve this smart grid vision and for the successful operation of the modern electric grid.

A secure communication system protects the end-to-end physical pathway that transports data from origin to destination. That pathway may: involve different transmission mediums, such as optical fiber, copper wire, and wireless technologies; transport diverse data including grid state information and control messaging; and use a variety of analog and digital formats (see Figure 1).

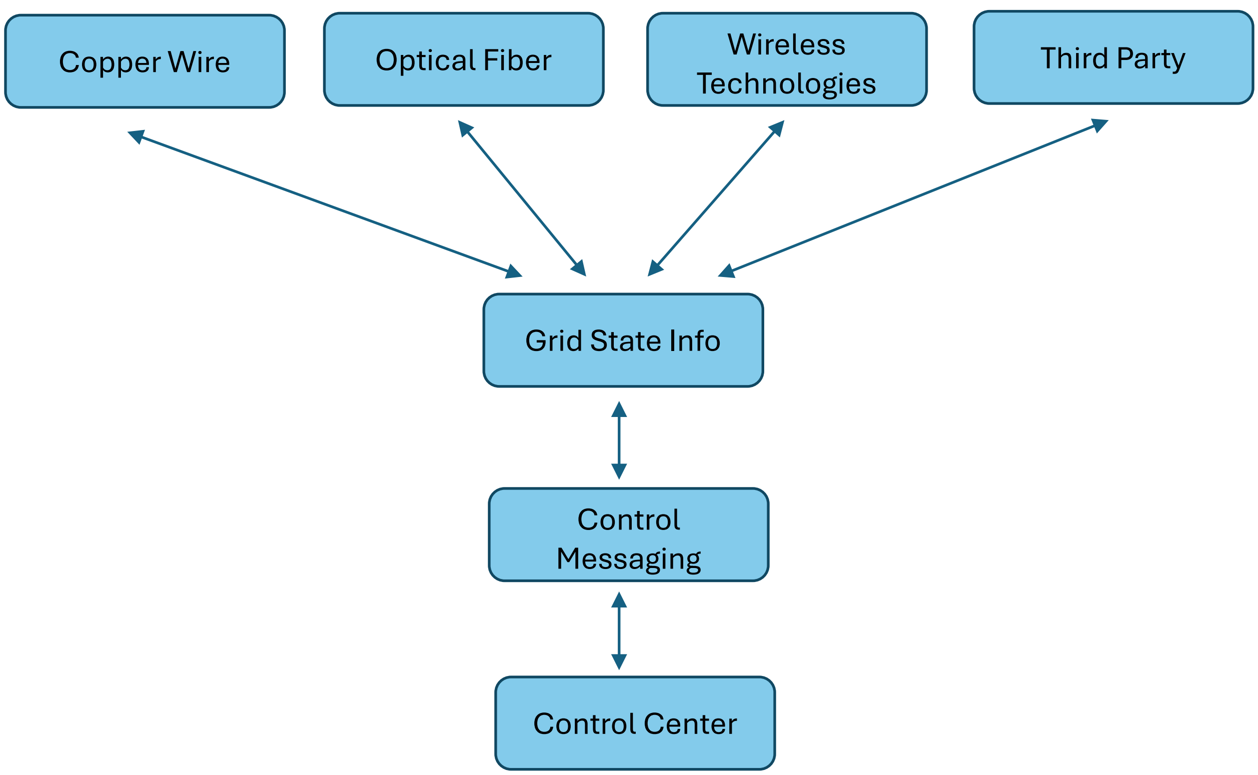


Figure 1: An example of a grid communication pathway.

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. Secure communications are critical for the successful operation of the electric grid[1].

For grid communication networks, the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) requirements cover control centers, many generation facilities, and transmission substations. NERC CIP sets the regulatory requirements for traditional cybersecurity for system categorization, security, controls, incident response, and so on. CIP-5[2] and CIP-12[3], however, define the electronic security perimeter and the communication between control centers, specifically for secure communications and their interoperability. This leaves a hole in a grid end-to-end communications path as the grid edge extends outside the normal substation "fence". This document is not intended as a replacement for the standards and regulatory requirements that govern grid communication systems, such as NERC-CIP or FERC requirements, or for vendor equipment security settings. Instead, this document is intended to fill some best practices gaps: such as 1) accounting for the interdependencies between the grid and the communications sector; 2) network management; 3) the transition from SONET to IP-based systems and the associated changes that need to be accounted for to maintain resilience; and 4) timing and synchronization that support reliable and resilient operation of the grid.

---

[1] U.S. Department of Energy, "Power Grid and Communications Interdependencies," 2023. https://securecomms.ornl.gov/publications/Power-Grid-and-Communications-Interdependencies-Key-Challenges-for-Reliable-Resilient-Operations.pdf

[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.

# 2. Communication Sector and Grid Interdependencies

Communication sector and grid interdependencies have been the subject of various studies by entities such as the National Security Telecommunications Advisory Committee (NSTAC) and the Federal Communications Commission (FCC) dating back to 1987. These studies have covered everything from day-to-day operations to long-term outages. An NSTAC report from 2006[4] states, "collaboration between the two sectors is most important at the regional and local levels to ensure the rapid recovery of both sectors."

The grid traditionally involved power flowing unidirectionally from synchronous generation to loads. Network communications for grid operation were also largely maintained and operated by the electric industry. Today, the grid incorporates bidirectional power flows between asynchronous generators and controllable loads, supported by a variety of digital technologies (shown in Figure 2), with increased grid communications requirements to support this more complex and information-rich architecture.

