Pacific Northwest
NATIONAL LABORATORY

PNNL-30780 Rev1

Energy Sector Position, Navigation, and Time Profile

Revision 1

September 2024

Carol Larvick
Scott Mix
Rich Mooney
Lori Ross O'Neil

U.S. DEPARTMENT OF ENERGY

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
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

Energy Sector Position, Navigation, and Time Profile

Revision 1

September 2024

Carol Larvick
Scott Mix
Rich Mooney
Lori Ross O'Neil

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Revisions

Rev. #	Rev. Date	Reason	Revision Changes
0	03/2021	N/A	Initial release
1	09/2024		Aligned with NIST IR 8323

Summary

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 (DOE). DOE 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 and Technology (NIST) to develop a PNT profile that is broadly applicable to all sectors and to serve as a foundation for sector-neutral guidance, NIST Internal/Interagency Report (NIST IR) 8323 *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*. This document builds on NIST IR 8323r1 to serve as specific guidance for the energy sector.

For purposes of this PNT Profile, energy sector time is between 0.5 µs (microseconds) and 1 µs precision and accuracy. Currently, the electricity subsector has systems that use this level of precision time, but the oil and natural gas subsector 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] E.O. 13905. 2020. Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. Federal Register. Accessed Dec. 15, 2020, at https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing.

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. The accuracy of the information and the perspectives presented in this report are the responsibility of the authors.

Acronyms and Abbreviations

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
DOE	Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
eLORAN	enhanced long-range navigation
GNSS	Global Navigation Satellite System
GOOSE	Generic Object-Oriented Substation Event (IEC 61850)
GPS	Global Positioning System – the U.S. implementation of GNSSIDS Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Protection System
IRIG	Inter-Range Instrument Group
IRIG-B	Inter-Range Instrument Group B variant
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
IT	information technology
ITU	International Telecommunications Union
LAN	local area network
LEO	Low Earth Orbit
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NIST-CSF	National Institute of Standards and Technology Cybersecurity Framework
NIST IR	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
PNT	positioning, navigation, and timing
PPS	pulse per second
PTP	Precision Time Protocol
SCADA	supervisory control and data acquisition

SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SQM	Signal Quality Monitoring
SRMA	Sector Risk Management Agency
SSA	Sector-Specific Agency
syslog	system log
TVE	Total Vector Error
UTC	Coordinated Universal Time
WAN	wide area network

Contents

Summary i
Acknowledgments ii
Acronyms and Abbreviations iii
1.0 Introduction 1
1.1 Purpose and Scope 1
1.2 Audience and Intended Use 2
2.0 [Identify] Current PNT Landscape in the Energy Sector 4
2.1 PNT Service Use and PNT-Reliant Devices 4
2.1.1 Control Room Operations 6
2.1.2 Broad Use of PNT-Dependent Applications 6
2.1.3 Multiple PNT Distribution Technologies May Be Present 8
2.1.4 Timing in Electric Utility Telecommunications Systems 9
2.2 Impacts and Consequences of Disrupted or Manipulated PNT Services 10
2.2.1 Governance in the NIST PNT Profile Versions 11
3.0 [Protect] Current Protection Landscape 12
3.1 PNT-Related Standards in Energy Sector 12
3.1.1 Precision Time Protocol (IEEE 1588-2019) 12
3.1.2 Time Tagging for Intelligent Electronic Devices (IEEE C37.237-2018) 13
3.1.3 Inter-range Instrument Group Timecode 13
3.1.4 Network Time Protocol 14
3.1.5 Substation Automation (IEEE/IEC 61850-9-3:2016 and IEEE C37.238-2017) 14
3.1.6 Synchrophasors (IEC/IEEE 60255-118-1:2018, formerly IEEE C37.118.1) 15
3.1.7 Time Synchronization System Network Design (IEEE 2030.101-2018) 15
3.1.8 Data Transport/Aggregation Standards 15
3.1.9 Disturbance Measurement Requirements (NERC PRC-002-2) 16
3.1.10 Oil and Natural Gas Sequence of Events Records 17
3.2 Practical PNT Protection in the Energy Sector 17
3.2.1 Firmware Management 17
3.2.2 Multiple Local Redundant Time Sources 18
3.2.3 Resilient GNSS Antennas 18
3.2.4 Multi-Band GNSS Time Sources 18
3.2.5 Multi-Constellation GNSS Time Sources 18
3.2.6 Backup Off-Site Time Source 19
4.0 [Detect] Threats and Consequences 20

