PNNL-30780

Energy Sector Position, Navigation, and Time Profile

March 2021

Jeff Dagle
Lori Ross O’Neil
Frank Tuffner
Chris Bonebrake
Matt Engels
Gregory B. Dindlebeck

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov**

PNNL-30780

Energy Sector Position, Navigation, and Time Profile

March 2021

Jeff Dagle
Lori Ross O'Neil
Frank Tuffner
Chris Bonebrake
Matt Engels
Gregory B. Dindlebeck

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

The Pacific Northwest National Laboratory has developed this positioning, navigation, and timing (PNT) profile for the Energy Sector at the request of the U.S. Department of Energy. The Department of Energy is the sector-specific agency for the Energy Sector and is responsible for providing guidance in the form of this PNT Profile, per Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services[1] (Executive Office of the President 2020) issued February 18, 2020.

Executive Order 13905 directed the National Institute of Standards & Technology to develop a PNT Profile that is broadly applicable to all sectors and to serve as a foundation for sector-neutral guidance, NISTIR 8323 *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*. This document builds on NISTIR 8323 to identify and serve as the required Energy Sector specific guidance.

For purposes of this PNT Profile, Energy Sector precise time is 0.5 µs (microseconds) to 1 µs accuracy. Currently, the electricity subsector has systems that use this level of precision time, but the oil and natural gas subsector currently does not. While the electricity subsector uses precision timing, it does not use positioning and/or navigation at this level of accuracy. For this reason, this PNT Profile will focus on only precise time for the electricity subsector.

[1] https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing. Date Accessed: 15 Dec. 2020

Acknowledgments

The Pacific Northwest National Laboratory project team gratefully acknowledges the guidance and assistance provided by Mr. David Howard of the U.S. Department of Energy. We also extend our thanks to Shabbir Shamsuddin for his oil and gas contribution to this document and Dr. David McKinnon, Pacific Northwest National Laboratory, for his peer review of this document. The accuracy of the information and the perspectives presented in this report are the responsibility of the authors.

Acronyms and Abbreviations

Note that only those that do not reside in the NISTIR 8323 are listed here.

ANSI	American National Standards Institute
C/N0	carrier-to-noise ratio
CFR	Code of Federal Regulations
COMTRADE	**Com**mon format for **Tra**nsient **D**ata **E**xchange for power systems
DNP3	Distributed Network Protocol 3
DOS	Denial of Service
eLORAN	Enhanced long range navigation
GLONASS	Global Navigation Satellite System
GOOSE	Generic Object Oriented Substation Event (IEC 61850)
IDS	Intrusion Detection System
IPS	Intrusion Protection System
ISA	International Society of Automation
IT	information technology
LAN	local area network
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NTP	Network Time Protocol
OT	operational technology
ONG	oil and natural gas
PDC	phasor data concentrator
PMU	phasor measurement unit
PNNL	Pacific Northwest National Laboratory
SIEM	Security Incident Event Manager
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SQM	Signal Quality Monitoring
TVE	Total Vector Error

Contents

Figures

Tables

1.0 Introduction

The electric power grid has a growing dependence on precise time. From an operational perspective, precise timing is used for logging and tracking events in the Energy Sector. More recently, precise time is an integral part of certain advanced measurements that are increasingly used for grid operations and planning applications. The most stringent requirement for precision timing used in the Energy Sector today is on the order of 0.5 µs (microseconds) to 1 µs accuracy, which arises from the increasing wide-scale deployment of GPS to provide precise timing for power system applications, specifically the phasor measurement unit (PMU). PMU leverages this timing capability to provide precise measurements of the power system.

However, the basic functionality of the grid itself—synchronous generators interconnected with vast regional grids—does not directly rely on precise time to operate. The disruption of GPS or other timing signals would not prevent today's grid from operating. The grid will continue to function, albeit with the possibility of confusion and corrupted data logs, regardless of the accuracy of the various time references that are used today. The typical accuracy on the internet ranges from about 5ms to 100ms.[2] Energy timing functions that can be met using less precise time, > 1 µs, should consider using Network Time Protocol (NTP), which gets its time from internet time.

On February 18, 2020, Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services,[3] was issued. This directed National Institute of Standards and Technology (NIST) to publish its Interagency Report, NISTIR 8323, *Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*,[4] which outlines how to identify, protect, detect, respond, and recover PNT resources. NISTIR 8323 is intended to help all sectors and their organizations identify systems dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. Each subsector is expected to develop its own sector-specific PNT profile that builds on NISTIR 8323.

To support the protection of Energy Sector's dependency on PNT, the Pacific Northwest National Laboratory (PNNL) has developed this Energy Sector focused PNT profile (known hereafter as PNT profile) at the request of the U.S. Department of Energy. The Department of Energy is the energy-sector-specific agency responsible for providing guidance in the form of this PNT profile for the Energy Sector, to be used to help identify, protect, detect, respond to, and recover from disruption or manipulation of PNT used by electricity, oil, or natural gas, with the intention of protecting the U.S. national critical infrastructure.

Due to the Energy Sector's dependence on GPS for positioning or navigation for applications such as unmanned aerial systems or field crew tracking, which are similar to other sectors (primarily transportation), this document will focus on time, more specifically those applications that rely on precise time, such as PMUs, and not applications that can be met with more granular time such as is delivered by networks via network time protocols. In evaluating precise

[2] http://www.ntp.org/ntpfaq/NTP-s-algo.htm Date Accessed: 27 Mar. 2021

[3] https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/ Date Accessed: 6 Nov. 2020

[4] https://csrc.nist.gov/publications/detail/nistir/8323/final, Date Accessed: 20 Feb. 2021

time use in the Energy Sector for this body of work, it became clear that the oil and natural gas (ONG) subsector did not presently have any precision timing requirements (more precise than NTP). In addition, the U.S. Department of Transportation is responsible for position and navigation for shipping and transportation of petroleum, oil, and natural gas. As the sector-specific agency for those products, its PNT profile will provide guidance for the ONG subsector, including positioning and navigation. For this reason, this document focuses on precision timing of the electricity subsector.

In addition to NISTIR 8323, PNNL has used other sources to develop this document including those from U.S. Department of Homeland Security, North American Electric Reliability Corporation (NERC), Institute of Electrical and Electronics Engineers (IEEE), research papers, industry input, and interviews with subject matter experts.

This PNT profile is intended to be a building block for Energy Sector organizations to develop their own PNT profiles, building upon NISTIR 8323's broad guidance that is sector-neutral. This document is Energy-Sector specific and has made every effort to consider and convey ways the electricity subsector is dependent on precise time and to thoughtfully consider if precise time is critical for its operations and if so, how to ensure resilience to maintain critical operations.