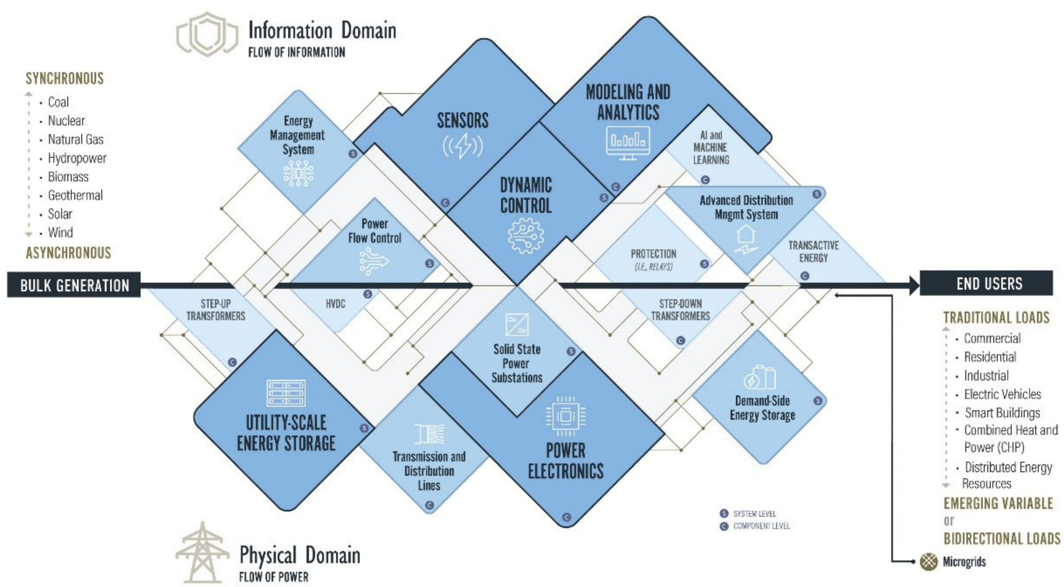


Figure 2: Increasing information loads on the evolving electric grid.

The current and evolving environment requires a high-speed, bidirectional pathway for digital, packetized communications supporting power system monitoring and control functions. This includes energy management, substation alarms, video monitoring, distribution automation, protection, and fault recording for both on- and off-network installations.  Grid communications now rely on a mixture of private, utility-owned

[4] NSTAC Telecommunications and Electric Power Interdependency Task Force (TEPITF), January 31, 2006.

infrastructure and commercial leased infrastructure to meet this demand, as reported by NSTAC in 2006[5] and by the Utilities Technology Council in 2019[6].

The increasing importance of commercial communications systems for grid stability was exemplified in April 2022, when the California Independent System Operator (CAISO) reported that for about fifteen minutes the state's energy requirements were completely met by renewables.[7] A large portion of renewable generation was controlled and monitored remotely using IP over commercial communications links; due to being distributed and not on utility communications networks. Commercial links are often the best or the only viable option for interconnecting and communicating with distributed energy resources (DERs). The use of DER aggregators will also continue to expand the use of communication networks out of the grid utilities' control,[8] increasing the electric power industry's dependence on the communications sector.

Agility in grid control increasingly relies on commercial communications providers and a variety of technologies, from wireless (e.g., 5G, microwave, Wi-Fi) to wireline (fiber, copper) to radio communications (P25, other repeater-based systems), and all these communications systems rely on electric power.  The complexity of this dependence and associated event consequences is often underestimated. Both sectors typically still conduct their restoration and recovery planning independently. Just as electric utilities must account for communications dependences when operating the grid resiliently, efficient post-event recovery also requires inclusion of communications facilities in restoration planning.

While the communication sector may provide backup power for several days at large sites, smaller sites, or sites operated by state and local entities may have backup power for a much shorter time frame. The grid utility may not prioritize restoration to communication sector assets due to their ability to maintain operation while relying on backup power. Even if a central office that a grid utility's control communication runs through is still powered, the grid utility's local communications devices can be nonfunctional if any node in the communications path is left unpowered by an outage. It is also possible that portions of the communications path are part of another grid utility's service territory, so one grid utility's outage event could impact another's communication path and operations.

Being able to operate through a failure event is a critical component to resilience. Natural disasters like hurricanes, earthquakes, floods, etc. can cause infrastructure damage and

---

[5] NSTAC Telecommunications and Electric Power Interdependency Task Force (TEPITF), January 31, 2006.

[6] Utilities Technology Council "Utility Network Baseline – April 2019", https://utc.org/wp-content/uploads/2019/04/UTC-Utility-Network-Baseline-Final.0419.pdf

[7] "For the first time in history, California's demand was 100% matched by renewable energy generation," PV Magazine, May 2, 2022. https://pv-magazine-usa.com/2022/05/02/for-the-first-time-in-history-california-was-100-powered-by-renewable-energy

[8] "Metering and Telemetry Requirements" PJM https://www.pjm.com/-/media/committees-groups/subcommittees/dirs/2021/20210303/20210303-item-06a-metering-and-telemetry.ashx

can shut down portions of communication networks. In these cases, the system should be able to degrade gracefully by rerouting the data through other paths so that the grid can still be managed. This also involves the grid utility understanding the critical data flows for its system and communicating those to any provider it depends on. This would allow the most important traffic to go through and keep up the essential services even in degraded conditions. This requires planning to include all parties involved in the communication path and coordinated with any local supporting response personnel.

It is critical for a grid utility to understand its critical communication path and the assets that belong to other sectors that it relies on for that path. This may include commercial communication providers, or in the case of P25, state and local entities. Grid utilities and their communications counterparts should conduct planning with all entities that are part of the communication pathway. This would allow communications infrastructure and power infrastructure to be restored in tandem so that critical communications nodes have power, and critical power infrastructure has the communications links required to operate it. These plans should be periodically reviewed and exercised with all partners involved in the planning and whenever infrastructure or dependencies change.

# 3. Network Management Systems (NMS) as a Best Practice for Grid Communications

## Introduction

Electric utilities are undergoing a transformation where the communication system has become the operational backbone of the grid. No longer a secondary support, the OT communication network is mission-critical infrastructure: enabling real-time monitoring, protection, control, and coordination.

As reliance on these networks grows, utilities must ensure that their communication infrastructure is reliable, secure, and visible. A Network Management System (NMS) is central to achieving this and is a key component to best practices for grid communications. Properly designed for OT environments, an NMS delivers situational awareness, supports troubleshooting, strengthens cybersecurity posture, and provides a foundation for proactive management.

## The Unique Context of Utility OT Networks

Unlike enterprise IT networks, utility OT networks have distinct characteristics that are key to developing capabilities from an NMS. These distinct characteristics include:

*Static architecture:* Devices use fixed IP addresses at the time of provisioning, not DHCP. Most communication paths between devices are fixed and can be periodic, reducing reliance on dynamic lookups and DNS. The pace of new component insertion may be slower than enterprise IT, enabling attention to measured, deliberate changes.

*Security hardening*: OT best practices usually involve a deny-by-default, permit-by-exception posture, including shutting down unused ports on switches and routers, limiting wireless connectivity, and tightly controlling changes. This may include locking MAC addresses to interfaces, host-level ACLs, and extensive use of encryption.

*Limited protocol support*: Many OT devices, particularly legacy RTUs and IEDs, do not support SNMP or modern monitoring features, but can support basic IP ICMP functions which may or may not be allowed in the OT network, depending on the security posture and risk tolerance for less-secure protocols.

