BURNS McDONNELL

WHITE PAPER

Overcoming Synchronization Cyberthreats in Today's Complex Energy Networks

By Dustin Williams, PE, and Nino De Falcis, ADVA Optical Networking OSA

With PLTE deployment and network technology advancing to accommodate new power generation, reliable and accurate synchronization is becoming vital. To make the experience seamless, utilities need to invest in equipment that can provide a real-time assessment of grid health as well as immediate notifications of events.

Until recently, power grids have always been passive, centralized systems. Energy flows have gone in only one direction, with AC power delivery from producers to consumers. But today, due to growth in the renewables sector and the fact that energy resources deliver energy across much wider areas, operators have to manage a more dynamic, complex and interconnected environment involving bidirectional AC and DC energy production and distribution.

This shift to a smart grid means extending support beyond large power plants to also include smaller-scale power producers like wind farms, electric vehicle (EV) charging stations and solar power generation sites. The one-way distribution network must evolve into an intelligent power grid supporting ever-changing power flows.

The ability to obtain and leverage accurate positioning, navigation and timing (PNT) information is crucial to the effort, and because PNT plays such an essential role in managing the smart grid, it is vital to protect its integrity. By deploying resilient solutions capable of offering multilayer detection, multilevel fault-tolerant mitigation, and highly accurate multisource backup, any threats to PNT can be successfully countered.

Barriers to Meeting Tighter Timing Requirements

Using a purely satellite-based source of time to synchronize substations creates significant risks. Any interruption to Global Navigation Satellite System (GNSS) signals could affect accuracy, negatively impacting the power grid's operational integrity. In the worst case, this could lead to power outages.

Regulators classify power grids as critical infrastructure, and countries worldwide have begun distributing guidelines for making the PNT data they depend on fully redundant. In 2020, the U.S. government issued Executive Order 13905, which aims to strengthen national resilience through the

responsible use of PNT services. The Department of Homeland Security (DHS) provided the framework of rules to harden the U.S. against interruptions caused by malicious actions. The DHS framework outlines four resiliency levels: from level 1, with only one source providing PNT data, through level 4, which involves a next-generation system deriving and distributing PNT from multiple sources. Additionally, a level 4 requirement is for systems to be able to operate for long periods without a GNSS- or ground-based timing source. This self-sustainability is critical for when signals are compromised. In addition to the DHS framework, an IEEE standard (P1952) on resilient PNT is currently in development.

The massive amount of data generated by distributed infrastructure, such as private solar panels and EV charging points, needs precise timestamping to effectively manage demand and supply. Historically, dedicated systems have provided timing at substations, using separate cabling and specific protocols. Such time code protocols deliver time information from a local clock that connects with each intelligent electronic device (IED). The time is coded as a digital data stream frequently supported by a pulse-per-second (1PPS) signal for precise alignment of the time code information. In many cases, GNSS is used for synchronizing the local time to a global reference.

Different timing protocols have their own benefits. Network time protocol (NTP) provides time of day (TOD) to substations that can be used to time stamp information such as event time or syslog time. Packet networks based on internet protocol (IP) and Ethernet are now widely available and largely use NTP for delivering time to substations and remote sites in a power grid. The one drawback of NTP is the lack of frequency and phase source; therefore, a protocol is still needed to provide frequency synchronization and phase synchronization. While GNSS-based timing can provide this frequency and phase accuracy, NTP cannot. Applications requiring synchronization of both frequency and phase need to use IEEE 1588 precision time protocol (PTP).

To accommodate the growing number of power grid elements requiring more precise timing, a shift must occur away from legacy NTP, which has millisecond accuracy needs, to PTP-based timing. By using PTP, with its sub-microsecond accuracy, a network can provide an elevated level of operational sophistication and higher accuracy in monitoring the power grid and localizing faults.