This document is not all encompassing and is intended to be customized by each organization. The resulting organization's PNT profile will become part of its organizational plan and should be reviewed and updated at the same frequency as other operational documents. Each organization should consider its operational dependence on PNT to determine its risk level for loss of availability or integrity of such services and risk approach to mitigate, accept, transfer, or avoid adverse impact. For example, loss of a PNT component such as precision time for a short period of time is acceptable but loss for an extended period may require mitigation such as failover to a backup resource.

This document is loosely aligned with the NIST Cybersecurity Framework and explores Energy Sector dependence on PNT in many forms, the current PNT protection landscape and protection methods for consideration by the Energy Sector, detecting threats to PNT and the consequences of these threats, mitigation of identified threats, responding and recovering from these threats, and finally a forward look at PNT protections in the Energy Sector and next steps.

2.0 [Identify] Current PNT Landscape in the Energy Sector

The first step in protecting an organization's PNT services is to identify which services are used where, when, and to what level of criticality. The Energy Sector typically uses PNT for synchronizing the internal clocks of information technology (IT)/supervisory control and data acquisition (SCADA), digital control systems (DCS), and process control systems (PCS) in the operation of substations, petroleum refineries, pumping stations, compressor stations, oil and gas pipeline operations, and operational technology (OT) computing and telecommunications equipment. The subsector also uses PNT for identifying the physical location of assets and resources. From an operational perspective, timing is required for logging and tracking events and for forensics during catastrophic incidents. For the ONG subsector, it has similar SCADA and IT/OT considerations, but generally the precision requirements are fewer because of the relatively slow dynamics of these infrastructures product movements and processing compared to the electric infrastructure. Coordinating the movement of product in a pipeline is a process that would be measured in hours and days, although the SCADA data for control and monitor is in minutes not milliseconds or microseconds. Therefore, the remainder of this section is primarily focused on the electricity subsector.

Identifying the exact impact and consequences of disrupted or manipulated PNT services is difficult due to the uniqueness in configuration of the many utilities with specific implementations of various vendor solutions. In general, utilities' IT/OT and SCADA systems can survive PNT service disruption for a time depending on the configuration of individual systems, geographic impact of PNT disruption, and quality of each PNT receiver's internal oscillator. An extended loss or degradation of GPS timing signals today could create operational disruption depending on the degree to which specific utilities are leveraging these PNT services to support their operational applications.

Specifically, we assess that the loss or disruption of GPS would affect PMUs the most, as they require the highest timing accuracies (microsecond range). Most PMUs receive their time synchronization using GPS clock receivers. If GPS synchronization is lost, then they can rely on internal clocks for a short period of time. If the GPS signal is disrupted or manipulated (spoofed), then the resulting measurement errors can be more significant. This can be particularly important when power system operators are measuring relative phase angles across wide area networks.

Some applications, while not yet in widespread use, require GPS-enabled precision time to support advanced protective relaying applications. The accuracy required for these devices can be in the 100ns range. Often, these devices are synchronized with each other at adjacent substations through dedicated fiber-optic links, and their dependence on absolute time (that would be provided by a GPS receiver) is not integral to their reliable operation.

Other applications, such as event disturbance recording and cybersecurity forensic investigations, have timing needs in the millisecond range. Inaccuracies in time stamps for sequence of events recordings can cause errors in aligning data and delay or disrupt the forensic investigation of disruptive events (blackouts).

In addition to identifying PNT service use, it is also important to identify the devices that rely on those services. Figure 1 shows a notional utility architecture for both enterprise and control systems. Time services are highlighted in yellow. In this case, synchronized precise time can refer to multiple sources such as global navigation satellite system (GNSS), which includes such things as GPS, global orbiting navigation satellite system (GLONASS), Galileo, Beidou, and other regional systems. The NTP server can get its time from various sources including GNSS or via a reference source such as NIST's time.gov from the internet. Time mechanisms and their related standards are discussed in greater detail in section 3.0.