*Mixed ownership:* Utilities operate a blend of owned fiber, leased services, and third-party MPLS/IP circuits, increasing reliance on service level agreements, coordination, monitoring, and response plans across parties.

*Path performance*: Known path performance is important for grid operations as latency, jitter, and throughput must be maintained at predetermined levels supporting grid operational processes like SCADA, teleprotection, and synchrophasors.

*Longevity:* OT devices may remain in service for decades, demanding backward compatibility alongside modern features.

These factors shape how traditional NMS capabilities should be applied in OT networks. Auto-discovery, for example, cannot rely on DHCP, DNS, or broadcast protocols. Monitoring must adapt to the reality of which devices are 'eligible' for visibility through diverse means.

## Best Practice Contributions of an NMS

Following is a set of functions that an NMS can provide to contribute to best practices of grid communications.

### Documenting what devices are on the network

An NMS can be the authoritative record of the network's operational state providing a device inventory, topology mapping, and configuration management.

- Device inventory: Established through manual seeding, selective auto-discovery, and integration with engineering databases. Often combined with credential management to ensure devices are both accounted for and properly maintained.
- Topology mapping: Representing both owned and leased infrastructure, allowing clear demarcation of responsibilities. Can include real-time link status tracking and performance history.
- Configuration management: Capturing device settings, version history, and audit trails, including disaster recovery (loss of device) support.

### Knowing What Normal Is (Baseline Determination)

Before anomaly detection can take place, a sound understanding of expected behavior (traffic patterns, volumes, etc.) must be established. This is called a network baseline. A critical best practice is defining the network's baseline:

- Configuration baseline: Recording current device settings, firmware, and known communication peers, including both static and derived forwarding tables.
- Performance baseline: Establishing expected latency, jitter, error rates, and bandwidth utilization under normal operating conditions.

Because OT networks are generally static, these baselines remain stable over long periods. That stability is an advantage: any deviation from the baseline—such as rising latency, unexpected packet loss, or altered device configuration—becomes a clear indicator of an issue.

This capability is particularly important for third-party services (leased fiber, MPLS) where utilities have reduced visibility. By maintaining independent baselines of path performance, utilities can rapidly identify degradations, trace them to root causes, and escalate with evidence to responsible parties.

## Knowing When a Change Happens

Unexpected or unauthorized changes can undermine both reliability and security. An NMS can support best practices for grid communications by tracking and alerting on changes such as:

- Device reconfiguration through SNMP traps, syslog, or configuration polling and comparison to archived baselines.
- Topology shifts such as a link rerouting or interface status changes.
- Performance deviations against the baseline.

This allows operators to distinguish between planned work and abnormal events, speeding both troubleshooting and incident response. Tight integration with risk-based configuration change request ticketing systems can simplify the traceability of changes to attribution and intent. All sanctioned and verified changes should be finalized through updating configuration baselines, incorporating modifications into the new expected system state.

## Identifying the Abnormal and Responding Faster

Once a baseline is established and changes are monitored, the NMS serves as a situational awareness tool:

- Pinpoints abnormal events quickly (e.g., performance degradation, loss of redundancy, unauthorized reconfiguration).
- Correlates network alarms with operational impacts (e.g., SCADA polling delays or failed protection messaging).
- Provides actionable data for root cause analysis, whether internal or across leased services.
- Reduces mean time to repair (MTTR) with roll-back to configuration baselines and supports proactive rather than reactive maintenance.

In practice, this means the difference between a slow, uncertain troubleshooting process and rapid restoration with high confidence.

## Eligible Devices for Monitoring

Since not all OT devices support modern monitoring, utilities can define tiers of visibility to accommodate all devices:

- Tier 1 – Fully monitorable: Modern switches, routers, firewalls, and OT devices with SNMP, syslog, or other telemetry support. Can include visibility into device resource utilization (CPU, memory, disk, link) in addition to device-level up/down status.
- Tier 2 – Partially monitorable: Devices with limited features (e.g., ICMP or limited SNMP via traps). The NMS monitors availability and basic device-level up/down status.
- Tier 3 – Indirectly observable: Legacy devices with no direct monitoring. Their state is inferred through upstream link performance or availability through ICMP (e.g. ping), SCADA alarms, or circuit baselines.

This tiered approach can improve and maximize the scope of devices monitored via the NMS and manage expectations for network baseline completeness.

## Cybersecurity Integration

Cybersecurity is inseparable from reliability and resilience, and an NMS is foundational and strengthens best practice by:

- Providing a record of assets, location, and configurations.
- Detecting unauthorized configuration changes.
- Highlighting anomalous traffic patterns that deviate from baselines.
- Detection of changes to the network performance over baseline.
- Supporting patch management and vulnerability awareness.
- Ability to feed data into Security Information and Event Management (SIEM) platform for unified security monitoring, if used by the utility.
- Credential management for bulk encryption keying material.

Modern approaches to system security and maintenance are reducing the historic separation of duties between network operations and security operations into a more unified team with improved situational awareness and empowerment to resolve issues at the time of discovery, reducing attacker dwell times.

## Planning for Scalability and Future Operations

As the grid becomes more distributed—with inverter-based resources, DERMS, AMI, and microgrids—the number of endpoints utilities may monitor as part of their network may grow. Applying best practices of an NMS can help support other grid operational processes, such as:

- Providing data to forecast future capacity requirements.
- Modeling impacts of new communication technologies (e.g., 5G, private LTE, satellite).
- Ensuring scalability while maintaining determinism and reliability.

### NMS Best Practices: What It Brings to a Utility

#### 1. What does "normal" look like across the network?

By establishing both configuration and performance baselines, the NMS defines what "normal" means for each device, link, and application path. Utilities gain the ability to compare current conditions against stable, long-term expectations. This transforms baseline data into a diagnostic tool that quickly highlights anomalies.

#### 2. How do we know when a change occurs?

The NMS tracks and alerts on configuration changes, topology shifts, and deviations from expected performance. With syslog, SNMP traps, or streaming telemetry, it distinguishes between planned maintenance and unexpected alterations — supporting both operational stability and compliance with change-control policies.  Continuous updating of the baseline as sanctioned changes occur ensures baselines remain accurate, rather than stale.

#### 3. How quickly can abnormal conditions be identified and resolved?

Through real-time monitoring and correlation, the NMS pinpoints performance degradations, loss of redundancy, or unauthorized modifications. Operators receive early warnings before small issues escalate into operational outages. This reduces mean time to repair (MTTR) and supports proactive maintenance.