4.1 Detecting Timing Attacks 20
4.1.1 Time Distribution Mediums 20
4.1.2 GNSS Attacks 20
4.1.3 Network-Based Time Attacks 22
4.1.4 Redundant Time Sources 22
4.1.5 Hardware/Software Attacks 23
5.0 [Respond] Responding to Detected Attacks 24
5.1 Reporting of Detected Attacks 24
5.1.1 Syslog and Simple Network Management Protocol 25
5.1.2 Security Information and Event Management 25
5.2 Analysis of Detected Event 26
5.3 Mitigation Measures 26
6.0 [Recover] Recovery Actions 27
6.1 Response and Recovery Plans 27
6.2 Communications 27
7.0 Summary 28
Appendix A – Considerations for Customizing Sector-Specific PNT Profiles for an Individual Organization A.1

Figures

Figure 1. Notional PNT Service Locations within a Utility 5

Tables

Table 1. PNT-Dependent Applications and Effects of PNT Loss 7
Table 2. Performance of PNT Distribution Technologies 9

1.0 Introduction

The electric power grid has a growing dependence on accurate and precise time coordinated to Coordinated Universal Time (UTC). 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 global navigation satellite systems (GNSSs), such as the U.S. global positioning system (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 GNSS 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 5 ms to 100 ms.[2] Energy timing functions that can be met using precise time in this range should consider using Network Time Protocol (NTP), which can get its time from internet-based sources.

1.1 Purpose and Scope

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 Internal/Interagency Report (NIST IR), 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 positioning, navigation, and timing (PNT) resources. NIST IR 8323 is based on the NIST Cybersecurity Framework (NIST-CSF) version 1.0 and 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 Sector Risk Management Agency (SRMA) (formerly known as a Sector-Specific Agency -SSA) is expected to develop its own sector-specific PNT profile that builds on NIST IR 8323.

To support the protection of the energy sector's dependency on PNT, Pacific Northwest National Laboratory (PNNL) developed an energy-sector-focused PNT profile (known hereafter

---

[2] NTP. "Section 5: How does it work?" The NTP FAQ and HOWTO. Network Time Protocol. Accessed March 27, 2021, at http://www.ntp.org/ntpfaq/NTP-s-algo.htm

[3] E.O. 13905. 2020. Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. Federal Register. Accessed Nov. 6, 2020, at https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing.

[4] NIST IR 8323. 2021. Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. National Institute of Standards and Technology. Accessed Feb. 20, 2021, at https://csrc.nist.gov/publications/detail/nistir/8323/final

as PNT profile) at the request of the U.S. Department of Energy (DOE). DOE is the energy sector's SRMA responsible for providing guidance 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 U.S. national critical infrastructure.

Because the energy sector's dependence on GNSS for positioning and navigation for applications, such as unmanned aerial systems and field crew tracking, is similar to other sectors (primarily transportation), this document will focus on time. More specifically, it considers 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 NTP. In evaluating precise 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 high-precision timing requirements (more precise than provided by 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 SRMA 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 January 2023, NIST published revision 1 of NIST IR 8323,[5] superseding the original version and based on NIST-CSF version 1.1. NIST then released version 2.0 of NIST-CSF in February 2023. At the time this document was updated, NIST had not provided a schedule for revisions to NIST IR 8323 to address the updated NIST-CSF. This document, the *Energy Sector Position, Navigation, and Time Profile,* has been updated in alignment with the NIST IR 8323, Rev. 1 document and with additional information and adjustments that have emerged since it was issued in March 2021.

In addition to NIST IR 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.

1.2 Audience and Intended Use

This PNT profile is intended to be a building block for energy sector organizations to develop their own PNT profiles, building upon NIST IR 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. Appendix A includes a list of questions from the NIST IR 8323 Rev. 1 that can be used to tailor this sector PNT document to an individual organization within the energy sector. 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

[5] NIST IR 8323r1. 2023. Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. National Institute of Standards and Technology. Accessed March 22, 2024, at https://doi.org/10.6028/NIST.IR.8323r1.

time, is often 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-CSF 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. The specific CSF sections referenced in this document are identified in the section title in brackets.

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 processes 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 monitoring is in minutes, not milliseconds or microseconds. Therefore, the remainder of this section is primarily focused on the electricity subsector.

2.1 PNT Service Use and PNT-Reliant Devices

Some applications, while not yet in widespread use, require GNSS-enabled precision time to support advanced protective relaying applications. The accuracy required for these devices can be in the 100 ns 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 GNSS 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 and misoperations).