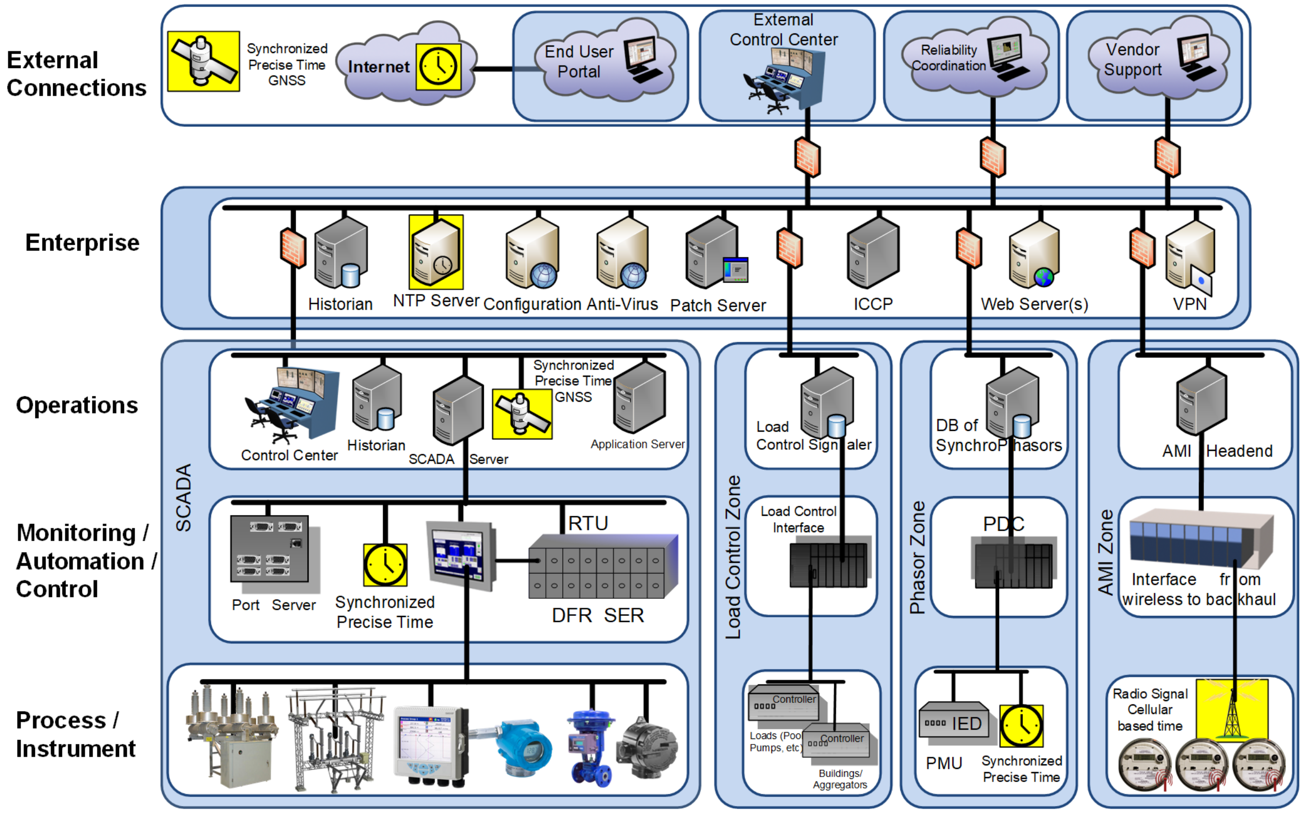

Figure 1. Notional PNT Service Locations within a Utility

The loss of GPS timing signals can also degrade control center operations such as time-tagging events, disturbance data collection, and ability to record events. This data may also be used for playback in dispatcher training simulators. Timing precision on the order of 100ms is necessary to support most control room applications. Disturbance monitoring has a Coordinated Universal Time (UTC) ±2ms requirement.[5] Precise timing is a key requirement to enable accurate post-event analysis. The sequence of events of a major disturbance can often include many events occurring in rapid succession, and properly interpreting cause and effect of various automated controls requires accurate and precise logging of events.

Some utilities have elected to include the results of measurements made by PMUs in the operation of their control rooms. Because the PMU itself is dependent on precise timing, loss of this timing would mean loss of that capability in the control room or in system operations. For this reason, NERC regards some PMU-enabled applications as critical cyber assets (depending on how these measurements are used in operational applications), and therefore they come under the purview of the NERC critical infrastructure protection requirements.

PNT services are used extensively throughout the Energy Sector for a variety of purposes. The impacts and resulting consequences of their loss should be considered during an organization's

[5] https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-002-2.pdf, Date Accessed: 6 Nov. 2020

asset inventory of PNT dependence. Table 1 below shows typical energy system applications dependent on PNT services and their impact due to loss, reduced integrity, or degradation.

Table 1. PNT Dependent Applications and Effects of PNT Loss

	Application Overview		PNT Disruption	
Application	**Purpose**	**PNT Use**	**Impact**	**Consequence**
Digital Fault Recorders (DFR)	Records synchronized power system signals from numerous analog sources within the substation. Relays and other end devices can have their own DFR internally for timestamping of digital events.	PNT is used to timestamp synchronized power system signals.	Disruption of PNT would result in inaccurate or loss of timestamps needed to record synchronized signals.	Timestamps with low integrity could lead to inaccurate situational awareness needed for critical event analysis, such as large blackout type of events. An adversary could prevent recorded signals from synchronizing with the event. This could delay outage investigation activities.
Line Current Differential Relays	Detect faults on both ends of a transmission line. If they do not have a direct fiber connection between them, then they are communicating over a communications channel that can present channel asymmetry. Data from the local and remote relays are compared to determine if there is a fault on the line.	PNT services are used to timestamp current magnitude and phase angle data and send it to the other relay.	If timing were disrupted, the protection function associated with the differential relay will be disabled until timing is restored.	An adversary could force a transmission line to be taken out of service by manipulating the PNT service, which would misalign shared data resulting in an indication of a false condition of the transmission line. This could lead to mistakenly taking the line out of service or cause misoperation of the protection system.
Network Time Protocol (NTP)	NTP is an internet-based protocol designed to synchronize the clocks of systems over a network.	NTP often relies on GPS signals to synchronize the network onto the primary clock.	Loss of integrity for NTP services could result in clock signals being changed.	An adversary could spoof and/or corrupt NTP services resulting in loss of synchronized time, which could lead to loss of situational awareness.

	Application Overview		PNT Disruption	
Application	Purpose	PNT Use	Impact	Consequence
Precision Time Protocol (PTP)	Similar to NTP, the PTP is a network-based time synchronization protocol capable of greater precision of time synchronization than NTP. It is governed by IEEE Standard 1588.	PTP provides time synchronization between network nodes; often the grand master clock is synchronized by a GPS signal or other known time source.	Loss of integrity for PTP services could result in clock signals being changed.	An adversary could spoof and/or corrupt PTP services resulting in loss of synchronized time, which could lead to loss of situational awareness or incorrect operation of connected devices.
Phasor Measurement Units (PMU)	Used to collect voltage and current data at substations in geographically large areas and send it back to a phasor data concentrator at a central location. Example implementations: wide area protection, frequency event detection, anti-islanding, droop control, wide area power oscillation damping, and system modeling verification.	PNT is used to timestamp each sample collected and sent.	Loss of PNT would affect timestamp integrity across many devices within wide areas which may adversely affect control rooms or system operations.	PMU data with low integrity could lead to inaccurate situational awareness. An adversary could either fake an event or mask a real one that is occurring. This could include islanding of the power system or forcing a wide area protection scheme, such as droop control or power oscillation damping to falsely operate.
Phasor Data Concentrator (PDC)	Receives and time-synchronizes phasor data from multiple PMUs to produce a real-time, time-aligned output data stream.	At the PDC, all the received data is aligned via their timestamp.	Loss of PNT would affect timestamp integrity of phasor data.	PDC data with low timing integrity could lead to inaccurate situational awareness.
Sequence of Events Recorders (SER)	This data is critical for event analysis, especially for large blackout type of events. Relays and other end devices can have their own SER internally for timestamping of digital events.	PNT is used to timestamp alarms from numerous sources within the substation	Loss of PNT would result in inaccurate or lost timestamps.	Timestamps with low integrity could lead to inaccurate situational awareness. An adversary could spoof event analysis timestamps. This would delay the investigation into the true cause of an outage.

	Application Overview		PNT Disruption	
Application	Purpose	PNT Use	Impact	Consequence
Substation Local Area Networks (IEC 61850-6:2009 GOOSE and IEC 61850-9-2:2011 Sample Values)	These are integrated protection systems.	Rely on precise time to align data and assist automatic operations.	Loss of PNT would prevent data alignment and lead to failure of automatic operations.	Precise time can be provided locally and there will be no impact if all equipment receives localized synchronized time and none of the schemes were integrated into wide area protection schemes or line differential schemes.
Time Division Multiplex (TDM)	TDM is a communication technique that synchronizes equipment across large areas (when higher level network protocols are not in use)	Relies on PNT services to synchronize their respective systems to function properly.	Without PNT services, communication circuits, including transmission protection circuits, balancing of load across the grid, and remote indication and control of power system equipment would become unavailable.	Loss of PNT could result in degradation of the power system.
Traveling Wave Protection	Fault detection and location for transmission lines time aligns high sampled data to record a transient signal resulting from fault on a transmission.	Precise time allows a device to provide a precise location to the fault by calculating the distance using the time and velocity of the signal.	Loss of PNT services will limit ability to detect location of faulted or failed equipment for transmission lines.	The impact would result in extended outages of transmission lines because manual discovery of the location of the failed equipment would be required.