### 4. How can we monitor third-party services with limited visibility?

Even when circuits are leased or delivered over MPLS/IP, the NMS tracks performance parameters (latency, jitter, error rates) against the baseline. This provides independent evidence when raising issues with service providers and ensures accountability through measurable service-level assurance.

### 5. Which devices can and should be monitored?

By categorizing devices into tiers — fully monitorable, partially monitorable, and indirectly observable — the NMS provides a framework for extending visibility pragmatically. This avoids wasted effort on non-eligible devices while maximizing the utility of available monitoring protocols.

### 6. How do we integrate reliability and cybersecurity?

The NMS reinforces cybersecurity by detecting unauthorized configuration changes, highlighting anomalous traffic, and integrating with SIEM platforms for event correlation. This allows utilities to view every event from both a reliability and a security perspective, unifying operational and security situational awareness.

### 7. How can we plan for future growth and scalability?

With historical performance data and traffic patterns, the NMS informs capacity planning, highlights bottlenecks, and models the impact of new technologies (e.g., private LTE, 5G). It ensures the communication network can scale to meet the operational demands of a distributed, dynamic grid.

## NMS Summary

By directly addressing these questions, the NMS demonstrates its role as a best practice enabler for grid communications. It turns uncertainty into clarity, speeds up root cause analysis, enforces accountability across owned and leased domains, and integrates cybersecurity into operational reliability. In doing so, the NMS supports both present operations and the evolving needs of tomorrow's grid.

# 4. Quality of Service and Resilience Considerations for SONET to IP Conversion

## Background

For decades, Synchronous Optical Networking (SONET)[9] was the workhorse of many private utility telecommunications systems and third-party services provided to utilities, especially those supporting the electric grid. As a Time Domain Multiplexing (TDM) technology, SONET systems have low, deterministic latency due to assigned time slots traveling over set point-to-point primary and alternate routes. Because of its deterministic low latency and jitter, integrated synchronization and timing, standardization (Telcordia GR-253), and SONET ring resiliency, it provided a superior platform for carrying information and time-critical protection traffic throughout the electric grid.

Driven by low cost, higher bandwidth, improved scalability and granularity, and robust applications, IP and Ethernet systems are now the norm throughout nearly all industries. Telecommunications service providers have moved toward packet-based technologies to meet this demand. SONET technology's limited capacity and lack of efficiency and flexibility for carrying packet-based data helped drive this move, as did a shrinking SONET equipment market, making this technology difficult to support.

Many electric utilities have followed this path. The use of Ethernet-based applications and intelligent devices within and beyond the utility boundaries continues to grow and drive the need for reliable, secure, and resilient bi-directional packet-based utility communications to distribute critical data and information where it is needed and within the requirements of associated grid services to operate as intended.

To successfully make this transition from SONET to packet technologies, Quality of Service (QoS) parameters must be understood and maintained differently than on TDM/SONET systems.

## Quality of Service Parameters

There are several QoS parameters that need to be considered and managed on both SONET and packet-based/IP systems, albeit with different methods. One key difference is that SONET systems include an NMS provided by the SONET vendor for their system. This provides all the performance management and monitoring that the system requires. Packet-based systems, however, can be made up of multi-vendor devices and are managed by standard IP visibility tools. The following is a comparison of the QoS parameters and considerations associated with each technology.

---

[9] U.S. Department of Energy. (2024). *Grid Communications Technologies.* Retrieved from https://securecomms.ornl.gov/publications/Grid-Communication-Technologies.pdf

## Latency

- SONET uses set routes that are pre-provisioned, with each device/node known, and can be optimized once for low, deterministic latency.
- IP technologies frequently use dynamic routing, making latency less deterministic. Packet re-transmission due to transmission errors and dropped packets will increase the latency, as can other factors, including network size, firewall delays, protocols used, traffic volume, and priority. Because of this variability, additional steps should be taken by the owner or provider of the packet-based system to achieve acceptable latency for more time-critical applications.

## Jitter

- SONET systems are greatly impacted by timing jitter, since they depend on accurate timing of the time slots to move data through the network. Part of the SONET standard includes jitter filtering at nodes to preserve an accurate signal. A SONET Primary Reference Source (PRS)[10] provides the basis for the SONET synchronization system that provides timing across the system and synchronizes the downstream clocks. It is critical to ensure there are no timing loops and that higher quality clocks always steer lower quality clocks as the synchronization signals are transported throughout the system.
- Packet-based systems use IP Packet Delay Variation (IPDV) "the difference between the one-way-delay of the selected packets"[11] to measure jitter. IPDV can be measured via a variety of tools such as Traceroute and Ping. Jitter should be regularly measured whether the network is internally owned or leased from a third party. Management of high IPDV values can be accomplished by adjusting jitter buffers, reducing congestion, and prioritizing traffic.

## Packet Loss

- SONET systems do not have packet loss. There can be data errors and sampling issues, but there is no real equivalent to packet loss in TDM.
- For packet-based systems, packet loss is when one or more packets are not delivered to their intended destination. Often this happens when there is network congestion due to oversubscription, routing errors, or higher than normal traffic. In wireless systems, packet loss can also be caused by a low signal to noise ratio. The extent of the problem and the network segment(s) contributing to the problem can be located with Traceroute or Ping. SNMP traps can also monitor for congestion if access to network elements is available.

---

[10] Telcordia Technologies, "SR-Notes-Series 01: Telcordia Notes on The Synchronous Optical Network (SONET)," December 1999. [Online]. Available: https://telecom-info.njdepot.ericsson.net/ido/PDF/SR_NOTES_SERIES_01.i01.pdf [Accessed 7 September2025]

[11] Internet Engineering Task Force (IETF), "IETF RFC 3393 IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)," 17 June 2022. [Online]. Available: htps://datatracker.ietf.org/doc/rfc3393. [Accessed 19 Dec. 2023]

## Availability

Availability, regardless of technology, is a measure of the portion of time that a system is accessible and useable. An availability percentage can be calculated by dividing the uptime by the sum of the uptime and downtime for the system. Knowing the acceptable downtime / minimum uptime that the individual grid services require provides information on what service level metrics should be required of a communications provider or achieved by the utility communications system. Some functions may tolerate hours or days of downtime (revenue metering) while others may only tolerate milliseconds of downtime (high-speed controls). If services are to be aggregated, the grid services having the strictest requirements will drive the overall system requirements. What can differ is how to provide resiliency to increase the availability of an OT system.