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 GNSS, which includes GPS and Galileo in Europe, as well as Low Earth Orbit (LEO) satellites, such as Iridium.[6] Note that there are security concerns associated with certain foreign-owned and -operated GNSS services, making systems owned and operated by close allies of the United States more attractive, regardless of what satellite constellation(s) the receiver is capable of using as a time source.

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.

[6] Note: Other countries have implemented GNSS, but their use in the U.S. is restricted (see https://www.gps.gov/spectrum/foreign/, accessed Aug. 16, 2024).

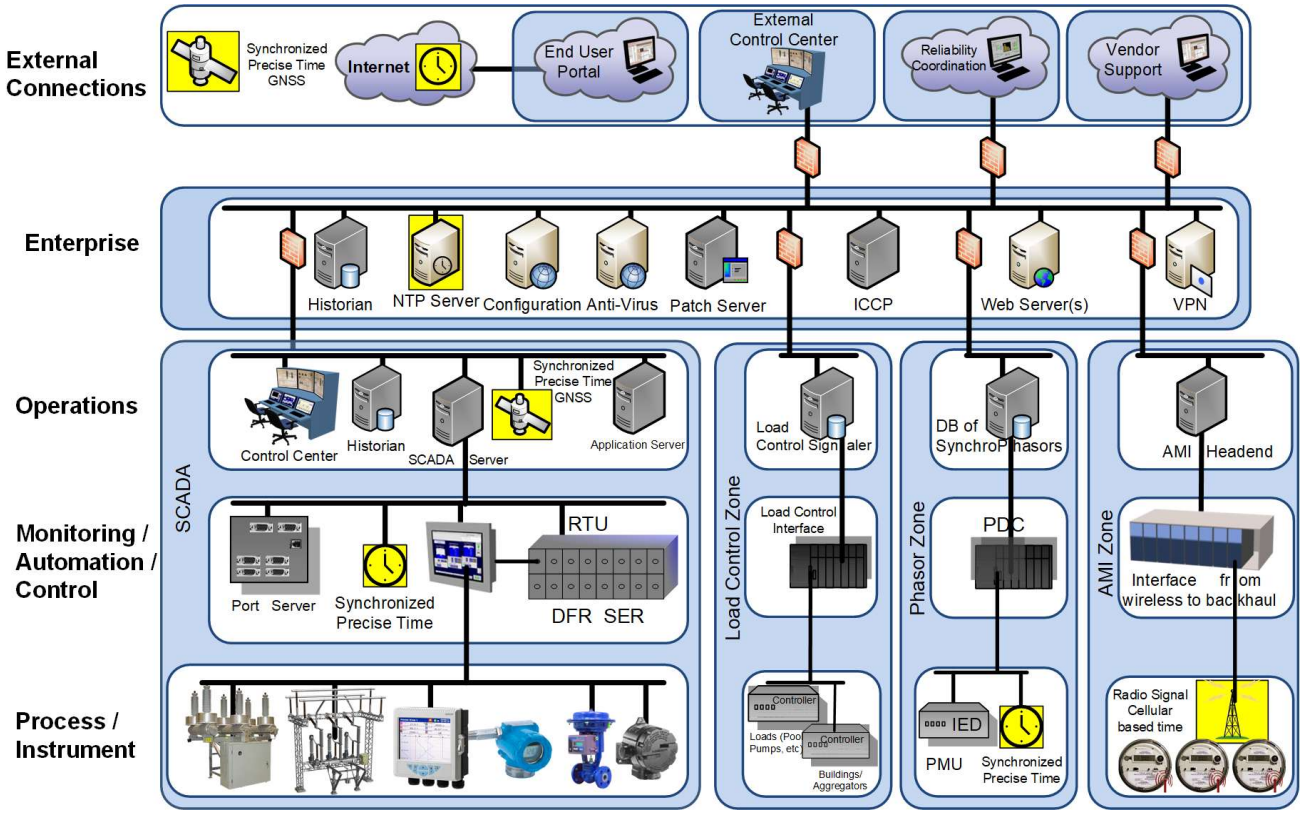


Figure 1. Notional PNT Service Locations within a Utility

Individual utilities should inventory their applications that require the use of time, as well as their time sources, to determine the time-based characteristics required by applications and to determine whether appropriate time sources have been implemented. For applications and end-use equipment, this information should include, at a minimum, the following:

- Time accuracy requirements
- Time precision requirements
- Time resolution requirements
- Acceptable timing tolerances
- Time signal input capabilities
  - 1 pulse per second (PPS)
  - NTP/Simple Network Time Protocol (SNTP)
  - Precision Time Protocol (PTP) (IEEE 1588)
  - Inter-Range Instrument Group B variant (IRIG-B)
- Backup/alternate time source capabilities.