The impact of a loss of PNT services and time synchronization in electric utility communications has not been fully enumerated in this document. Each utility will need to determine its own unique risk approach to this issue and any remediation actions. Developing PNT profiles that cover this area as well as the applications listed above could help develop consistency in the approach and understanding the consequences of a loss of time synchronization in electric subsector communications.

When a system emergency occurs (such as an electrical reliability event or cybersecurity attack), the exact sequence of events surrounding it is reconstructed from information stored in control rooms, data archives, fault recorders, system logs, intrusion detection systems, and so on around the system. The availability of distributed precise time reduces the challenges associated with reconstructing and understanding the sequence of events.

Without the precision of the distributed time signal, the sequence of events could still be reconstructed, but the reconstruction would become a process that occupies considerably more time (possibly months instead of days) and consumes many more resources.

With a disruption in PNT services, most power system devices will recognize that there is a disruption in timing and alarm as such. With a disruption, typically no adverse reaction occurs, but reliability and functionality of these devices that support power system are degraded, thus degrading the power system itself.

It is important to restate the above consequences may or may not happen due to the configuration and security measures that may be in place. It is expected that organizations will develop refined PNT profiles that consider the above examples and will likely lessen these consequences to their specific environment.

3.0 [Protect] Current Protection Landscape

PNT has several applications in energy systems, from tracking assets to providing a common time basis for actions over a large geographic area. For daily operations, precise timing is one of the primary and critical usage applications of PNT capabilities in the Energy Sector. To make sure the integrity of the time signal is maintained and trusted, standards-based and best-practice techniques are used. While most of the techniques covered in this section focus on the overall integrity of the timing signal (as an input source, not necessarily the quality of the timing source), some of the practices seek to prevent or provide notice of degradation on the timing quality. Where appropriate, aspects that could be leveraged for additional protection, but may not be implemented or are in early stages, will be briefly mentioned.

3.1 PNT-Related Standards in Energy Sector

Standards-based guidance focuses on both the interoperability and integrity of the timing signal and determines if a specific application has any requirements for timing signal usage. The first set of standards explicitly relates to the timing signal itself, rather than applications.

3.1.1 Precision Time Protocol (IEEE 1588-2019)

One of the most widely deployed precision time standards (beyond the requirements that can be met with NTP) is IEEE 1588-2019[6]. The standard primarily focuses on defining the method to translate the timing signal information into a format that can easily be transmitted over a network. The standard defines how different aspects of the precision timing are encoded so any device following the standard can use the timing signal. This includes how devices coordinate the synchronization of this signal over the network. IEEE 1588-2019 does include provisions for defining different types of clocks or sources on the network, so devices may leverage them accordingly. The pure standard supports the distribution of accurate time with 1 ns resolution, but this is heavily dependent on the clock source and network conditions. Practical implementations typically result in an accuracy in the range of 10 ns to 100 ns. This accuracy enables the use of IEEE 1588-2019 in many Energy Sector applications, such as protection and wide-area coordination and fault location scenarios.

Most of the IEEE 1588-2019 standard is aimed at the interoperability aspect. The IEEE 1588 Power Profile defines PTP for use in power systems. The standard does include provisions for key-based authentication/verification of the timing signals. With the proper security key, validity of the timing-based messages can be verified and allow some of the intermediate clocks to perform correction updates to verify the overall integrity of the timing signal. Beyond the key authentication, the IEEE 1588-2019 standard also includes two annexes that provide information on how to improve the integrity and resilience of the timing signal.

IEEE 1588-2019 Annex K provides an example for how to detect rogue GrandMaster clock signals on the network. GrandMaster clocks represent trusted, original timing signal sources on the network. The annex primarily treats the rogue clock as either a legacy entry or a misconfigured message elsewhere on the network and details how to eliminate its impacts via the message exchange under the IEEE 1588 standard. However, it may not provide significant defense against an intentional injection of a rogue clock.

[6] https://ieeexplore.ieee.org/document/9120376, Date Accessed: 6 Nov. 2020

Annex P of the IEEE 1588-2019 standard deals more directly with providing an accurate clock in degraded network conditions (natural or deliberate degradation). Annex P provides suggestions on using GrandMaster clocks on different networks and networking paths to avoid common degradation approaches. Annex P suggests physically separate networks and GrandMaster sources, such as GNSS receivers separated physically far enough to prevent a common interferer.

Beyond the key-based security inside IEEE 1588-2019 and the security suggestions in Annex K and Annex P, the timing information is also secured via typical network security practices. IEEE 1588-2019 dictates the payload of an information packet, so overall message encryption and secure networks associated with the specific protocol are typically deployed. Appropriate network segregation and traffic management are also used to not only keep the timing messages secure but also maintain the accuracy of the clock distributed. Further security suggestions are available in RFC 7384[7] from the Internet Engineering Task Force, although many of the suggestions have been incorporated into the 2019 version of IEEE 1588.

3.1.2 Time Tagging for Intelligent Electronic Devices (IEEE C37.237-2018)

The IEEE C37.237-2018[8] standard defines how time tags are associated with specific measurements. The standard itself does not dictate any accuracy or precision requirements, beyond being sufficient for the intended use of the device and that the source of time is traceable by a recognized international standard. The C37.237-2018 standard outlines the information needed to meet this requirement, including recommending specific profiles or implementations (such as IEEE C37.238-2017 mentioned later) or suggesting ways of encoding the information into a transport standard, like the Inter-Range Instrument Group B variant (IRIG-B) (covered next).

3.1.3 Inter-range Instrument Group Timecode

The IRIG Timecode is a serial standard provided by the Range Commanders Council Telecommunications and Timing Group. The B-variant (IRIG-B) of IRIG Standard 200-16[9] (2016) is commonly used by Energy Sector devices for precision timing. IRIG-B is typically transmitted over a dedicated coaxial-based network from the precision clock source to the devices that require it. Practical timing accuracy is usually in the 1.0 to 10.0 microsecond range. Like IEEE 1588-2019, this level of accuracy enables the use of IRIG-B in many Energy Sector applications, especially for wide area monitoring and control.

The IRIG-B base standard does not include any provisions for security or error checking. Timing quality (precision and accuracy) information can be encoded into extra control bits on the signal (per IEEE C37.237-2018 mentioned earlier), but the base standard does not explicitly define such aspects. Securing the distribution of the precision timing signal relies on physical security of the device network. Nonstandard variants of IRIG-B include timing error information that could be leveraged for very simple security, but these variants are not commonly deployed in the Energy Sector.