- SONET systems include extensive, flexible monitoring and alarming that can be used to inform a Network Operations Center (NOC) directly via a substation alarm unit and/or via an NMS. Signal attenuation and excessive errors can prevent a grid service from performing its function, as can a complete loss of signal. However, SONET systems are normally configured as rings, with automatic path or line switching times below 50 ms, and often closer to 5ms with smaller rings. Because of this, a significant amount of downtime is avoided, maintaining a high availability for the system.
- IP/packet-based systems generally do not include vendor-specific NMS functionality; however some systems, such as MPLS systems, may. Nearly all manufacturers provide Management Information Bases (MIBs) for their equipment that can be used by any NMS to provide monitoring and configuration access. Having this visibility and access greatly increases the resiliency and availability of a network by providing actionable data to correct system issues before they impact the availability of a system.

## Bandwidth and Throughput

Bandwidth is the maximum amount of data that can be transmitted over a network connection, while throughput is the actual rate at which data is successfully transmitted over a connection during a set time period.[12]

- On SONET systems, bandwidth and throughput are normally static and remain that way, due to set time slots being provisioned. Throughput is very close to the allocated bandwidth. The bandwidth is reserved only for that traffic and cannot be used by adjacent channels. However, much bandwidth can be wasted with empty time slots traversing the network, and the time slot cannot increase without being deleted and reprovisioned.
- For IP networks, bandwidth and throughput can be very different. Bandwidth is not allocated; it is shared, often in a very dynamic manner. Through enforcing policies, it can be limited to set values or data can be allowed to "burst" beyond the stated

[12] U.S. Department of Energy, "Understanding and Managing Quality-of-Service in Grid Communications,"2024. [Online}. Available: https://securecomms.ornl.gov/publications/Understanding-and-Managing-Quality-of-Service-in-Grid-Communications.pdf. [Accessed 28 August 2025]

limit, making it variable and very efficient. Throughput, within that bandwidth, can be impacted by congestion, packet loss and re-transmission, and other factors. The throughput can vary for any given connection because packet systems are designed to efficiently transport data. This can be adjusted by using Quality of Service policies. It is important to monitor the throughput of your network, whether leased or owned, to ensure that the QoS requirements of each grid service, and the aggregate, can be met by the throughput being attained. Understanding throughput requirements in the context of the behavior of grid services during power system events, when large amounts of data may be transmitted at once, will assist in requesting bandwidth and specifying or accepting QoS policies.

## QoS Policies and Service Level Agreements (SLAs)

Quality of Service policies, documented by SLAs, are key to managing traffic on a packet-based system. These policies are a "set of rules or mechanisms designed to manage network resources efficiently and to ensure the performance, reliability, and priority of various types of data traffic on the network."[13] While ensuring QoS parameters stay within the requirements of the grid services being carried can be a challenge, there are many methods available to achieve this on a communications system.

The first step is to classify packets of traffic into categories based on the requirements of the grid services and then mark them with specific priorities. Category criteria can be sources and destinations, type of service, latency limits, or other parameters. This is then used to group similar requirements into a class of service (CoS) and then adjust the QoS policy for that traffic. An example would be placing latency-sensitive services (e.g., protective relaying) into the same class having high priority in network queues, which then maintain latency QoS for this class by dropping other, non-time critical classes to avoid congestion.

When services are obtained by a third-party communications provider, SLAs are paramount. Ensuring adequate bandwidth to enable appropriate throughput and avoid packet loss and high latency can be critical for some applications, while allowing bursting for mirroring operational databases may be more important for other applications. It is important to ask questions and understand as much as possible about how the traffic will be categorized and managed. Some providers are willing to collaborate with utilities on SLA development if the utility understands some of these key aspects.

Finally, having a network management system that can monitor performance under the SLA can arm the utility with data if there are network performance issues, preferably before the SLA requirements are no longer met.

[13] U.S. DOE, "Understanding and Managing Quality-of-Service", 9-10.

## Multi-protocol Label Switching (MPLS)

Many utilities have upgraded their private SONET communications systems to other technologies for reasons noted earlier in this section coupled with other drivers within their own environment. Many have chosen to convert to a version of MPLS because it attempts to deliver more deterministic latency. Additionally, many network equipment providers implementing MPLS also provide traditional TDM interfaces, easing integration with legacy SONET equipment. This provides a transition step for current equipment and makes for a relatively smooth transition without having to change to IP-capable end equipment (e.g., meters and relays). This allows the utility to replace non-packet-based equipment with packet-based equipment on its own lifecycle, not on the lifecycle of the communications system.

Multiple distinct architectural implementations of MPLS have been standardized by the Internet Engineering Task Force (IETF). The primary two are IP/MPLS (IETF 3031) and MPLS-TP, a more recent "Transport Protocol" collaboration between the International Telecommunications Union (ITU) and IETF. MPLS-Transport Profile (MPLS-TP) is a version of MPLS specifically designed for the strict timing requirements of mission-critical networks, such as those in energy, transportation, and industrial automation. It has the following characteristics:

- Bidirectional Label Switched Paths (LSPs): Unlike IP/MPLS, which uses unidirectional LSPs, MPLS-TP uses bidirectional LSPs. This means data in both directions follows the exact same, congruent path, simplifying operations and ensuring more deterministic performance.
- Traffic engineering constraints: MPLS-TP adds constraints that remove some complex and unpredictable MPLS functions, such as Equal-Cost Multi-Path (ECMP) routing and LSP merging. By restricting how traffic is managed, MPLS-TP ensures a more fixed and predictable data flow. Both have pros and cons and can be used to emulate existing TDM traffic. Both can implement some form of traffic engineering in the sense of manual provisioning to control latency and other QoS parameters. It remains the responsibility of the utility or their engineering agents to decide what variations of these protocols will best fit their particular requirements and topologies.

In some cases, a reconsideration of how time-critical functions are designed and implemented to obtain redundancy and low latency is necessary. One interesting example of this is the approach that San Diego Gas and Electric implemented for their transition from SONET to MPLS. Implementing two channels on each relay, combined with alternately routed redundancy, provided a way to meet their requirements.[14]

[14] D. Dietmeyer, K. Lawlor, K. Allameh, E. A. Udren, K. Fodero and K. Garg, "Teleprotection with MPLS Ethernet Communications - Testing and Experience With Practical Installations," 2025 78th Annual Conference for Protective

There are multiple sources for MPLS equipment, each with implementation variations. Considerable thought should be devoted to requirements, architecture, and planning followed by multi-stage testing, whether by the utility or utility-witnessed testing at a vendor or third-party facility.