Circuit emulation in utility networks is a critical service that provides relay communication and, in some cases, SCADA backhaul. Frequency synchronization is critical for these services, as the time-division multiplexing (TDM) circuits require precise pulses to align the data and prevent bit slips, which lead to data corruption. Additionally, applications such as synchrophasors need accuracy better than 1 microsecond. For fault location, accuracy to 100 nanoseconds is required. The micro-PMU needs less than 1 microsecond, substation LAN communication protocols have to be time stamped at 100 microseconds for GOOSE IEC 61850, and 1 microsecond is required for IEC 61850 sample values. Should GNSS- or ground-based timing be compromised by deliberate attacks like jamming, spoofing or natural phenomena, accuracy in the aforementioned categories would still need to be maintained. Without highly accurate timing and frequency and phase synchronization from PTP, the smart grid is vulnerable to partial outages and blackouts.

Facing Sophisticated Threats

Threats to PNT can either be internal or external (see Figure 1). Primary external threats include jamming (interfering with GNSS signals), spoofing (the act of transmitting false GNSS signals) and the destruction of GNSS satellites. Given the potential threats, it is essential to avoid dependency on GNSS alone. All of these threat vectors can cause significant disruption to PNT data and represent a major public safety threat. Spoofing is primarily the work of military operations and is the most difficult to detect, whereas GNSS jamming can be carried out relatively quickly.

Attacks on NTP and PTP, as well as on active GNSS receivers, are the primary forms of internal threats to PNT. Traditionally, NTP is used by power grids to distribute timing to substations. On public networks this represents a significant area of vulnerability because hackers can harness a process called NTP amplification, which acts as a distributed denial of service attack (DDoS). In this attack, the hacker requests information from a remote system, spoofing the source address as an IP of the target system. Suppose multiple requests are created from different NTP servers, and all point back to the client system, which is the target system. In that case, this leads to degrading service for legitimate requests by overflowing the system with the received information. The mitigation for NTP attacks is to isolate the power networks from internet traffic or verify devices on the network are secured with the latest version of NTP.