[7] https://tools.ietf.org/html/rfc7384, Date Access: 11 Nov. 2020

[8] https://ieeexplore.ieee.org/document/8604153, Date Access: 16 Nov. 2020

[9] https://www.wsmr.army.mil/RCCsite/Documents/200-16_IRIG_Serial_Time_Code_Formats/200-16_IRIG_Serial_Time_Code_Formats.pdf, Date Accessed: 11 Nov. 2020

3.1.4 Network Time Protocol

NTP[10] is another standard method for distributing precision timing information across networks. Much like IEEE 1588-2019, NTP provides information on how to synchronize different clocks and clock sources on the network. While NTP can provide accurate time down to less than 1 millisecond, practical implementations typically result in accuracy between 50 and 100 milliseconds or more. A simplified version of NTP (SNTP) is also available for use, particularly in older devices, but has less accuracy and precision than the base NTP standard. With these levels of timing accuracy, NTP is not used in any time-critical applications of the Energy Sector. NTP is suitable for market-bidding operations or SCADA-level applications requiring time synchronization.

NTP supports key-based authentication and integrity checks. A security-focused fork of the NTP library is available, but it is unclear how widely adopted it is, especially in Energy Sector applications. As was the case with IEEE 1588-2019, this security primarily focuses on the packet payload that NTP defines. Additional network security practices such as limited networks or encryption can be put in place, although they may affect the accuracy of the NTP distribution.

3.1.5 Substation Automation (IEEE/IEC 61850-9-3-2016 and IEEE C37.238-2017)

The previous standards all deal with the distribution of precise and accurate timing information but are general standards that can apply to energy and other sectors equally. The IEEE/International Engineering Consortium (IEC) 61850-9-3-2016[11] and IEEE C37.238-2017[12] standards are extensions of the IEEE 1588 standard that provide specific guidance for power system applications. It is important to note that IEEE/IEC 61850-9-3-2016 and IEEE C37.237-2017 are just different versions of the same standard. IEC 61850-9-3-2016 was an enhancement of the old C37.238-2011[13] standard, and now C37.238-2017 is an enhancement of the IEEE/IEC 61850-9-3-2016 standard. All points of discussion in this section relate to C37.238-2017 but may be valid for older versions of the standard.

C37.238-2017 provides guidance on how to apply IEEE 1588 to power system applications. This includes expected uses and values for different fields in the standard and guidance for interfacing with other time transmittal methods, such as IRIG-B mentioned above. Furthermore, to help aid in adoption of IEEE 1588, C37.238-2017 outlines different time accuracy categories and provides recommended settings. No additional key security or deployment security information is provided over the IEEE 1588-2019 document.

3.1.6 Synchrophasors (IEC/IEEE 60255-118-1-2018, formerly IEEE C37.118.1)

The international synchrophasor standard codified by IEC/IEEE 60255-118-1-2018[14] is a joint IEC/IEEE standard that describes the measurement requirements and approach for phasor measurement units. One aspect of the standard is a requirement that the total vector error between the reference signal and the measurement be less than 1%. From a timing accuracy perspective, this requires the time to be accurate within ±26 μs for a 60-Hz system, assuming only angle error. However, the standard recommends a time source at least 10 times as

[10] http://www.ntp.org/, Date Accessed: 11 Nov. 2020
[11] https://ieeexplore.ieee.org/document/7479438, Date Accessed: 6 Nov. 2020
[12] https://ieeexplore.ieee.org/document/7953616, Date Accessed: 6 Nov. 2020
[13] https://ieeexplore.ieee.org/document/5963699, Date Accessed: 6 Nov. 2020
[14] https://ieeexplore.ieee.org/document/8577045, Date Accessed: 11 Nov. 2020

accurate (±2.6μs for a 60-Hz system) to ensure other contributors to measurement inaccuracy remain below the 1% total vector error (TVE) limit.

In addition to the TVE requirement, IEC/IEEE 60255-118-1-2018 also imposes a requirement on the time tagging of the measurement. Each measurement value requires not only the time of the measurement but also an inclusion of the time quality information such as accuracy of the source clock and leap second status. This additional information is meant to enable adherence to the requirement in the standard that the timing of the measurement be accurately placed within 1 μs of a specified 100-year period.

3.1.7 Data Transport/Aggregation Standards

In the Energy Sector, several other standards are associated with precise and accurate timing but primarily from an application perspective. These standards primarily deal with data transfer between devices and focus on interoperability between compliant devices. Some of the more common standards in the Energy Sector are:

- IEC 61850-9-2-2011 (Sampled Values)[15]
- IEC 61850-6-2009 (GOOSE)[16]
- IEEE 1815-2012 (DNP3)[17]
- IEEE C37.118-2-2011 (PMU data)[18]
- IEEE C37.247-2019 (PDC standard)[19]
- IEC 60255-4-2013/IEEE C37.111-2013 (COMTRADE)[20]

Every one of these standards includes a provision for including precise timestamps for the data being transported. Aside from required data rates in some standards, most of the listed standards do not make any additional requirements on the precision or accuracy of the timing used; it is dictated by the specific deployment, application, or capability being used. Some standards, such as IEC 61850-9-2:2011, have "guideline" versions (similar to the profiles associated with IEEE 1588 mentioned earlier), but these are often unofficial standards or application notes. Some of the standards also include provisions for timestamping collections or aggregations of the data but have phrasing about reasonable rounding and precision (not specifics). Standards like IEEE C37.247-2019 have a requirement for an accurate clock but only to accommodate retransmission delays, with generalized requirements on time accuracy.

3.1.8 Disturbance Measurement Requirements (NERC PRC-002-2)

Unlike the previous standards described, the NERC PRC-002-2[21] standard is not a device or interoperability standard but a compliance standard. The PRC-002-2 puts requirements in place for disturbance monitoring and reporting on the bulk electric system. A significant part of the

[15] https://webstore.iec.ch/publication/66549, Date Accessed: 11 Nov. 2020
[16] https://webstore.iec.ch/publication/63319, Date Accessed: 11 Nov. 2020
[17] https://ieeexplore.ieee.org/document/6327578, Date Accessed: 11 Nov. 2020
[18] https://ieeexplore.ieee.org/document/6111222, Date Accessed: 11 Nov. 2020
[19] https://ieeexplore.ieee.org/document/8830511, Date Accessed: 11 Nov. 2020
[20] https://ieeexplore.ieee.org/document/6654239, Date Accessed: 11 Nov. 2020
[21] https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-002-2.pdf, Date Accessed: 11 Nov. 2020

reporting aspect is that all required data must be timestamped to Coordinated Universal Time with an accuracy of ±2 ms.