## SONET to IP Recommended Maintenance Practices

In moving from SONET to an IP system, maintenance practices should be considered and adjusted to the new system, with the intent to repeat maintenance actions on at least a yearly basis. The following areas are a good place to begin.

Security best practice is to adopt a deny-by-default position for an IP system. After denying all, review the list of ports required on all devices by consulting equipment documentation. Enable only the ports needed by each device. Know the protocols to be used on the system and pay particular attention to the ports required by each protocol. Some examples of key ports to investigate include:

- Port 20,000 for DNP3
- Port 502 for Modbus/TCP
- Port 22 for SSH

When configuring firewalls, ensure that the last rule will drop all remaining unmatched traffic. Limiting the number of trusted parties responsible for firewall configuration changes and having a process in place to review and approve changes or additions to firewall rules can help increase network security. Firewall rules should be reviewed at least annually.

Measure the baseline for each of the network's QoS parameters when the system is installed and check against that baseline as a maintenance item. Key parameters for utility systems include end-to-end latency and throughput.

- As new traffic types are added to the system, ensure that the traffic priorities in QoS policies or SLAs are still appropriate. Adjust if needed.
- A properly configured NMS system can help automate these maintenance actions by including sensors to measure the QoS parameters at strategic points within the network. As the network grows, add additional sensors to expand visibility.

## SONET to IP Conversion Summary

Navigating the transition from SONET to IP/packet-based technologies is a complicated process with many alternatives to be considered whether obtaining third party services or implementing a private utility system. Understanding Quality of Service parameters and how specific grid services drive the QoS requirements provides background for implementing QoS policies and SLAs to enable communications to successfully support

---

Relay Engineers (CFPR), College Station, TX, USA, 2025, pp. 1-20, doi: 10.1109/CFPR67343.2025.11013212. [Online}. Available: https://ieeexplore.ieee.org/abstract/document/11013212. [Accessed 28 August 2025] grid functions. Pre-testing new services or a new internal system prior to placing an OT communications network in place is key to uncovering and resolving QoS issues before they can impact grid operations. Having strong maintenance practices in place will help the communications system reliably support the electric grid.

# 5. Synchronization and Timing

In modern power utility infrastructures, precise time synchronization must be reliably distributed to numerous endpoints. A wide range of Operational Technology (OT) systems—supporting bulk power generation, transmission, and distribution—depend on synchronized time to ensure simultaneous and coordinated operation. These include supervisory control and data acquisition (SCADA) systems, protective relays, in-band and out-of-band communication networks that support grid infrastructure, as well as both modern and legacy grid sensors. Time alignment across these systems ensures deterministic behavior and accurate event correlation, which is essential for reliable grid operation. Furthermore, regulatory compliance mandates accurate timestamping for sequence-of-event (SOE) recording and fault recording, necessitating precise synchronization.

The **Network Time Protocol (NTP)** is a widely adopted, internet-based protocol for synchronizing the clocks of devices connected to IP-based networks. NTP typically achieves synchronization within a few milliseconds, which is sufficient for general Information Technology (IT) applications. It is commonly implemented using geographically dispersed servers, often accessed over public or private internet connections via the NTP Pool Project or public NTP servers. Lately, more organizations have been turning to internal, trusted NTP servers linked to an internal timing master source. NTP supports authentication mechanisms that allow clients to verify the identity of time servers, mitigating the risk of synchronization with unauthorized or malicious sources. Although NTP offers adequate accuracy for non-critical systems, its millisecond-level precision is insufficient for time-sensitive grid operations like protective relaying and synchrophasor measurements, which require sub-microsecond accuracy.

For applications requiring higher precision, the **Precision Time Protocol (PTP)**—as defined by the IEEE 1588 standard—is a more suitable solution. Introduced in 2002 and now in its third iteration, PTP enables sub-microsecond and even nanosecond-level accuracy when deployed over properly engineered networks with deterministic latency and end-to-end control. PTP is widely used across industries including telecommunications, finance, industrial automation, and electric power grids. It achieves high precision by compensating for network-induced delays at each hop.

PTP operates through a master-slave architecture, where a timing master (grandmaster clock (GMC)) transmits time information via IP packets (IEEE 1588-2008 Annex D, a.k.a. 8275.2) or Ethernet frames (IEEE 1588-2008 Annex F, a.k.a. 8275.1). Time slaves receive this information and, using the embedded timestamps, generate a 1 pulse-per-second (1 PPS) signal and a synchronized clock output at the required frequency. These signals are referenced to a defined time base (epoch), typically in nanosecond precision, enabling deterministic execution of time-critical functions.

Both NTP and PTP serve as foundational time distribution protocols that enable coherent operation across IT and OT domains. Accurate time synchronization is crucial for coordinated switching and relay operations, governing transactional integrity in data-centric processes, audit support, and log correlation. Deviation beyond 1 microsecond between time-sensitive systems may result in anything from minor inconsistencies to critical protection system misoperations.

**IRIG-B (Inter-range Instrumentation Group time code B)** is a widely used time distribution protocol that transmits time-of-day information in a fixed, serial format, typically once per second. It is known for its reliability and is commonly used in electric power systems, especially for synchronizing devices like protective relays, SCADA systems, and phasor measurement units (PMUs), often via dedicated coaxial or fiber-optic cables. IRIG-B delivers dedicated timing signals that require a physical, point-to-point connection, offering accuracy in the range of 10 microseconds to sub-millisecond levels, depending on the implementation. Although it lacks the flexibility of network-based protocols like NTP or PTP, IRIG-B continues to be favored in legacy grid infrastructures due to its robustness and deterministic performance. As modern power systems increasingly adopt network-based timing distribution methods, the remainder of this document will focus on the NTP and PTP protocols.

Time synchronization operates through a hierarchical model known as **time strata**, where:

- **Stratum 0** denotes the primary reference source (e.g., atomic clocks, GPS clocks),
- **Stratum 1** systems interface directly with Stratum 0 and act as primary distribution servers,
- **Stratum 2 and beyond** receive and propagate time downstream using NTP or PTP, maintaining accuracy appropriate to their role in the synchronization hierarchy.

NTP remains adequate for general-purpose applications; however, PTP is essential for the sub-microsecond timing requirements of modern power systems, ensuring reliability, regulatory compliance, and coordinated operation across the grid.