For time sources (e.g., GNSS receivers), the information should include, at a minimum, the following:

- Time input source (e.g., local GNSS receiver, internet)
- Time output accuracy
- Time output precision
- Time output resolution
- Time output tolerances (jitter, latency, etc.)
- Time output format
  - 1PPS
  - NTP/SNTP
  - PTP (IEEE 1588)
  - IRIG-B
- Holdover characteristics
- Input source resilience (e.g., backup primary time sources).

2.1.1 Control Room Operations

The loss of GNSS 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 100 ms is necessary to support most control room applications. Disturbance monitoring has a UTC ± 2 ms requirement.[7] 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, some PMUs may be determined to be Bulk Electric System (BES) Cyber Systems (depending on how these measurements are used in operational applications), and, therefore, they come under the purview of the NERC Critical Infrastructure Protection (CIP) requirements.

2.1.2 Broad Use of PNT-Dependent Applications

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

[7] PRC-002-2. N.d. Disturbance Monitoring and Reporting Requirements. North American Electric Reliability Corporation. Accessed Nov. 6, 2020, at https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-002-2.pdf.

Table 1. PNT-Dependent Applications and Effects of PNT Loss

Application	Application Overview		PNT Disruption	
	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 whether 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 manipulate the PNT service, misaligning shared data. This could result in an indication of a false condition of the transmission line and lead to opening the line when not needed (misoperation) or not allowing it to open when actually needed (failure to operate).
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 and destabilize the grid.
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.

Application	Application Overview		PNT Disruption	
	Purpose	PNT Use	Impact	Consequence
Sequence of Events Recorder (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.
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. UTC time is needed for coordination between substations.	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. Accurate time is also needed to coordinate actions across more than one physical location (substation).
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 line.	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.

2.1.3 Multiple PNT Distribution Technologies May Be Present

Table 2 includes examples of the technologies that may be employed within an electric utility to distribute precise time or precise timing to various applications. Depending on the application, the accuracy required from PNT sources, and the physical distance between locations, multiple technologies may be used to achieve full synchronization or time tagging at multiple locations. It is important to understand and document the technologies used for each application when determining the performance required and the potential impacts if the technology is unavailable or manipulated.

Table 2. Performance of PNT Distribution Technologies

Technology	Technology Overview		Performance	
	Purpose	PNT Use	Accuracy	Time-of-Day?
Network Time Protocol (NTP)	NTP is a network-based protocol designed to synchronize the clocks of systems over a network.	NTP often relies on GNSS signals to synchronize the network onto the primary clock. NTP can also use internet-based time sources with less accuracy but fewer equipment requirements.	5–100 ms	Yes
Precision Time Protocol (PTP)-LAN	Similar to NTP, the PTP is a network-based time synchronization protocol capable of greater precision of time synchronization than NTP. It is specified by IEEE Standards 1588 and C37.238.	PTP provides time synchronization between network nodes; often, the grand master clock is synchronized by a GNSS signal or other known precise and accurate time source.	< 1 µs	Yes
PTP-WAN	PTP-WAN allows PTP network messages to be accurately transferred across a WAN to provide a precise time source at multiple locations. It is specified by IEEE Standard 1588.	PTP provides time synchronization between network nodes; often, the grand master clock is synchronized by a GNSS signal or other known precise and accurate time source.	Varies by implementation	Yes
IRIG-B	The most common of 6 standard IRIG time code formats for a one-way digital time signal used in the electric power industry for providing precise time-of-day and time of year to grid devices. IRIG-B is specified within IRIG Standard 200-4.	IRIG-B is often derived from a GNSS signal and used for precise time tagging of system events in relays, PMUs, and other devices.	< 100 ns	Yes
1 PPS	The 1 PPS signal is used as a reference clocking signal to synchronize clocks in a communications system or other network.	The 1 PPS signal is available via GNSS or supplied by a signal generator.	50 µs	No

2.1.4 Timing in Electric Utility Telecommunications Systems

For utilities that own, operate, and maintain internal telecommunications systems, it is common to use a timing system, often linked to a GNSS signal or atomic clocks (such as cesium or rubidium), for synchronizing the nodes at each location in the system. Although time-of-day is not required, lack of precise timing can cause errors in the data being transported. For utilities that use at least some third-party providers for their telecommunications, their grid services

using the telecommunications provided will have dependencies on that provider's timing systems.