3.1.9 Oil and Natural Gas Sequence of Events Records

As previously mentioned, the ONG subsector infrastructure timing requirements are less intensive than the electricity subsector requires, although the basic elements of the command and control infrastructure relying on SCADA and unique OT computing and communications equipment are similar. Specifically, 49 CFR 191.3 defines what makes an "incident" and 49 CFR 191.15 states criteria for a written report, but no mentions of data records or timestamps are included. The timeframe for reporting events resolves only to the nearest hour. 18 CFR 284.12 talks about communication standards, but these are very general (intra-day and "within the hour" are mentioned). ISA/ANSI/IEC 62443-4-2 and TR62443-3-1 are related to cybersecurity, but as far as we can ascertain, there are not specific references to PNT associated with these requirements. We believe that utilities make use of timing associated with NTP and likely some use of GPS receivers associated with field equipment, but we judge that the operational impacts if this is disrupted are manageable.

3.2 Practical PNT Protection in the Energy Sector

While the previous section outlined standards associated with PNT, and timing specifically, in the Energy Sector, this section will examine current practices in the industry to ensure precise and accurate time is available. Many of these techniques deal with the precision clock source itself, whereas the standards mentioned were primarily dealing with the distribution of the accurate clock source. That is, most of these items deal with the precision clock source, not the distribution of the timing information as was the focus of the previously mentioned standards.

3.2.1 Firmware Management

Users of GNSS receiver clocks can secure their devices against evolving threats by updating device firmware frequently and securing the update process to prevent third-party access. Vendors typically support their timing products with updates to the internal software (firmware) that can prevent unintended operation or vulnerabilities present when the device was originally designed, procured, commissioned, and maintained. Some receiver clocks have had trouble with faulty leap-second implementations and interpretation of GPS system flags in the past. Such errors can be fixed by vendor firmware upgrades, which should be applied when available.

The firmware update process and resources should be strictly secured when not in use by the personnel responsible to prevent unintentional and/or malicious access. Users of GNSS receiver clocks should be familiar with any available security options for their clocks. Possible options may include setting a geographic position lock or precluding position or time jumps.

3.2.2 Multiple Local Redundant Time Sources

Electrical substations, remote ONG sites, and other self-contained environments requiring a reliable time source may consider using multiple GNSS time sources. Redundant pairs of GNSS receiver clocks with physically separated antennas can provide resilience against natural loss of signal and single-time source failure. Such a system may detect simple GNSS spoofs, but it cannot determine which of the two clocks is no longer genuine without additional software or hardware.

3.2.3 Resilient GNSS Antennas

Users of GNSS receiver clocks may consider operating with GNSS antennas that preclude signal reception below shallow elevation angles (<20°) to make simple ground-based spoofs more difficult, preclude use of satellites with long atmospheric dispersion paths, reduce multipath interference in urban environments, and eliminate many nuisance GNSS signal interferences.

3.2.4 Multi-Band GNSS Time Sources

GPS and other GNSS use multiple frequency bands to propagate their respective PNT information from orbiting satellites to Earth-based receivers. A typical GNSS receiver clock in use in the U.S. Energy Sector today receives only the GPS L1 frequency (1575.42 MHz).

Modern GPS receiver clocks are dual-band capable and can receive both the L1 and L2 (1227.0 MHz) GPS frequency bands, which carry identical information. Dual-band receiver clocks can provide added resilience against simple single-band spoofing. These clocks also enable more precise PNT resolution due to a direct measurement of atmospheric dispersion rather than an estimation.

3.2.5 Multi-Constellation GNSS Time Sources

Modern GNSS clocks can receive and decode two or more GNSS constellations (i.e., GPS, BeiDou, GLONASS, Galileo) simultaneously. Multi-constellation time sources can add resilience during natural events like solar storms or man-made events like constellation abnormalities. This capability can also offer added resilience against targeted single-GNSS spoofs and jams. Users of GNSS receiver clocks may consider using multiple GNSS constellations if their clocks can receive them. However, sophisticated attacks could defeat this protection.

3.2.6 Backup Off-Site Time Source

If networking infrastructure to a remote site is in place, use of off-site, high-precision backup timing sources should be considered to offer considerable resilience against any local GNSS intrusions. IEEE-1588 Precision Timing Protocol is an ideal candidate for this.

4.0 [Detect] Threats and Consequences

Many devices and functionalities in the Energy Sector rely on synchronized and precise time. Detection of loss or manipulation of PNT that is typically used to provide synchronized precise time is key in understanding potential impacts to those devices and functionalities. Detecting any loss or manipulation to PNT and reporting it to appropriate personnel in real time is essential to maintaining reliable and trusted operations.

4.1 Detecting Timing Attacks

For most current applications, PNT is used as a source in providing synchronized time at almost any geographic location. When operating a system that relies on quality time, it is important to understand the health of the devices that are supplying time to devices. It is also important to understand the impact of potentially operating with degraded or loss of time.

4.1.1 Time Distribution Mediums

As mentioned in Section 3.1, various standards define transport methods for distributing time and standards for communication protocols define requirements for the quality of time that is needed. There are basically three mediums for which time is distributed: 1) wirelessly (e.g., GNSS), 2) network based (e.g., IEEE 1588, NTP, etc.), and 3) serially (e.g., IRIG). Each of these has its own inherent weaknesses and would require different methods to detect attacks or abnormalities in the timing signal transported across them.

In time distribution systems, both wireless and network-based transport methods are more susceptible to attacks than serial-based systems. This is due to the nature of the serial links (either point-to-point or limited interconnected devices). For this reason, it is significantly less likely that a serial-based time signal will be attacked directly but would be more indirectly attacked from either the device generating the signal, or the location of time provided upstream of the serial signal (e.g., GNSS).

4.1.2 GNSS Attacks

GNSS attacks can either create a loss of signal (e.g., jamming or interference[22]) or a falsification of the signal (e.g., spoofing or meaconing). GNSS is a relatively weak broadcast signal and is transmitted unencrypted for the civilian market. This means that the signals are not authenticated or protected. As mentioned in Section 3.2, there are multi-band GNSS signals and different GNSS constellations. While not impossible, the complexity of generating an attack that covers multiple bands or constellations is improbable.

Various techniques and technologies can assist with the detection of GNSS attacks. GNSS firewalls or wireless intrusion detection systems (IDS) would be capable of detecting attacks. By using different mathematical algorithms, multiple GNSS bands, and more than one GNSS constellation, many attacks can be detected and protected against. An added benefit to some of these technologies is that they can be applied to existing infrastructure and add potential operational functionality (i.e., a GNSS firewall can have access to multiple bands and

[22] Interference may include atmospheric disruption or signals from other systems that may adversely affect your organization’s ability to use GNSS. Refer to Section 5.0 of this document regarding planning and response plans.

constellations, but generate and output only the L1 band for an older GNSS clock, thereby adding access to a greater number of broadcast time sources).