## Deploying Internal NTP and PTP

Wide-area time synchronization is essential for maintaining coordinated operations across power generation, transmission, and distribution systems. Traditionally, this synchronization has relied on the Global Positioning System (GPS) and NTP. Since its introduction in 1980 and formal standardization in 1988, NTP has been broadly supported in commercial grid infrastructure, enabling device synchronization through publicly accessible internet-based time sources, such as those provided by the National Institute of Standards and Technology (NIST).

However, the reliance on internet-based time services introduces significant cybersecurity vulnerabilities. NTP is susceptible to various attack vectors, including man-in-the-middle (MitM) attacks where time packets are intercepted and altered, distributed denial-of-service (DDoS) attacks targeting time servers, and masquerade attacks in which adversaries impersonate legitimate time sources. These exploits can disrupt grid operations or conceal malicious activities within critical systems. While NTP remains widely used, its dependency on public networks presents inherent risks.

To enhance security and resilience, organizations are increasingly adopting internal, trusted time sources such as GMCs. These devices typically derive time from Global Navigation Satellite Systems (GNSS) and incorporate advanced features such as spoofing detection and extended holdover capabilities, allowing them to maintain accurate time synchronization independently for extended periods, even in the absence of GNSS signals (refer to Figure 3).

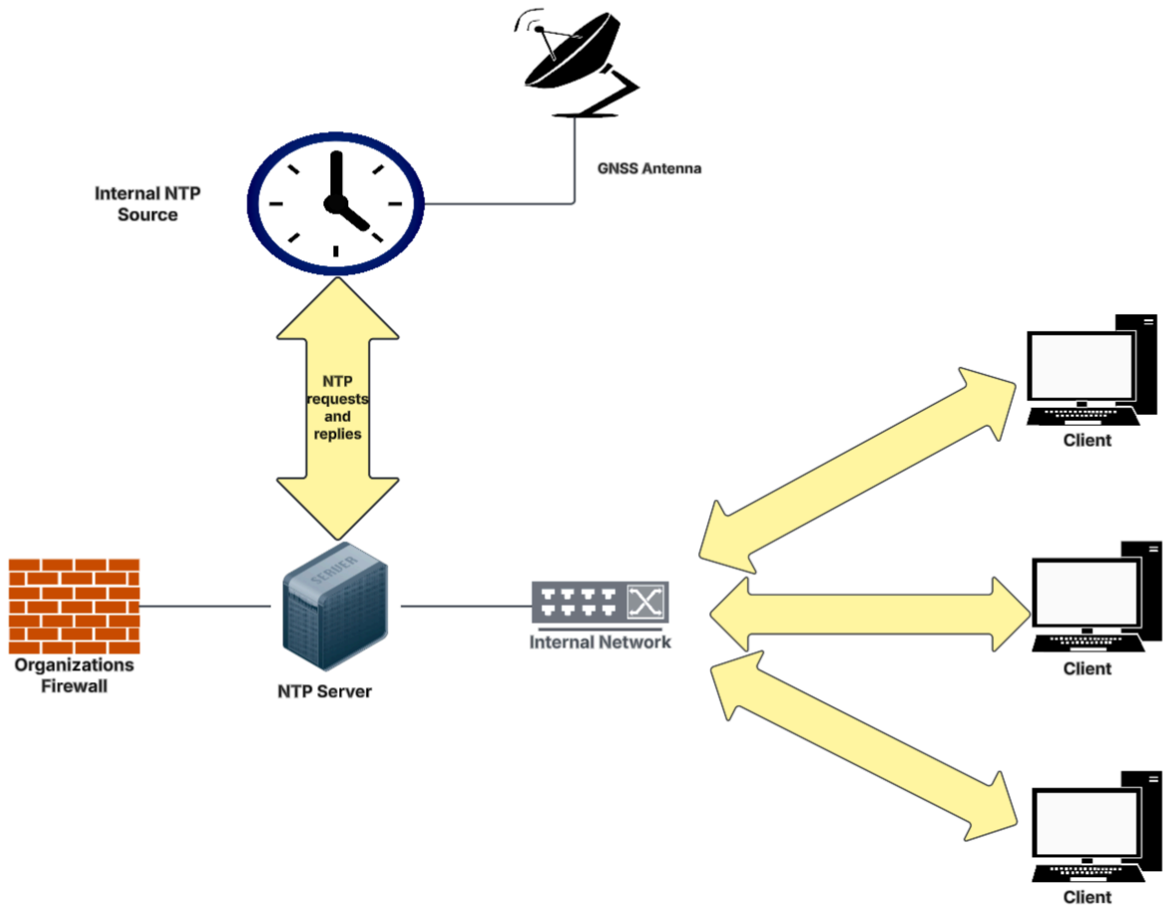


Figure 3: An example illustrating how an internal NTP setup enhances network timing security by eliminating the need for the firewall-exposed path required by external NTP sources.

In contrast, PTP offers a robust alternative to NTP by addressing its security vulnerabilities and significantly improving timing precision and reliability. By utilizing internally managed, point-to-point communication links, PTP ensures secure, high-accuracy timing distribution and avoids the firewall traversal issues commonly associated with traditional NTP systems. Despite its technical advantages, PTP remains less commonly integrated into existing grid infrastructure as compared to NTP. For systems that lack native PTP support, it is advisable to configure a GMC to serve as both a secure PTP source and an internal, trusted NTP server. This ensures that time synchronization at Remote Synchronization Units (RSUs) remains isolated from the vulnerabilities of publicly accessible NTP servers, such as spoofing or denial-of-service attacks (refer to Figure 4).

NTP has historically provided dependable time synchronization, however, the increasing cybersecurity demands of critical infrastructure—such as the electric power grid—necessitate more robust solutions. Integrating PTP and internal timing architectures, including hardened GMC deployments, offers a path toward secure and reliable time distribution using diverse synchronization mechanisms.

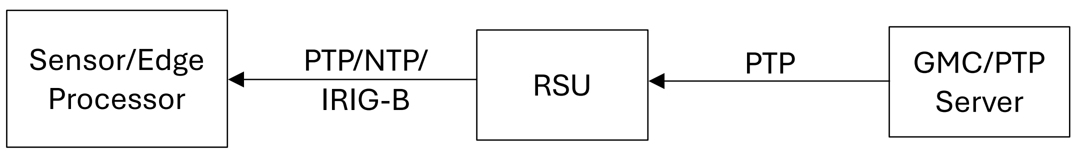


Figure 4: Proposed architecture for establishing a timing signal using different methods for synchronization.