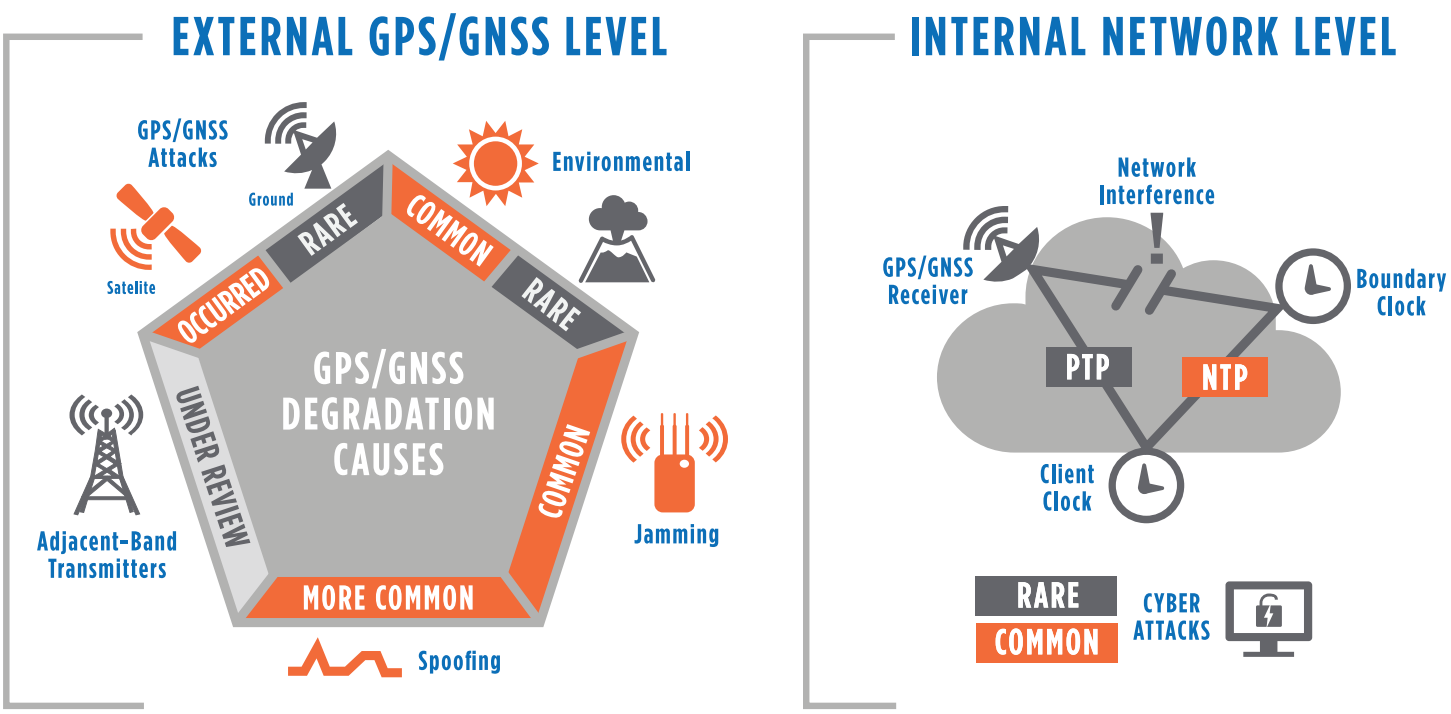

***Figure 1:** PNT cyberthreats and GNSS vulnerabilities. Source: Oscilloquartz.*

Securing Smart Grid Timing Components and Substation Timing Architectures

Protecting the integrity of the smart grid means countering both internal and external threats to PNT. To do this, smart grid operators must leverage a zero-trust framework of PNT sources inside and outside their private networks. With this approach, no single PNT source is trusted. Instead, multiple PNT sources are used within the smart grid to verify each source's data and make comparisons in real time to determine which are most accurate and valid.

Using multiple sources depends on having the means to communicate and distribute timing. PTP provides this means and the required accuracy for phase and frequency, and it has matured support for network applications such as smart grid networks. PTP can be implemented with physical hardware time stamping to minimize delay and achieve the elevated accuracy required by substation systems. PTP is also complemented by timing functions in the packet network transport equipment. Transparent clocks compensate for packet processing delays in packet switches. Boundary clocks combine grandmaster functionality with clock recovery to eliminate delays and packet delay variation.

With these mechanisms, the packet network becomes time-aware and improves the quality of PTP delivery.

In short, the packet network needs to be built to be PTP-aware to deliver the high-accuracy frequency, phase and time services required by smart grid technologies.

Yet PTP remains vulnerable as long as it relies on GNSS as the only source of accurate network timing. For example, a jamming or spoofing device could be used to block GNSS reception on an edge grandmaster at a substation. At the same time, a concurrent attack at the network's core could compromise the ability of an enhanced primary reference time clock (ePRTC) to receive GNSS signals.

In this situation, the first line of defense would be intelligent software and monitoring systems, which would alert grid operators to the GNSS attacks. The response to the attack occurs upstream from the substation, where the core ePRTC has become an unreliable source of timing due to loss of the GPS source. The ePRTC is equipped with a cesium clock that propagates a trusted PNT backup source into the smart grid network. The ePRTC cesium clock has no antenna, no RH signal, and is a stratum 1 clock that can propagate highly accurate timing — accurate to 1 microsecond over four months — throughout the network. It would then become the trusted timing source until GNSS service can be reestablished. PTP-based timing would continue to be propagated, and the attack would not compromise the grid.

Trust in Zero Trust

Today's smart grid is a vast patchwork of PNT-dependent infrastructure, transforming how energy is produced and managed. The smart grid also provides opportunities for utilities to leverage intelligent control and management systems to operate grids more efficiently, safely and much closer to capacity.

However, cyberattacks on PNT infrastructure are increasing in sophistication and frequency just as the smart grid is facing unprecedented demand from an increasing number of applications and distributed energy resources. It is therefore vital that migration to self-sustainable PTP-based timing networks accelerates if the utility sector is to successfully counter the external and internal threats to the PNT data that this infrastructure depends on.

The cornerstone of secure and self-sustainable timing networks is the concept of zero trust. That's why smart grids and all other critical infrastructure dependent on PNT should employ a multisource approach to building timing networks comprising intelligent management software and timing devices equipped with good PTP holdover.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

About Oscilloquartz

Oscilloquartz is a pioneer in time and frequency synchronization. We design, manufacture and deploy end-to-end synchronization systems that ensure the delivery and assurance of highly precise timing information over next-generation packet and legacy networks. As an ADVA company, we're creating new opportunities for tomorrow's networks. For more information, visit oscilloquartz.com.

212645-0223