Some of the features that can be found in a GNSS firewall can be found in newer GNSS receivers. Each vendor's implementation to detect jamming or spoofing of GNSS signals may be different and can include proprietary algorithms. These security features may be an option and not available by default.

Some common methods for the detection of GNSS jamming and spoofing are:[23],[24]

- Amplitude discrimination – Monitoring the received signal through input power analysis via the automatic gain control of the receiver can be an identifier of anomalous GNSS signal transmission.
- Structural content power analysis – By taking advantage of the cyclo-stationary GNSS signals, these signals can be filtered, delayed, and compared to remove the Doppler effect and produce a line spectrum. Using appropriately designed comb filters, detection of anomalous GNSS signals can be determined using statistical analysis and comparison to thresholds.
- Time of arrival discrimination – GNSS signals from different satellites will have different time of arrival, but signals generated by a simulator or spoof will likely have the same time of flight as the source is singular and the distance to the receiver is the same. Monitoring the variable bias of the clock bias estimates can identify relative motion between the source and receiver to identify potential spoofed signals (single source).
- Effective carrier-to-noise ratio (C/N0) – Not to be confused with signal-to-noise ratio, C/N0 is the ratio of the carrier power to the noise power in per-unit bandwidth (dB-Hz). An abnormally high C/N0 can be an indication of a spoofing attack. It should be noted that jamming signals can artificially raise the noise floor.

  Monitoring C/N0 is a common feature of many commercially available GNSS receivers.
- Signal Quality Monitoring (SQM) – If authentic and spoofed signals overlap, then the interaction between them can create distortion in the shape of the correlation peak. Monitoring for any asymmetric, abnormally sharp, or elevated correlation peaks can be an indication of overlapping spoofing signals.
- Using the diversity of multi-band and multi-constellation signals – Generating spoofed signals for multi-band and/or multi-constellation is significantly more difficult than a single band (e.g., GPS L1). Taking advantage of additional sources of PNT signals allows for increased correlation between various and diverse data/signal sets.

  The availability of multi-band and multi-constellation capabilities is relatively common in commercially available GNSS receivers/antennas; however, it is likely an optional add-on and not a default feature.
- Direction of attack or angle of arrival – GNSS signals are broadcast from multiple locations across the sky, but spoofed signals tend to originate from near the horizon (ground based).

[23] https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf, Date Accessed: 13 Nov. 2020

[24] https://insidegnss.com/nobodys-fool-spoofing-detection-in-a-high-precision-receiver/, Date Accessed: 13 Nov. 2020

If the angle of arrival of GNSS signals all originate from a single angle or direction, this could indicate a spoofing attack.

- Cryptographic authentication – Common for military applications, authentication and encryption of GNSS signals can assist with protecting the authentic signals. Civilian receivers typically do not have access to these signals and rely solely on the unauthenticated and unencrypted signals. One potential fault with cryptographic signals is that they can still be susceptible to meaconing (replay) attacks if performed within the same key period (i.e., the attack only works if played back during a time the same cryptographic keys are used but will not have an effect after the keys have been changed).

Some GNSS detection tools and techniques are not readily available and may be emerging technology. Initial testing of detection algorithms combined with the latest GNSS technology (e.g., hardware that natively supports multi-band and multi-constellation) has shown great promise in detecting and even preventing attacks on GNSS receivers.[25]

4.1.3 Network-Based Time Attacks

Network-based time attacks can consist of packet injection, man in the middle (MitM), packet loss, denial of service (DOS), addition of rogue time sources, etc. These attacks are the same as those for network-based attacks not centered on time distribution. Many IT solutions are developed specifically for network-based attacks and can be used similarly to detect attacks on time via the network. Intrusion detection systems (IDS), software-defined networking (SDN), intrusion prevention systems (IPS), and various other sensors attached to a network can identify and alert on suspected malicious network activity.

As mentioned in Section 3.1.1, Annex K and P of the IEEE 1588 standard and RFC 7384 define mechanisms to protect time distribution and also methods to potentially detect some attack scenarios. Where these mechanisms exist, they should be used to assist with detection of timing attacks.

Outside of the mechanisms established by the standards themselves for signal protection, all other forms of network-based attacks are considered part of network communications or IT infrastructure and are not within the scope of this document.

4.1.4 Redundant Time Sources

Detection of PNT loss or degradation can be achieved through coordination of redundant time sources. Using diversity in the type of time source could also increase the likelihood of detection. For example, having one time source rely on GNSS signals while another uses network-based signals like IEEE 1588 could help (especially when the time sources are not geographically collocated). Other sources may include eLORAN[26] (enhanced Long-Range Navigation), precision internal oscillators, or potentially cellular signals.

[25] https://insidegnss.com/nobodys-fool-spoofing-detection-in-a-high-precision-receiver/, Date Accessed: 13 Nov. 2020

[26] https://rntfnd.org/wp-content/uploads/eLoran-Definition-Document-0-1-Released.pdf, Date Accessed: 13 Nov. 2020

4.1.5 Hardware/Software Attacks

Attacks on devices, either to the hardware or to software/firmware, can be difficult to detect. For traditional IT-based systems, software tools can be installed on devices to detect, protect, and recover from attacks. For devices typically used for energy delivery systems, that is not always possible and detection, if possible, likely happens as part of the supply chain or maintenance cycle. Some portions of energy-delivery systems are hosted on more traditional operating systems (e.g., Microsoft Windows or Linux); however, there are some sensitives to running traditional IT cybersecurity software as any impact to the system's performance could be detrimental.

Some devices can support change management or can have it supported externally via additional devices. In a geographical location with devices on a local area network, a singular device may monitor device configuration and potentially even the version and integrity of the firmware. When such capabilities exist, it is possible to detect tampering of device configuration or software/firmware changes.

When procuring, commissioning, or performing maintenance on equipment, checks can be performed to verify and validate the configuration and version of software/firmware installed. Some vendors have utilities that assist in verifying software/firmware authenticity and determining if it has been tampered with (e.g., signed firmware, hashes, etc.). When available, attacks on the device can be detected during the procurement, commissioning, and maintenance cycles.

4.2 Reporting of Detected Attacks

Part of the detection process is reporting to and alerting personnel of the detection. Providing this awareness allows personnel to respond and take action if necessary. The detection data/signal needs to traverse the network to reach the central control center where personnel are staffed. IT-based solutions already exist for this that can be and are being leveraged in energy-delivery system environments to report information about the systems' operation and events. Additionally, reporting potential attacks to the relevant Information Sharing and Analysis Centers (ISACs) will enable more effective cross-sector awareness of systemic issues.