## PTP/NTP Security

PTP and NTP provide time synchronization services over grid infrastructure that includes IP networks, time servers, and various supporting systems. An internal, trusted NTP setup enhances network timing security by eliminating the need for the firewall-exposed path or open ports required by external NTP sources. Therefore, robust configuration management across all infrastructure components, coupled with continuous monitoring of both the infrastructure and the operational state of PTP/NTP services, is essential to meet the cybersecurity requirements of time-critical service delivery.

In addition to standard system and network cybersecurity measures, dedicated monitoring of PTP and NTP operations plays a critical role in maintaining overall network integrity. Monitoring activities can be classified into three principal categories: server monitoring, network traffic monitoring, and data analytics.

### NTP Monitoring

- **NTP Server Monitoring** focuses on assessing the availability, dependencies, and operational status of NTP servers. Proactive monitoring can help detect early indicators of anomalies—whether caused by malicious activity or unintentional system failures—and trigger timely corrective actions such as reconfiguration, maintenance, or replacement. Common monitoring tools include open-source options such as *ntpd* and *NTPmon*, as well as commercial solutions like *SolarWinds* and *Paessler PRTG Network Monitor*.

- **NTP Network Traffic Monitoring** provides a comprehensive view of the operational status of the NTP communication network by analyzing timing traffic patterns. It enables the detection of abnormal conditions, such as DDoS attacks targeting NTP over UDP port 123. Monitoring tools like *Wireshark* and *SonicWall* can be utilized to observe and assess this traffic in real time.
- **NTP Monitoring Data Analytics**—potentially augmented by AI/ML algorithms—can be applied to both real-time and historical traffic data to identify anomalies, including deviations in traffic volume or timing patterns. Such deviations may signal cyberattacks or benign faults such as misconfigurations or degraded network performance.

### PTP Monitoring

PTP is typically used as the primary time distribution backbone for high-precision synchronization over terrestrial IP networks, particularly in critical infrastructure environments. Ensuring the accuracy and security of PTP-based time distribution requires comprehensive monitoring of server health, network traffic, and system performance metrics.

- **PTP Server Monitoring:** Monitoring PTP master clock systems is foundational for maintaining reliable time dissemination. Key server parameters and configurations should be retrieved and validated regularly through network management protocols or command-line interfaces. Compliance checks and configuration audits ensure consistency and prevent misconfigurations. *Dataminer* is one example of a tool supporting PTP server monitoring.
- **PTP Network Traffic Monitoring:** Monitoring PTP traffic enables visibility into time synchronization flows over the network. PTP Version 1 (IEEE 1588-2002) operates over IPv4 using multicast messaging, while PTP Version 2 (IEEE 1588-2008) and Version 2.1 (IEEE 1588-2019) support both IPv4 and IPv6 in multicast and unicast modes. Capturing traffic with specialized tools allows for anomaly detection and performance validation. *Meinberg PTP Track Hound* is a purpose-built tool for PTP traffic analysis.
- **PTP Monitoring Data Analytics:** Offline or near-real-time analytics using AI/ML techniques can identify both malicious and non-malicious anomalies. Detected threats may include man-in-the-middle attacks, impersonation, best master clock (BMC) algorithm manipulation, and denial-of-service attempts. Operational issues such as asymmetric delays, clock drift, jitter, hardware degradation, or configuration errors can also be diagnosed through in-depth analysis of time synchronization behavior.

## Synchronization and Timing Summary

Utilizing PTP in accordance with established standards ensures that a properly engineered and implemented network infrastructure can deliver the level of timing accuracy required by a range of time-sensitive power system applications. These include protective relaying, synchrophasor and phasor measurement unit (PMU) networks, SCADA systems, substation automation, and energy market operations, among others.

A critical consideration in deploying NTP-based synchronization in critical infrastructure such as the modern power grid is to implement a trusted internal NTP configuration that improves network timing security by removing the reliance on firewall-exposed paths or open ports. Another consideration is the flexibility to integrate diverse timing delivery methods between the root time source (e.g., a GMC) and RSUs. This approach allows the timing architecture to be optimized based on the capabilities and constraints of the underlying transport technologies across different segments of the network.

# 6. Conclusions

As the grid evolves, the communications architecture will need to evolve with it. That architecture affords a structured means by which the evolving complexities of the modern electric grid can be managed. This document provides best practices that can be implemented in the grid of today and evolve towards the grid and grid architecture of the future.

The evolving grid and its control communications increasingly rely on commercial communications providers and a variety of technologies, from wireless (e.g., 5G, microwave, Wi-Fi) to wireline (fiber, copper) to radio communications (P25, other repeater-based systems), and all of these communications systems rely on electric power. A reliable and resilient grid must account for this complex set of interdependencies in its planning activities, especially those involving restoration and recovery. The participation of all relevant parties in both planning and exercising of plans can prevent unexpected conditions that impede the reliable operation and recovery of the grid.

An NMS is a best practice enabler for grid communications. By documenting the operational state, defining and monitoring baselines, detecting changes, and accelerating response to abnormalities, an NMS strengthens the resilience of the communication infrastructure. In doing so, it transforms the OT network from a hidden dependency into a managed, trusted, and strategic asset that supports both present operational demands and the future grid. For utilities facing the dual pressures of modernization and heightened reliability expectations, adopting and maturing NMS capabilities is a foundational best practice for grid communications.

When transitioning from legacy SONET to an IP/packet-based technology, key factors to understand are how requirements of grid services translate to requirements for QoS parameters such as latency, bandwidth and throughput, IP packet delay variation, packet loss, and availability. Being able to translate these into QoS policies and SLAs assists in providing what the grid needs to function properly while putting a communications system in place to meet the requirements of tomorrow's electric grid. Investigating packet technologies with attributes useful to electric utilities and being diligent in the development of requirements, plans, and testing options further improves this transition.

Secure and reliable timing is another key component to a reliable and resilient grid that can operate through adverse events. A trusted internal NTP configuration improves network timing security by removing the reliance on firewall-exposed paths or open ports. It also provides the flexibility to integrate diverse timing delivery methods between the root time source (e.g., a GMC) and RSUs. This approach allows the timing architecture to be optimized based on the capabilities and constraints of the underlying transport technologies across different segments of the network. PTP should be used in accordance with established standards to ensure that a properly engineered and implemented network infrastructure can deliver the level of timing accuracy required by a range of time-sensitive power system applications.

Grid utilities implementing these best practices will take a much-needed step forward to a resilient, secure, adaptive architecture in support of grid stability and reliability.