The impact of a loss of PNT services and time synchronization in electric utility telecommunications 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.

2.2 Impacts and Consequences of Disrupted or Manipulated PNT Services

Identifying the exact impact and consequences of disrupted or manipulated PNT services is difficult because of 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 short 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 GNSS 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, for applications that currently are widely deployed, we assess that the loss or disruption of GNSS would affect PMUs the most, as they require the highest timing accuracies (microsecond range). Most PMUs receive their time synchronization using GNSS clock receivers. If GNSS synchronization is lost, then they can rely on internal clocks for a short period of time. If the GNSS 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 WANs.

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 accurate and 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 systems are degraded, thus degrading the power system itself.

For utility telecommunications systems, the impact of a loss or disruption of the timing source can be more subtle. Normally, telecommunications equipment will have internal clocks that can provide holdover timing. At some point, the holdover timing signal will drift and eventually cause errors in the data being carried, often on multiple services and multiple locations at nearly the same time. Having centralized monitoring and alarming on the telecommunications timing source(s) can help manage this scenario.

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.

2.2.1 Governance in the NIST PNT Profile Versions

Governance appears as part of both the original NISTIR 8323 document and the updated version, NISTIR 8323r1, as part of the “Identify” section, in both cases citing one subcategory as applying to the PNT profile: GV-4: Governance and risk management processes address cybersecurity risks. It is worth noting that there are no applicable updates or revisions to this section that impact the U.S. energy sector. Additional references have been added to reflect changes in critical infrastructure outside of the U.S. energy sector (e.g., E911 and foreign GNSS); however, they do not apply for purposes of this document.

This does serve as a reminder to be aware of any replacements or upgrades of legacy equipment that did not depend on PNT services in the past that now have a requirement for a PNT connection. These devices must be identified and enrolled in the governance program.

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 whether 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,[8] also known as PTP. 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 and allows a process for customization by specifying parameter settings and performance specifications in documented profiles. The IEEE 1588 Power Profile (IEEE C37.238-2017 with IEEE/IEC 61850-9-3:2016; see Section 3.1.5) defines the PTP profile for use in power systems.

The standard also includes 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

[8] IEEE. 2020. 1588-2019 – IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. Institute of Electrical and Electronics Engineers. Accessed Nov. 6, 2020, at https://ieeexplore.ieee.org/document/9120376.

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.

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[9] 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[10] (COMTAG) 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 IRIG-B (covered next).

3.1.3 Inter-range Instrument Group Timecode

The IRIG Timecode is a standard for serial time communications provided by the Range Commanders Council Telecommunications and Timing Group. The B variant (IRIG-B) of IRIG Standard 200-16[11] (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.

---

[9] IETF. 2014. Request for Comments: 7384. Internet Engineering Task Force. Accessed Nov. 11, 2020, at https://tools.ietf.org/html/rfc7384.

[10] IEEE. 2019. C37.237-2018 – IEEE Standard for Requirements for Time Tags Created by Intelligent Electronic Devices—COMTAG. Institute of Electrical and Electronics Engineers. Accessed Nov. 16, 2020, at https://ieeexplore.ieee.org/document/8604153.

[11] Timing Committee of the Telecommunications and Timing Group. 2016. IRIG Serial Time Code Formats. U.S. Army Range Commanders Council. Accessed Sept. 17, 2024, at https://www.trmc.osd.mil/wiki/download/attachments/113019842/200-16_IRIG_Serial_Time_Code_Formats.pdf?version=1&modificationDate=1623181164717&api=v2.

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, Annex A, 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.

3.1.4 Network Time Protocol

NTP[12] 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 theoretically 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 resilience, accuracy, and precision than the base NTP standard. With these levels of timing accuracy, NTP has been historically used in SCADA-based sequence of events applications but is no longer 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 Electrotechnical Commission (IEC) 61850-9-3:2016[13] and IEEE C37.238-2017[14] 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 essentially different versions of the same standard. IEC 61850-9-3:2016 was an enhancement of the original IEEE C37.238-2011[15] standard, and now IEEE C37.238-2017 is

[12] NTP. “Welcome to the home of the Network Time Protocol (NTP) Project.” Network Time Protocol. Accessed Nov. 11, 2020, at http://www.ntp.org.
[13] IEEE. 2016. 61850-9-3-2016 – IEC/IEEE International Standard – Communication Networks and Systems for Power Utility Automation – Part 9-3: Precision Time Protocol Profile for Power Utility Automation. Institute of Electrical and Electronics Engineers. Accessed Nov. 6, 2020, at https://ieeexplore.ieee.org/document/7479438.
[14] IEEE. 2017. C37.238-2017 – IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications. Institute of Electrical and Electronics Engineers. Accessed Nov. 6, 2020, at https://ieeexplore.ieee.org/document/7953616.
[15] IEEE. 2011. C37.238-2011 – IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications. Institute of Electrical and Electronics Engineers. Accessed Nov. 6, 2020, at https://ieeexplore.ieee.org/document/5963699.

an enhancement of the IEEE/IEC 61850-9-3:2016 standard.[16] All points of discussion in this section relate to IEEE C37.238-2017 but may be valid for older versions of the standard.

IEEE 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, IEEE 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[17] is a joint IEC/IEEE standard that describes the measurement requirements and approach for PMUs. One aspect of the standard is a requirement that the total vector error (TVE) 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 accurate (±2.6 µs for a 60-Hz system) to ensure other contributors to measurement inaccuracy remain below the 1% 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 Time Synchronization System Network Design (IEEE 2030.101-2018)

As noted in its scope statement, the IEEE 2030.101 standard describes considerations that should be included when designing, installing, and monitoring time synchronization and distribution systems within in electric power substation. It includes time sources, such as GNSS, and time distribution systems, such as IRIG-B, NTP (or SNTP), and IEEE Std C37.238, plus IEC/IEEE 61850-9-3, which use PTP. This guide assumes that the time source (e.g., GNSS) and the intelligent electronic device (e.g., the protection relays) have accurate internal clocks.

3.1.8 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

[16] Work is underway (in 2024) to update IEEE/IEC 61850-9-3 to align it with IEEE 1588-2019 and other industry standards.

[17] IEEE. 2018. 60255-118-1-2018 – IEEE/IEC International Standard – Measuring Relays and Protection Equipment – Part 188-1: Synchrophasor for Power Systems – Measurements. Institute of Electrical and Electronics Engineers. Accessed Nov. 11, 2020, at https://ieeexplore.ieee.org/document/8577045.

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)[18]
- IEC 61850-6:2009 (GOOSE)[19]
- IEEE 1815-2012 (DNP3)[20]
- IEEE C37.118-2-2011 (PMU data)[21]
- IEEE C37.247-2019 (PDC standard)[22]
- IEC 60255-4:2013/IEEE C37.111-2013 (COMTRADE).[23]

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.

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

Unlike the previous standards described, the NERC PRC-002-2[24] standard is not a device or interoperability standard but a compliance standard. NERC PRC-002-2 puts requirements in

---

[18] IEC. 2020. IEC 61850-9-2 Consolidated Version: Communication Networks and Systems for Power Utility Automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled Values Over ISO/IEC 8802-3. International Electrotechnical Commission. Accessed Nov. 11, 2020, at https://webstore.iec.ch/publication/66549.

[19] IEC. 2018. IEC 61850-6 Consolidated Version: Communication Networks and Systems for Power Utility Automation – Part 6: Configuration Description Language for Communication in Power Utility Automation Systems Related to IEDs. International Electrotechnical Commission. Accessed Nov. 11, 2020, at https://webstore.iec.ch/publication/63319.

[20] IEEE. 2012. 1815-2012 – IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3). Institute of Electrical and Electronics Engineers. Accessed Nov. 11, 2020, at https://ieeexplore.ieee.org/document/6327578.

[21] IEEE. 2011. C37.118.2-2011 – IEEE Standard for Synchrophasor Data Transfer for Power Systems. Institute of Electrical and Electronics Engineers. Accessed Nov. 11, 2020, at https://ieeexplore.ieee.org/document/6111222.

[22] IEEE. 2019. C37.247-2019 – IEEE Standard for Phasor Data Concentrators for Power Systems. Institute of Electrical and Electronics Engineers. Accessed Nov. 11, 2020, at https://ieeexplore.ieee.org/document/8830511.

[23] IEEE. 2013. C37.111-2013 – IEEE/IEC Measuring Relays and Protection Equipment – Part 24: Common Format for Transient Data Exchange (COMTRADE) for Power Systems – Redline. Institute of Electrical and Electronics Engineers. Accessed Nov. 11, 2020, at https://ieeexplore.ieee.org/document/6654239.

[24] NERC. n.d. PRC-002-2 – Disturbance Monitoring and Reporting Requirements. North American Electric Reliability Corporation. Accessed Nov. 11, 2020, at https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-002-2.pdf.

place for disturbance monitoring and reporting on the bulk electric system. A significant part of the reporting aspect is that all required data must be timestamped to UTC with an accuracy of ±2 ms.

3.1.10 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, in the Code of Federal Regulations (CFR), 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 GNSS 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, after testing on a few devices to validate proper operation of grid functions post upgrade.

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.

Firmware updates can also be used to modify or add functionality to existing receivers. For example, a receiver that supports IEEE 1588 and that was procured and installed in 2017 cannot take advantage of any features of IEEE 1588 that were introduced in the 2019 version of the standard, but installing a firmware update may implement the new features. Similarly, if some features were considered optional, a manufacturer may have not implemented them, but a firmware update may enable them.

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 or other external 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.

Alternatively, augmenting a GNSS time source with a backup time source using a different technology, such as an LEO satellite or an enhanced long-range navigation (eLORAN) signal, may be able to overcome intentional jamming of the GNSS frequencies.

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 (referred to as horizon nulling configurations), preclude use of satellites with long atmospheric dispersion paths, reduce multipath interference in urban environments, and eliminate many nuisance GNSS signal interferences.

Some specialized resilient or "adaptive" GNSS antenna technology is export controlled. While this should not present a problem for most U.S.-based installations, careful review of export control regulations should be undertaken prior to implementing these solutions.

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 because of 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 (e.g., GPS, 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, and there are still security concerns, as noted in section 2.1.

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.

An example of this could be using IEEE 1588 configured using a telecommunications profile, such as the International Telecommunications Union (ITU) G.8275.1[25] or G.8275.2.[26] Note, however, that in order to use these profiles, the wide-area telecommunications network and its associated equipment must be appropriately configured and capable of properly processing IEEE 1588 messages. This approach still requires an accurate clock to be used as a primary time source, but this may be a GNSS clock receiver located at a central control center with a precise and accurate long-term backup or holdover oscillator (such as a cesium oscillator), which are available from many sources. Cesium oscillators are expensive and impractical to operate in substation or field environments but may be a prudent solution if installed at a centralized location for use by many field or substation locations.

[25] ITU. 2022. Precision Time Protocol Telecom Profile for Phase/Time Synchronization with Full Timing Support from the Network. International Telecommunications Union. Accessed June 27, 2024, at https://www.itu.int/rec/T-REC-G.8275.1/en.

[26] ITU. 2022. Precision Time Protocol Telecom Profile for Phase/Time Synchronization with Partial Timing Support from the Network. International Telecommunications Union. Accessed June 27, 2024, at https://www.itu.int/rec/T-REC-G.8275.2/en.

4.0 [Detect] Threats and Consequences

Many devices and functionalities in the energy sector rely on synchronized accurate and precise time. Detection of loss or manipulation of PNT that is typically used to provide this synchronized 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 PNT-dependent 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) serial dedicated cable (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 cable-based systems. This is due to the nature of the serial links (either point-to-point or limited interconnected devices) and often behind a physical security perimeter. 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[27]) 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

[27] Interference may include atmospheric disruption, solar interference, or signals from other systems that may adversely affect your organization's ability to use GNSS. Refer to Section 6.0 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:[28,29]

- 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.

---

[28] NASPI Time Synchronization Task Force. 2017. Time Synchronization in the Electric Power System. North American SynchroPhasor Initiative. NASPI-2017-TR-001. Accessed Nov. 13, 2020, at https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf.

[29] Broumadan, A., S. Kennedy, and J. Schleppe. 2020. "Nobody's Fool: Spoofing Detection in a High-Precision Receiver." Inside GNSS. Accessed Nov. 13, 2020, at https://insidegnss.com/nobodys-fool-spoofing-detection-in-a-high-precision-receiver.

- 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). 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.[30]

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, and more. 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. 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, as well as 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, precision internal oscillators, or potentially cellular signals.

[30] Broumadan, A., S. Kennedy, and J. Schleppe. 2020. “Nobody’s Fool: Spoofing Detection in a High-Precision Receiver.” Inside GNSS. Accessed Nov. 13, 2020, at https://insidegnss.com/nobodys-fool-spoofing-detection-in-a-high-precision-receiver.

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 LAN, 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 whether 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.

5.0 [Respond] Responding to Detected Attacks

Developing and executing on planned responses when anomalous PNT data or behavior are detected can significantly reduce the impact of these events. Several activities should be included in these plans to ensure that impacted people, processes, and technologies are aware of the event, the event is understood, and the event is contained.

5.1 Reporting of Detected Attacks

Part of the respond function is reporting to and alerting personnel of the detection. Providing this awareness allows personnel to respond and act 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 electricity industry and enhances industry's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.[31] 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.[32]

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.

Electric utilities are required to submit DOE-417 forms (Electric Emergency Incident and Disturbance Report) to DOE 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.[33] 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.[34] This site is a useful resource for users to determine any GPS issues, testing, or outages.

---

[31] NERC. 2024. "Electricity Information Sharing and Analysis Center. North American Electric Reliability Corporation. Accessed Sept. 17, 2024, at https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.
[32] CESER. n.d. "Energy Sector Cybersecurity Preparedness." Office of Cybersecurity, Energy Security, and Emergency Response, Department of Energy. Accessed Sept. 17, 2024, at https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity.
[33] GPS.gov. n.d. "GPS: The Global Positioning System." Accessed Sept. 17. 2024, at https://www.gps.gov.
[34] USCG. n.d. "Navigation Center." United States Coast Guard. Accessed Sept. 17, 2024, at https://www.navcen.uscg.gov.

Some systems, like GNSS receivers, may not be connected to the network and may 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 IEC/IEEE 60255-118-1) 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.

To assist with reporting events and incidents, there are tools and systems that can be used to provide information and evidence related to these events. The next two subsections highlight a few common examples.

5.1.1 Syslog and Simple Network Management Protocol

Many devices, including GNSS receivers, support reporting status and events via system logs (syslog)[35] or Simple Network Management Protocol (SNMP).[36] 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.

5.1.2 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 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.

---

[35] Network Working Group. 2009. Request for Comments: 5424. Accessed Nov. 13, 2020, at https://tools.ietf.org/html/rfc5424.
[36] Network Working Group. 2002. Request for Comments: 3410. Accessed Nov. 13, 2020, at https://tools.ietf.org/html/rfc3410.

5.2 Analysis of Detected Event

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.

5.3 Mitigation Measures

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 and long-term holdover oscillators or backed-up off-site 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 [Recover] Recovery Actions

The general PNT profile in NIST IR 8323 R1 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. This automatic recovery is especially important for devices that are located in unstaffed remote locations where response times for manual recovery could be many hours.

6.1 Response and Recovery Plans

Response plan processes and procedures are developed, 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[37]
- 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 or other GNSS constellations could be an important first step in addressing disruptions.[38]

PNT recovery plans incorporate lessons learned from ongoing incident handling activities into incident recovery procedures, training, and testing, and then implement the resulting changes accordingly. Recovery plans include activities required to

- Return the PNT services and capabilities to normal operation
- Communicate with appropriate users, applications, and stakeholders through this effort
- Improve and advance the recovery plans through lessons learned.

6.2 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.

---

[37] FERC, NERC, and REs. 2020. Cyber Planning for Response and Recovery Study (CYPRES). Federal Energy Regulatory Commission, North American Electric Reliability Corporation, and Regional Entities. Accessed Feb. 20, 2021, at https://cms.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf.

[38] GPS.gov. n.d. “GPS Service Outages and Status Reports.” Accessed Dec. 15, 2020, at https://www.gps.gov/support/user/#civilian.

7.0 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 relate 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.

Appendix A – Considerations for Customizing Sector-Specific PNT Profiles for an Individual Organization

The following information is reproduced from page 5 of the NIST IR 8323 R1 document to assist individual organizations in incorporating appropriate and applicable aspects of the profile to develop a stronger risk management program in areas where PNT data is used.

“Organizations within various sectors can customize the PNT Profile by considering the following:

- What processes and assets require PNT data (direct recipients of PNT services)?
- What processes and assets are dependent on other assets that require PNT data (i.e., what are the secondary effects)?
- What processes and assets are vulnerable to the disruption or manipulation of PNT services? • What are the integrity and availability thresholds of PNT to avoid mission impact?
- What safeguards are available?
- What is the impact to the organization should a process or asset be lost or degraded?
- What techniques can be used to detect events of concern?
- What techniques can be used to respond to events of concern?
- What techniques can be used to recover pre-event capabilities?”

Pacific Northwest National Laboratory

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

www.pnnl.gov