The NERC Electricity Information Sharing and Analysis Center (E-ISAC) gathers and analyzes security data and shares appropriate data with stakeholders. The E-ISAC, in collaboration with DOE and the Energy Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electric industry and enhances industry's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents[27]. The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE and industry and managed by the E-ISAC, providing bi-directional cyber-risk information sharing[28].

Utilities that are stakeholders in the E-ISAC can share data, receive aggregated analysis, and implement the best practices provided to help mitigate, respond, and recover quickly.

[27] https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx

[28] https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity

Electric utilities are required to submit DOE OE-417 forms (Electric Emergency Incident and Disturbance Report) with information on electric incidents and emergencies, including those related to PNT. DOE uses this information to fulfill its overall national security and other energy emergency management responsibilities, as well as for analytical purposes.

GPS-specific reporting can be made to GPS.gov website, the official U.S. government site for GPS and related topics[29]. The U.S. Coast Guard Navigation Center (NAVCEN) is the designated point of contact for providing operational GPS user support to the civilian community and provides operational status of GPS satellites.[30] This site is a useful resource for users to determine any GPS issues, testing, or outages.

Some systems, like GNSS receivers, may not be connected to the network and only be connected serially (e.g., IRIG) to the devices that need time. This would inhibit the GNSS receiver from providing any status via the network to the personnel that could use it. If the GNSS receiver can be connected to a network (most are as they also supply NTP), then it possibly can provide status or potentially be monitored by another device that can report status. While connecting any device to a network provides benefits, it also increases the attack surface, so this connection needs to be thought out and implemented wisely.

Some protocols (e.g., IRIG, IEEE 1588, and C37.118) define the use of quality flags for the signal. These should be appropriately used and could be an indicator of potential PNT loss or degradation.

4.2.1 Syslog and Simple Network Management Protocol

Many devices support reporting status and events via system logs (syslog[31]) or Simple Network Management Protocol (SNMP[32]). Using these mechanisms provides a way to gain situational awareness of the devices that make up a system. When an event is detected that affects PNT, it can be reported using one of these protocols to alert personnel of the situation.

Not all devices support system logs or SNMP, but other devices on the same network or connected to them may. If possible, these devices can communicate with each other (either via standard or proprietary means) and provide system logs or SNMP capability for the entire location instead of each device reporting individually.

4.2.2 Security Information and Event Management

A Security Information and Event Management (SIEM) system is designed to collect, process, filter, and display information about all of the attached systems on a given network. Devices that support syslog or SNMP can generate data that is ingested by a SIEM system and therefore make it significantly easier for a user to obtain the desired information without having to sort through it all manually and potentially losing important information in a sea of day-to-day operational data.

Several SIEM solutions are available commercially and other similar solutions that provide similar functionality are also available. These solutions were initially designed for IT

[29] https://www.gps.gov/

[30] https://www.navcen.uscg.gov/

[31] https://tools.ietf.org/html/rfc5424, Date Accessed: 13 Nov. 2020

[32] https://tools.ietf.org/html/rfc3410, Date Accessed: 13 Nov. 2020

infrastructure but are increasingly being adapted to OT infrastructure, including energy-delivery systems. Using a SIEM or similar tool allows for copious amounts of system data to be processed via automation and presents users with meaningful and real-time information to aid in responding to a detection of loss or degradation of PNT.

5.0 [Respond & Recover] Mitigations

The general PNT profile in NISTIR 8323 is applicable to the Energy Sector with few changes and should be followed as such for the respond and recover functions. The technical aspects of responding to and recovering from PNT service interruptions are largely automated without need for human intervention, including notifications to downstream users and applications.

5.1 Response Plan

Response processes and procedures are executed and maintained to ensure response to detected cybersecurity incidents in accordance with pre-defined thresholds. A response plan should include:

- Assignment roles and responsibilities[33]
- Categories of incidents with graded approach based on PNT application needs
- PNT resilience level requirements based on application criticality and impact
- Any internal and external stakeholders and applicable organizational sharing policies. For example, determining the overall status of the GPS constellation could be an important first step in addressing disruptions.[34]

5.2 Communications

Ensure that detected cybersecurity events on the PNT system are reported consistent with the incident categories in the response plan. Suspected intentional interference should be reported to the appropriate channels.

Share cybersecurity incident information with relevant stakeholders as defined in the organizational sharing policies.

5.3 Analysis

Investigate any cybersecurity-related notifications generated from PNT anomaly detection systems or protocol-generated flags. Ensure logs and records are preserved.

Understand the full implication of a cybersecurity incident and consider the organizational impact on PNT services that may affect PNT-dependent downstream applications, users, and systems—i.e., protection logic, fault recorders, timestamping, and phasor measurement. Conduct forensic analysis on collected cybersecurity event information to determine the root cause of PNT disruption or manipulation.

Categorize cybersecurity incidents according to the level of severity, impact, and user/application affected, consistent with the response plan.

[33] 2020 FERC, NERC and REs Report, "Cyber Planning for Response and Recovery Study (CYPRES)" https://cms.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf Date Accessed: 20 Feb. 2021

[34] GPS service outages and status reports can be found at https://www.gps.gov/support/user/#civilian Date Accessed: 15 Dec. 2020

5.4 Mitigation

Contain cybersecurity incidents to minimize impact on the PNT system and consider that PNT systems can revert to a known good state and should be monitored for status flags to confirm reversal to a known good state.

Given successful containment measures, implement PNT-based mitigation measures that can include alternate sources to operate through the incident. High-precision holdover oscillators or backed-up offsite network-based PNT services can allow PNT users and applications to operate for some time without their primary PNT source. Apply available patches/upgrades/updates to applicable devices to mitigate the vulnerability or incident.

6.0 Summary

While the Energy Sector as a whole and the electric power grid specifically have a growing dependence on precise time, the basic functionality of the grid itself does not rely on precise time to operate. The disruption of PNT services would not prevent today's grid from operating efficiently and reliably. The grid will continue to function, albeit with the possibility of confusion and corrupted data logs, regardless of the accuracy of the various time references that are being used today. And while some utilities are making use of precision time for advanced measurements and protection applications, the engineering rigor associated with these implementations should ameliorate the reliability concerns associated with disruptions to their timing sources.

Sophisticated technical solutions exist today to cover PNT cybersecurity needs in the Energy Sector, complemented by mature industry standards and operating practices. PNT users in the Energy Sector should have well-prepared response and recovery plans in place. Plans and PNT technology should be updated periodically to ensure continued resilience against evolving threats and to incorporate lessons learned.

Specifically, as they related to dependency on precision time associated with critical applications, we recommend that PNT plans be developed and tested as part of the utility's regular continuity of operations tests in the form of tabletop exercises and testing activities.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov