

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1500-08
Natl. Inst. Stand. Technol. Spec. Publ. 1500-08, 28 pages (January 2017)
CODEN: NSPUE2

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.1500-08>

Acknowledgements

The authors gratefully acknowledge the significant contributions from individuals and organizations from industry, government and academia who provided the thoughtful presentations, questions, and discussions leading to the content and knowledge described in the report. In particular, we would like to acknowledge our distinguished presenters and panelists, Dewey Day, Vahid Madani, Brenden Russell, Robert Orndorff, Glen Chason, Sarah Mahmood, Terry Jones, Jeffrey Dagle, Judah Levine, Grace Gao, Rick Blum, Phil Evans, Mark Adamiak, and Carmine Chase. We also acknowledge the reviewers of the report, John Garguilo and Eugene Song.

We would also like to express our sincere appreciation to our management teams, collaborative partnerships, and our conferencing services team who enabled the workshop held at the National Institute of Standards and Technology (NIST):

- NIST Engineering Laboratory's Smart Grid and Cyber-Physical Systems Program Office, Chris Greer, David Wollman, Avi Gopstein
- NIST Information Technology Laboratory's Software Systems Division, Ram Sriram and John Messina
- NIST Physical Measurement Laboratory's Time and Frequency and Quantum Measurement Divisions
- IEEE Standards Association

The workshop report is authored by the Steering Committee of the Timing Challenges in the Smart Grid Workshop.

Presentations and webcast are available at:

<https://www.nist.gov/news-events/events/2016/10/ieeenist-timing-challenges-smart-grid-workshop>

Executive Summary

Correct time and timing is one of the foundational elements in enabling the communication and orchestration of technologies for accurate and optimal wide area monitoring, protection and control (WAMPAC) in the power industry. The National Institute of Standards and Technology (NIST) and the International Electrical and Electronic Engineer -Standard Association (IEEE-SA) conducted a workshop to gather inputs from stakeholders to identify, analyze, and provide guidance on technologies, standards and methodologies for addressing the practical timing challenges that are currently being experienced in wide area time synchronization.

One of the key drivers for the workshop is the need to prioritize NIST efforts in addressing precision timing needs in power systems. NIST has established a Smart Grid Testbed, which includes the Precision Timing module to support the IEEE 1588 Power Profile efforts and to serve as a basis for timing measurement and security research. The objective of the workshop was to identify the timing challenges, the community of experts, and potential collaborators as well as key research priorities to guide future efforts to ensuring that the integrity, availability, accuracy, and precision of timing requirements are met in power systems.

Precision timing synchronization with requirements ranging from one microsecond to hundreds of nanoseconds within and across substations is currently being characterized and monitored by utilities in order to advance capabilities in real-time measurement and control and to reap the economic and environmental benefits of more intelligent and efficient use of generation and storage resources while meeting customer demands. The proliferation of widely deployed smart sensors for WAMPAC, distribution and energy management systems, along with the increasing need for fault detection and location as well as maintaining system stability in real time using spatio-temporal and temporal-frequency analyses, all require precision timing. These new capabilities offer increased flexibility to grid operators, but they also raise new security concerns.

Among the concerns expressed include timing discontinuities such as leap seconds, Daylight Savings Time, and GPS Week Number Rollovers. Additionally, the increasing prevalence of jamming and the potential for spoofing is leading security, time and network experts in power systems or other domains to explore alternative propagation methods of traceable time. These include eLORAN, Iridium, IEEE 1588 Precision Time Protocol (PTP), Network Time Protocol (NTP), radio (WWVB is the NIST operated time signal radio station near Fort Collins, Colorado.), atomic clocks, and other terrestrial and satellite-based timing propagation solutions.

Given the current stage of exploration and characterization for real time control, utilities and system integrators identified the top industry challenge to be integrity assurance, with the first steps being device conformance and interoperability testing, performance monitoring and timely detection of any potential anomalies. Developing thorough, robust conformance and interoperability test methods would provide a degree of assurance that precise time will be properly distributed and devices can synchronize to a required degree of accuracy as defined by industry. System end-to-end interoperability and performance

testing also provides assurance that the time distribution across multiple devices from various manufacturers can meet industry specifications. The ability to provide real time monitoring and time uncertainty values to the end user or application will allow a system to decide on the applicability or weight of the data with respect to its end application. The rapid detection of intentional and unintentional time anomalies was identified by several utilities as a key near-term requirement.

In parallel, it is also important to assess and understand the impact of time uncertainties on current and future applications such as modeling, prediction, and optimization of transmission and distribution grid control algorithms. As the industry moves towards mesh networks for localized generation and distribution of power, more opportunities emerge for engaging in timely forecasting and responses. Questions regarding how errors and uncertainties in time can impact grid operations continue to be explored. In addition, there is a need for Research and Development (R&D) support in the power industry in order to fully exploit the capabilities afforded by having precise time to realize unparalleled coordination, control, responsiveness, and prediction capabilities.

Table of Contents

| | |
|--|-----------|
| Executive Summary | 2 |
| I. Introduction | 5 |
| II. Application Requirements | 6 |
| III. Time Distribution in Power Systems | 9 |
| IV. Time Issues and Challenges | 10 |
| V. Time Distribution Sources | 11 |
| VI. Time and Security | 13 |
| VII. Potential R&D Areas | 14 |
| VIII. Priorities | 16 |
| IX. Current Efforts and Collaborative Opportunities | 17 |
| X. Conclusion and Future Work | 20 |
| Appendix 1. Agenda | 22 |
| Appendix 2. References | 24 |

I. Introduction

Under the Energy Independence and Security Act, NIST has been tasked to engage and coordinate stakeholders to establish a consensus-based framework for Smart Grid interoperability standards. One of the key drivers for the workshop was the need to coordinate and prioritize efforts in addressing precision timing needs in power systems. NIST has established a Smart Grid Testbed, composed of multiple modules, including Microgrid Control, Cyber (Cybersecurity, Network Communications, and Precision Timing), Smart Storage, and Smart Sensors. The Precision Timing module was initially designed to support measurement and standards in PTP [1] and understanding how precision clocks can be used to improve power systems applications [2, 3]. The NIST Smart Grid Precision Timing Project provided a novel, open source, software-based prototype to monitor PTP performance [4] with the plan to extend its capabilities to serve as a basis for timing measurement and security research. As a program, we have also explored the effects of leap second on phasor measurement unit (PMU) implementations [5].

Recognizing the growing need for robust and resilient precision timing, IEEE-SA and NIST have been supporting the University of New Hampshire InterOperability Lab (UNH/IOL) in the development of a Test Plan for IEEE C37.238-2011 [6] and a Test Suite Specification along with a certification program for the draft IEEE C37.238 PTP Profile for Power System Applications. UNH/IOL, with NIST guidance and support, will also be exploring the security implementation of network time distribution, namely IEEE 1588 security extensions in the current draft standard. Additionally, with the timing and cybersecurity expertise, the NIST Smart Grid Program has also explored research areas to improve precision timing capabilities [7,8], precision time metrology [9,10], and anomaly detection [11].

The objective of the workshop was to identify the challenges, the community of experts and potential collaborators as well as key research priorities to guide future NIST efforts in ensuring that the integrity, availability, accuracy, and precision of timing requirements are met in power systems.

In dynamic distributed measurement and control systems where scheduling of resources, seamlessly orchestrated coordination, and hard deadlines must be met, measurement data, state estimators and control commands are temporally valid for a specific, sometimes brief duration. To provide the common time reference for correct temporal behavior, all systems must be synchronized to a common traceable time and frequency reference source. Time-sensitive applications in power systems include sensing, data fusion, and ensuring deterministic latencies in communication, computation (software) and control actions.

In the U.S. power grid, where each interconnection stretches over a large geographical expanse, achieving correct timing can be challenging. Time distribution issues include, but are not limited to, resolving multiple time scales, Global Navigation Satellite System (GNSS) receiver performance, packet delay variations in the communication infrastructure, and cyber-physical security as well as concerns for reliability and

resilience when a reference source becomes unavailable or unreachable. The workshop included presentations on wide area precision clock synchronization requirements based on their implementation of smart grid devices and systems.

One of the primary priorities identified is the need for verification and monitoring of the timing system integrity. One of the current challenges is ensuring that the devices can interoperate, properly handle timing discontinuities (leap second) and monitor/detect anomalous behavior. This report includes current industry, academic, and government efforts discussed at the workshop to improve timing integrity through a comprehensive understanding of timing performance impact, pertinent timing performance metrics, conformity and interoperability testing and end-to-end system monitoring. Efforts are also underway to enable detection of anomalous behavior and achieving more robust design and deployment using redundant and diverse routes and alternative means to reach time sources. These efforts serve as key steps towards the integrity and resiliency assurance of precision time distribution in power systems.

During the workshop, it was noted that utilities rely on academia, national labs and government for research development, device and interoperability testing and simulation trials given minimal budget and the need for well-characterized testing prior to evolving technology for deployment in critical power systems applications. An industry need exists for unbiased research and development of measurement and test methods to ensure and monitor timing integrity. The knowledge incurred from research can then be transferred to and validated by industry through field testing and characterization before full deployment in the power grid. It is also important to provide a feedback channel between research and utilities to fully understand the impact of environmental and system complexities that can potentially degrade the quality of the precision time synchronization.

II. Application Requirements

Utilities and literature that were referenced during the workshop coordination and presentations identified the wide area precision timing requirements necessary in measurement, protection and control applications. In addition to evolving automation technology requirements, industry standards and guidance, including the IEEE Power Systems Relay Committee (PSRC), the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Power Systems Management and Associated Information Exchange Committee, and the North American Electric Reliability Corporation (NERC), also outline specific requirements for time synchronization and time-stamping [12, 13, 14, 15, 16].

The most stringent application identified by utilities is Traveling Wave Fault Detection, which requires synchronization on the order of hundreds of nanoseconds in order to precisely locate a fault to the scale of hundreds of feet as the electricity waves are traveling at near the speed of light. When an event occurs between two traveling wave fault detectors, the anomalous waves are time-stamped. Comparing the timestamps between the two detectors provides information on the fault location.

To that end, synchro metrology (synchronous sensors) is among the key technologies in building awareness among the grid to make timely decisions on the network. These time-stamped power quantities are used for monitoring, control, prediction, and optimization applications. Among the main uses with the most stringent time requirements is the ability to take time-synchronized measurements using PMUs and provide consistent reporting rates at 60 times per second. Synchrophasors are used for WAMPAC applications such as Frequency Event Detection that can cover a geographical area over hundreds of miles. Discrepant shifts in phase angles alert system operators to dynamic voltage and frequency stability issues. The higher reporting rates provide higher resolutions that can detect fast transients in the system. Synchronization is required through the hierarchy of the data flow from PMUs to Phasor Data Concentrators (PDCs) to Super PDCs. With the proliferation of synchronous sensing in the power grid, there is an opportunity for greater reliance on using measurements for WAMPAC. However, the requirements are on the order of 1 μ s and better to meet and exceed the IEEE C37.118-2011 *Standard for Synchrophasor Measurements for Power Systems* requirement for ensuring that the Total Vector Error (TVE) remains under 1 percent for synchrophasor applications [12].

In protection applications, line differential relays, spanning distances on the order of hundreds of miles, compare current measurements to detect and respond to faults and trip breakers in time. Relays rely on GNSS synchronization, but can be synced by communications if available. Protective Relays requirements are on the order of tens of microsecond to one millisecond.

Finally, the less stringent requirements include Sequence of Events and Digital Fault Recording where the utilities and system integrators reported requirements of 50 μ s to ms. Sequence of event recorders are used to know exactly when the breaker trips. Such recorders answer questions for the protection engineers on the chronological relationships, allowing investigation of issues such as lightning strikes and downed poles.

Digital Fault Recorders (DFRs) monitor the current and voltage on the grid at high sample rates. Time-tagged data can be matched with other recorders to analyze system events. Everything is time-aligned to correlate events. Automated lightning correlation monitors the time-stamped voltage and current wave forms to determine the point of origin.

Substation local area network communication protocols such as IEC 61850 Generic Object Oriented Substation Events (GOOSE) and Sampled Values (SVs) also require accurate time synchronization on the order of 1 ms and 1 μ s, respectively. Time synchronization is needed within the substations where merging units (MUs), other sensors must provide time-stamps to each measurement. Substations will begin to explore and rely on IEEE C37.238-2011 Standard Profile for use of IEEE 1588 Precision time protocol for power system applications [13] and IEC/IEEE 61850-9-3 (2016) *Communication networks and systems for power utility automation: Precision time*

protocol profile for power utility automation [14], which require $\pm 1 \mu\text{s}$ synchronization accuracy. Table 1 summarizes the time accuracy and precision requirements.

Accurate measurement of the timeliness of application response and communication latency over a distributed area also requires synchronized time to provide a common frame of reference when time-stamping two events, such as send and receive. Dynamic control also relies on fast and/or deterministic latency. Line Differential Protection requires reliable communication and time synchronization. Time errors contribute to discrepancies in the latency measurement with respect to the actual communication and processing latencies. Currently, not all latency and latency variation requirements for WAMPAC are well-understood and the impact still needs to be assessed.

Distribution and Energy Management Systems (DEMSs) use precision time. Distribution Management systems (DMSs) rely on wide area wireless synchronization for time stamping at the time of sampling. Energy Management systems (EMSs) data are time-stamped by the server synchronized to NTP at the server receipt time.

Table 1 Wide area precision time requirements in current power systems

| Application | Time Accuracy Requirement |
|--|----------------------------------|
| Traveling Wave Fault Detection and Location | 100 to 500 ns |
| Synchrometrology (synchrophasors) Wide Area Protection Frequency Event Detection Anti-Islanding Droop Control Wide Area Power Oscillation Damping (WAPOD) | Better than $1 \mu\text{s}$ |
| Line Differential Relays | 10 to $20 \mu\text{s}$ |
| Sequence of Events Recording | $50 \mu\text{s}$ to ms |
| Digital Fault Recorder | 1 ms |
| Communication Events | |
| Substation Local Area Networks (IEC 61850 GOOSE) | $100 \mu\text{s}$ to 1 ms |
| Substation Local Area Networks (IEC 61850 Sample Values) | $1 \mu\text{s}$ |

Finally, with the power grid evolving from generally steady centralized generation with local sensor inputs and control to dynamic, localized mesh networks of Microgrids with remote sensor inputs to leverage and optimize variable generation sources, there continues to be evolving research indicating greater reliance on synchronized time. Time is used in understanding the relationships over time, including frequency variations over time (temporal frequency analysis) as well as time and location variations over time (spatial-temporal analysis) with respect to fault detection/location of fast transients and

developing better grid models for power systems applications. In particular, handling system transience, such as weather events, requires fast dynamic response to maintain voltage and frequency stability in the grid. Better time agreement leads to better situational understanding and improved control for anti-islanding and wide area power oscillation damping (WAPOD) applications [17].

Response latency requirements are detailed in industry standards such as IEEE 1547 Standard for Interconnecting Distributed Resources with Electric Power Systems [18]. Latency requirements for real-time control of distribution networks remains a key research area. The complexity of coordinating remote inputs requires additional constraints and a systematic method to ensure that the use of distributed inputs for control can outperform locally available information [19]. Time latency tolerances can be variable and dependent upon power system characteristics and control schemes but are generally on the order of milliseconds for distributed generation. Measurements messages are received on the order once every 16.7 ms for reporting rates of 60 messages per second in PMUs. Volatility of generation sources and the ability to aggregate measurements and compute states are estimated on the order of 100 ms for real-time applications, providing explicit power set points for ensuring voltage stability in distribution grids with mesh networks of uncontrollable loads, stochastic and deterministic energy resources [20,21].

III. Time Distribution in Power Systems

Utilities rely on the use of GPS for wide area time synchronization as the means of acquiring a standard reference atomic time signal into the substations and for equipment in the field over a wide area. For utilities with accessible and available network communication lines, network-based devices can use network-based time distribution protocols such as the Network Time Protocol (NTP) [22]. Various utilities are also at different stages in deploying and characterizing IEEE 1588 Precision Time Protocol (PTP) [23] deployments. The communication technologies being explored are Ethernet-based fiber connections with Synchronous Optical Networking (SONET) and Carrier Ethernet. The communication infrastructure is being designed and deployed to support the increased proliferation of data exchange due to the wide area sensors. Utilities are beginning to leverage the advanced communication infrastructure to propagate time information as well. For wide area PTP deployment, the International Telecommunications Union (ITU) PTP Telecom Profiles for Frequency (ITU G.8265.1) [24] as well as Phase/Time (ITU G.8275.1) [25] for inter-substation communication between hubs to substations, was reported to cover over 150 miles between end points.

Within the substation the methods of time propagation include Inter-Range Instrumentation Group-B (IRIG-B) time signal [26] with time quality and leap second specifications based on IEEE C37.118 [12], NTP and PTP from a GNSS source. In some large substations, full redundancy of time sources and devices to monitor and corroborate measurement results are deployed. Advanced communications networks rely primarily on optical fiber as the physical communication medium. In PTP deployments, Grandmaster clocks with an atomic clock, such as rubidium, are used for providing holdover

capabilities necessary to deal with source and propagation glitches. Transparent clocks (TCs) are used to provide full timing support over the networks. The IEEE C37.238 PTP Power Profile is typically used in intra-substation communications.

Historically, time signals are assumed to function properly and are typically an afterthought, as the accuracy and precision had been sufficient for post-fault analysis. With the onset of dynamic control, an increasing number of utilities are recognizing the need to characterize and monitor the integrity of all time signal going into their devices and to ideally have access to the time quality information as part of the assessment process before making control decisions. In characterizing and monitoring new time distribution technologies, some utilities have dedicated efforts to monitor the source and network time propagation performance to ensure that it maintains or exceeds the industry requirements.

Device testing of newly acquired equipment and at each firmware upgrade is necessary to ensure proper operations under normal and anomalous conditions or special events such as known timing discontinuities. GNSS simulators are used to evaluate the GNSS receivers to ensure that the devices can properly handle leap seconds, Daylight Savings Time (DST) changes, week rollovers, satellite anomalies and year rollovers. IRIG-B monitors have also been developed to monitor the signal and observe any glitches as well as conformance to industry standards such as IEEE C37.118-2011.

System-level end-to-end testing is also necessary to ensure precision clock synchronization in typical and stress scenarios. For network-based protocols, noise impairment tests, Ethernet Packet Corrupters (ability to duplicate or drop packets) are used to observe the impact on time accuracy performance.

IV. Time Issues and Challenges

Having time as a foundational aspect of the power grid opens up new security concerns, which was the most prominent challenge brought up at the workshop. Several utilities echoed the sentiment that timing gives more flexibility but also challenges the security of the system. The impact of time errors among devices have the potential to be misinterpreted as power system disturbances. In one measurement device where its GPS receiver locked to a single satellite in test mode, this led to the loss of two 500 kV transmission lines. Before providing advanced grid automation capabilities it is imperative to ensure *integrity of the timing* and the measurement.

Among the most significant challenges is the ability to provide *sub-microsecond synchronization*, or in some cases, hundreds of nanoseconds, *over a large geographical expanse*. With GNSS as the primary source, the technology can be susceptible to intentional and unintentional interference due to the low power signal propagation. Well-established security concerns include the increased use of personal privacy devices (jammers) and the potential for spoofing of GNSS signals. Alternative solutions to GNSS are few and costly.

Network-based time distribution technologies such as NTP and PTP have also been used. Over a wide area, these technologies are challenged by *packet delay variations* over the networks that provide partial or no time support.

There have also been instances of device implementation behavior where it does not *conform to the time requirements in industry standards*. After a GPS loss, it was noted that the time-quality bits in IRIG-B timing data, and similarly PTP implementations, were not properly updated to indicate the loss of the primary source and that the device is either on holdover or may have a time stamp with degraded accuracy.

The variations in precision synchronization performance among device implementations is further amplified by the detection and handling of *anticipated time discontinuities* and *unanticipated time anomalies*. Anticipated time discontinuities include the leap second and DST depending on whether the time stamps are in local, Coordinated Universal Time (UTC). The temps atomique international (TAI) time scale, which the GPS timescale and PTP timescale are based, is a continuous, monotonically increasing atomic timescale traceable to the reference standards ensembled from over 50 national laboratories throughout the world. However, in devices designed to prevent unanticipated time anomalies, where the devices are prohibited from large jumps forward or backward as part of security assurance features, this can make them difficult to test and verify correct behavior for anticipated discontinuities such as leaps seconds and rollovers. *Addressing multiple timescales*, such as TAI, UTC, or a variant of a local time, in a system of synchronized clocks and resolving between different systems can be an error-prone process when devices are implemented differently.

There continues to be the speculation for *higher levels of accuracy* driven by synchro metrology applications in distribution grids where events (wind and solar generation variations) can happen at faster rates than the traditional power frequencies (e.g. 60 Hz). In addition, the requirements need to be considered in the context of evolving technologies in distributed computing, where the latencies in network communication and data processing can affect the ability to take control actions in time.

With respect to the power industry, another key challenge is fully understanding the *quantifiable synchronization performance metrics*, in addition to accuracy to define correct behavior in clocks, time, and time distribution. Once the metrics are identified, there is a need for reproducible and repeatable test methods for the devices. In particular metrics relevant to reliability, availability and serviceability (RAS) need to be identified and quantified. Some of the speculated metrics include holdover time, clock stability, etc., which are defined in other industries such as telecom and transportation. *Business challenges* such as affordability, flexibility, and sustainability must also be considered when seeking a viable solution for time assurance.

V. Time Distribution Sources

All four utilities present at the workshop rely on GNSS as the propagation medium for a traceable standard time reference. While some devices have a built-in GNSS receiver,

many devices rely on time distribution signals and protocols such as IRIG-B, NTP, or PTP to synchronize the clocks at the sensors, controllers, and applications. Given the known cyber and physical vulnerabilities of time propagation, another thrust of providing time assurance is to have alternative sources and diverse means and routes for propagation to avoid single points of failure in critical systems.

The principles of time distribution requires a trusted source (typically a time reference from a national or international entity, such as TAI or UTC) that can provide the current time and a propagation methodology that can accurately account for the propagation delays of transporting the current time message. The workshop covered some of the current and future methods of time propagation.

GNSS provides means to a free time distribution service to GNSS receivers. The number of satellite constellations such as GPS, GLONASS (Global Navigation Satellite System, transliteration from Russian), Galileo, and Beidou continues to increase. Signals are readily vulnerable to natural, accidental and intentional interferences such as celestial jitter, geomagnetic interference, satellite anomalies, jamming through use of personal privacy devices, spoofing, Denial of Service (DoS), and timing drift. Test cases with a GNSS simulator or recording – leap seconds, Daylight Savings Time (DST) changes, GPS Week and Year Rollovers – can be used to verify the behavior of the GNSS receiver. Iridium satellite systems are privately owned and therefore time distribution from these satellites is provided as a paid service. The accuracy of the synchronization can be as good as 10 ns using a high quality oscillator, but is typically on the order of 200 ns with a Temperature Controlled Crystal Oscillator (TCXO).

Pacific Gas & Electric (PG&E) and Bonneville Power Administration (BPA) have explored the use of PTP and characterizing the performance before full integration into their advanced WAMPAC systems. PTP can easily provide sub-microsecond precision synchronization within substations in a local area network. However, to achieve the same precision over a wide area comes at a greater cost. The telecom industry, through a Cooperative Research and Development Agreement (CRADA) at NIST has shown it is feasible to have a system time accuracy well under 100 ns over a dedicated optical fiber network. Given the utilities are exploring the Telecom Profile for long-distance time synchronization, PTP can be seen as a viable option for distribution of a traceable time reference.

Ground based radio signals such as, *WWVB* [27] and *differential WWVB* systems have demonstrated the ability to maintain close to one microsecond precision synchronization for systems up to 10 km away from the radio's signal source. RF Beacons (terrestrial beacon network) provide broadcast beacons with propagation accuracy similar to GNSS.

eLORAN signals can penetrate buildings. Reference station is needed within about 50 km of the device to achieve one microsecond accuracy. Continued research and testing is needed of *eLORAN* deployment and operation in noisy power systems environments, where it may be a challenge to receive Low Frequency RF signals. One potential solution is to transmit the signal underground.

Time Measurement and Analysis Service (TMAS) is a NIST provided measurement service to continuously monitor a local system's time compared to UTC(NIST) based on simultaneous common-view measurements using GPS and the Internet [28]. *TMAS* can be used to monitor the accuracy of a local synchronization system to the NIST standard reference UTC(NIST) and provides a means to meet traceability requirements.

VI. Time and Security

Knowledge of how we can understand the impact of compromised or erroneous time will provide the basis of a risk assessment framework in addressing the security concerns and designing cost-effective, robust solutions.

Given that the accuracy of time synchronization was traditionally an afterthought and often operated sufficiently well to not cause noticeable issues, there has been even less credence in security for time synchronization. However, the integrity of the time is now on the forefront of application requirements, as it directly impacts the measurement quality and the ability to make intelligent control decisions.

Furthermore, the increased communication and decentralization opens up the system to security vulnerabilities, where DoS attacks have been exploited in NTP. Requirements analysis based on the threat model defined in RFC 7384 *Security Requirements of Time Protocols in Packet Switched Networks* [29], have provided guidance to the standards community for both NTP and PTP in developing frameworks and guidance for securing network-based protocols [30].

PTP Integrated Security Mechanism has a four-pronged approach:

- (A) *PTP Integrated Security Mechanisms*. The integrated approach includes a time, length, value (TLV) definition for authentication and integrity verification, including the key distribution protocol, Group Domain of Interpretation (GDOI), and symmetric key management, Timed Efficient Stream Loss-Tolerant Authentication (TESLA, a lightweight broadcast/multicast authentication mechanism adopted by IEC 61850). Integrity checks are based on the Integrity Check Value (ICV) in the proposed TLV.
- (B) *External Transport Security Mechanisms*. The external transport mechanisms include Internet Protocol Security (IPSec) and IEEE 802.1AE MAC Security Standard (MACSec), which provide integrity protection and authentication at the transport (Ethernet) layer.
- (C) *Architecture Guidance*. The guidance will be based on redundancy, including diverse sources and paths to PTP grandmasters, along with the inherent measurements related to architecture and performance measurements such as delay and offset.
- (D) *Monitoring and Management Guidance*. The guidance will include a definition of metrics in the PTP data sets to be monitored to detect security issues as well as the security guidance on optional management protocols, including the IEEE 1588 Management messages.

The Internet Engineering Task Force (IETF) Network Time Security (NTS) specification draft development is exploring additional security for NTP including the use of Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS) combination as well as the need for confidentiality of time, where any information visible, including timing trends, allows for pervasive monitoring and can be considered a potential point of vulnerability.

In presentations from PG&E and BPA, *redundancy* is the among the current means of verifying correctness of the time and providing system resiliency to potential time glitches. Different levels of *redundancy* from time source redundancy in a single measurement device to full system redundancy (multiple PMUs with separate time distribution sources) can provide a means to monitor whether the source of error in any detected deviations is in the time or in the power quality.

VII. Potential R&D Areas

Integrity assurance

What are the key timing assurance metrics for the power systems domain?

Measurements and standards dictate accuracy and precision requirements as important metrics in the power systems domain. However, the quality of the time or clock is also dependent on other performance metrics such as stability, holdover, etc. Such metrics remain to be identified through rigorous experimentation on how clock and time parameters can impact power systems applications.

How can we trust the device's / system's time?

The development of device (conformity) and end-to-end system (interoperability) *test methods* needs to be addressed to ensure that they are robust, repeatable, and reproducible in both test environments and in field deployments. One of the key areas is determining the metrics that will have impact on the end applications. The metrics can then be applied to the test methods and characterized under test and field operation conditions. Test methods must also be provided for firmware testing at each upgrade and testing of edge cases over the lifetime of the device. Security test methods in verifying the ability to provide assurance to authentication, integrity, and potentially confidentiality will also be beneficial to the power systems industry.

What is the performance characteristics of the source signal? How well is the system synchronized?

Real-time monitoring of time sources and distribution mechanisms along the traceability chain are necessary to pinpoint the source of timing issues. At Dominion Virginia Power (DVP), IRIG-B monitoring is done with a low-cost Arduino, and can be adapted on other low-cost embedded platforms. Similar means of providing trustworthy monitoring of network-based time distribution such as PTP and NTP is being developed. Questions remain on whether software-based monitoring can be within a tolerable uncertainty and precision compared to industry requirements. Monitoring of GNSS receiver behavior and potentially the GNSS satellite data from usable satellites may also provide insights to the

performance and potential anomalies encountered with precision clock synchronization of the system.

How to rapidly determine a timing problem?

Anomaly detection will also become critical as automation systems begin to rely on timing. Anomaly detection can be applied to GNSS, network-based protocols such as NTP or PTP, or other means of time distribution to ensure that the time signals propagated are normal. The anomalies to be detected include time step, frequency step and missing data. At the NIST Time and Frequency Division, the common-view time transfer, which provides a multisource voting scheme to determine whether there is a problem as well as the source of the problem. A model is developed for each clock and the system as a whole through a feedback loop where the model is adjusted based on its ability to predict a future time and frequency offset.

Secure Timing (Integrated and External)

Requirements for robustness in the presence of directed attacks on distributed precision time service with respect to physical and cyber-attacks as well as resiliency in presence of storms and earthquakes, electromagnetic pulse, and geomagnetic disturbances are the key drivers in the need for more research to develop such technologies. The Grid Modernization Initiative (GMI) 2020 goal is for synchrophasors to remain reliable during transient events, including natural disturbances and malicious (cyber and physical) attacks. Reliability of synchrophasors is fundamentally tied to the ability to synchronize the clocks of the measurement devices during the transient events. Quantifying the success of the ability to secure time can be based on the NIST Framework for Cyber-Physical Systems [31] and the Department of Energy's (DoE) Cybersecurity Capability Maturity Model (C2M2) [32].

What are other sources of time propagation that can provide cost-effective, traceable sub-microsecond time synchronization over a wide area in power system environments?

The industry is looking for other references in ensuring multiple points of truth and avoiding single points of failure. Alarming and notification (based on IEEE 1613 Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations [33]) will also be key components to provide a fault-tolerant timing signal.

What is the impact of timing uncertainty on next-generation Smart Grid applications?

Another identified need is deeper understanding of how time errors impact the evolving technology landscape of next-generation Smart Grid applications. The questions on the *sensitivity of application to time errors* remain. Understanding of the safety, economic, and other impacts of time sensitivity on future grid applications is necessary to drive some of the more costly efforts in providing assurance to traceable time synchronization. With the trend towards decentralized control, variable generation sources, and transactive prosumers, the impact of the preciseness of time synchronization between nodes and timeliness of actions is speculated to become a greater need.

Developments of experimental test benches have begun in this area to help assess the WAMPAC applications, namely wide area passive anti-islanding protection and WAPOD, tolerances to compromised time signals [17]. Impacts of compromised time signals include corrupted wide area grid monitoring, false protection activation, and degradation of wide area protection performance. In WAPOD applications, compromised time signals have been shown to increase in overshoot/undershoot, rise in the decay ratio, longer settling times, and eventually system instability [17].

Can algorithms for next-generation Smart Grid applications be improved to be less sensitive or even immune to time errors? In parallel to getting the time correct, algorithms that are immune or less sensitive to dynamic time errors can also be explored.

VIII. Priorities

Because the power industry has not yet reached the stage where synchronized time is relied upon for critical control needs, the primary need is the ability to qualify, characterize, and monitor devices as well as end-to-end systems. *Integrity assurance* was identified as the key priority. Research is needed on understanding the impacts, which will provide input to industry standards and technology efforts on the types of requirement metrics and the parameterization of the metrics. Integrity assurance is key, and research focused on system time performance monitoring, anomaly detection, and other assurance methods, is needed as exploration and reliance of automation technologies in power systems increase.

A. Testing and certification

The *importance of testing* was emphasized in several presentations and during discussions as device behavior under normal and anomalous conditions can be critical in achieving sufficient accurate time synchronization, especially under tight tolerances of 1 microsecond or better. Understanding the key application performance metrics along with robust, repeatable, and reproducible measurement and test methods are necessary in ensuring that the timing equipment, end devices, and their respective clocks meet power systems application requirements and constraints. Practical stress scenarios must be identified and simulated. Traffic impairments need to be injected, and system behavior needs to be tested and monitored.

B. Monitoring and anomaly detection

The ability to monitor and detect anomalies in the end device, system, propagation medium and the reference source is necessary to be able to discern the trustworthiness of the measurement data, whether control action needs to be taken, or can be taken within the prescribed latency tolerance. Monitoring with sufficient accuracy and precision for applications requiring a traceable reference source is needed. Device, end-to-end, and field monitoring and testing are also necessary to understand the metrics and parameters impacting the performance of the time quality and ultimately the end measurement and control applications.

C. Impact analysis

Research on the use of time for next-generation WAMPAC applications is needed to determine the performance metrics that can impact the feasibility and effectiveness of WAMPAC applications such as anti-islanding and demand response that would provide voltage and frequency stability with potential presence of dynamically variable loads and generation sources. The impact analysis will help provide an understanding of our dependency on synchronized time and the specific performance metrics that will impact power systems quality and operations. Several efforts have begun to explore and understand the theoretical and experimental impact of timing errors in synchrophasor applications [17,18,19,34].

D. Alternative sources and security

Another key research priority is determining alternative sources capable of microsecond or better precision, and securing the sources and propagation mediums of time from both malicious and unintentional compromises on timing integrity. Research and field experimentation of new infrastructure for propagation of traceable reference time signals, ensembling techniques of using multiple sources to derive a more accurate and precise virtual time, and building better holdover capabilities with chip-scale atomic clocks are some of the potential solutions being explored. In terms of security, both standards and research domains are active in authentication and integrity of the time source and propagation mediums.

The use of highly precise time synchronization for critical applications is still in a nascent phase. It is important to be able to measure, test, and monitor for problems as these devices and applications are being characterized and tested to see if they are robust enough for automation in critical infrastructure applications.

IX. Current Efforts and Collaborative Opportunities

Secure and Resilient Time Distribution

The Department of Homeland Security (DHS) leads a timing for critical infrastructure program, while the Electric Power Research Institute (EPRI) leads a timing and security program specifically for the power industry. Both programs are specifically targeting the industry's reliance on GNSS and seeking various options to make power systems more resilient against or in light of time errors.

In the initial work, DHS is emphasizing system-level testing to understand and inform the performance metrics and impacts required for the risk framework. Initial results show all receivers tested are vulnerable to jamming. Mitigation with receiver characterization testing (lab, open air system-level testing) was also done. The next steps are understanding the impacts of a GPS disruption. The DHS work is transferred to industry through a feedback cycle between manufacturers and end users to address any issues found. DHS has also drafted a "Best Practices for Time & Frequency Sources" document to help users reduce the aperture of vulnerability [35]. DHS continues the program to assure time for critical infrastructure through development of assured timing technologies, system-level testing and analyses, as well as timing manipulation detection.

Pacific Northwest National Laboratory (PNNL) and the North American Synchrophasor Initiative (NASPI) are developing a time synchronization guidance document targeted specifically for the stringent requirements of the synchrophasor applications. In 2016, NASPI launched the Time Synchronization Task Force (TSTF) to examine the synchrophasor application requirements and solutions for assurance of synchronized time. PNNL has an integrated Cyber Radio Frequency (RF) along with their power systems testbeds to explore sources and impacts of timing errors. One example is their research in the ability to interfere with the time synchronization through GNSS spoofing.

The University of Illinois Urbana-Champaign Information Trust Institute has published results [36,37,38] looking into attack vectors on GNSS and the ability to provide low-cost solutions to mitigate the attacks. One technique is using multiple GNSS receivers at a local site to do Direct Time Estimation by observing the clock bias and clock drift of each receiver over time and determining the current time based on Maximum Likelihood estimation. Over a larger geographical area, cooperative authentication through pairwise checking by cross-correlation with encrypted P(Y) signal was used. Detection mechanisms for GNSS spoofing in power systems are also being explored in industry and academia [39]. Impact analysis of GNSS spoofing on power systems applications is also being researched [17].

Lehigh University presented on phase offset estimation techniques to ensure robustness of time distribution mechanisms such as PTP in presence of attacks [40,41].

Oak Ridge National Laboratories (ORNL) has been exploring secure means of time distribution in the power grid [42]. Funded by DoE's Cybersecurity for Energy Delivery Systems (CEDSS) program, the team is exploring a means time authentication secured by quantum correlations (TASQC). The proof-of-principle demo is available at PNNL's Cyber-RF test bed with a utility demo scheduled for 2017.

Leap Second Preparation

DHS has a US CERT leap second document [43] that has been recently updated to accommodate the December 31, 2016 leap second event specifically for critical infrastructure. NASPI has also augmented the guidance with industry-specific insights and guidance from prior testing done at DVP, Independent System Operator (ISO) New England (ISO-NE), and NIST [44].

PTP Power Profile

There are several related ongoing efforts that impact the use of PTP in power systems. The *IEEE 1588 WG* is currently drafting the revision IEEE 1588 version 2.1. At the main protocol level, the standard deals with the time error measurements, high accuracy requirements, architecture, security, and upkeep. UNH/IOL proposes to develop a network-based monitoring tool providing application-independent monitoring, with minimal impact on the performance of the system [45]. A 1588 Tool Box for Monitoring is also part of a IEEE 1588 revision effort, where it is recognized that in field monitoring can be a challenge (and even a physical 1 pulse per second (PPS) signal can have errors) [46]. The effort will include funding and guidance support from NIST in research and

prototyping of the security options in the draft revision of IEEE 1588. Emphasis on the future vision of secure time is to ensure that timing compromises can be detected sufficiently early enough. In particular, the monitoring and security working groups are seeking participants.

The IEEE Power Systems Relay Committee (PSRC) C37.238 is in the final stages of developing the IEEE 1588 PTP Power Profile. The revision will augment the IEC 61850-9-3 with additional TLVs to support end devices using IRIG-B and end applications requiring knowledge of the dynamic time errors of the end device.

IEEE Conformity Assessment Program (ICAP) launched a Conformity Assessment Steering Committee (CASC) group in 2016, composed of utilities, system integrators, and manufacturers of time providers. The University of New Hampshire-Interoperability Lab has been drafting a Conformity and Interoperability of IEEE C37.238 Test Suite Specification (TSS) with support from NIST. Conformance is essential for ensuring future interoperability and enabling early identification of non-conformances. Interoperability is driven from the stakeholders, who determine the use cases and priorities relevant to industry. Additional items being considered for coverage in the TSS include redundancy and security (optional 1588 TLV) tests. The CASC continues to seek participation and reviewers to ensure pertinent use cases are covered, the test coverage is complete and the tests are robust, repeatable and reproducible.

Testbeds capable of holistic assessment of impact of time errors

NIST is ramping up on the CPS and Smart Grid InterOperability Testbeds where the concepts outlined in the Framework for Cyber-Physical Systems [31] can be explored and refined. The testbed will integrate Microgrid capabilities with smart sensors, cybersecurity, network communication, and timing capabilities to assess potential impacts and improve standards conformance / interoperability as well as advancing metrology in Smart Grid systems. The testbed will also include federation capabilities both internally with NIST labs and with external collaborative partners in academia, national laboratories, and industry.

The PNNL testbed's primary focus is on renewable integration (understanding the system-level effects), storage, cybersecurity for energy delivery system, end use efficiency and demand response, and analytic innovations. The goal of the testbed is to leverage computing technologies and new algorithms to provide real-time situational awareness, advance models for prediction and response system transparency. The testbed includes a physical control center (live PMU data, PMU data archive, etc.), live security data streams, with a future power grid initiative on control of complex systems. Joint testing can be realized through a federated testbed (powerNET functional Testbed), which includes a distributed control and sensing software platform, agent-based distribution, and PowerNetFederation (hardware-in-the-loop across labs).

Industry Guidance and Standards Efforts

Through standards and metrology efforts, the IEEE PSRC and IEC TC57 are leading industry standards and guidance development through the development of the PTP Power

and Utility Profiles as well as complementary standards such as IEEE C37.118 Synchronphasor Performance and Communications, Design and Implementation of Time Synchronization Distribution Systems for Substation Automation and Time Tagging in Protection and Disturbance Recording Intelligent Electronic Devices (IEDs). The NIST Smart Grid program leads and supports several of the efforts in the IEEE PSRC as well as through the Smart Grid Interoperability Panel (SGIP). The testbeds at NIST can also be used to support the development of reference implementations as well as the development of conformance and interoperability tests.

PNNL / NASPI TSTF is providing guidance and test capabilities to address timing issues specific to synchronphasor applications. They are hosting industry education events and developing consensus on requirements and practical solutions primarily for synchronphasors, and potentially applicable to other power systems measurement and control devices.

On a broader scale, the IEEE 1588 WG is finalizing a new draft with the potential for improved security and monitoring components. In addition the IETF is also looking at security for network time distribution.

X. Conclusion and Future Work

The key challenge echoed by many of the participants in the workshop is the ability to have *confidence* in the time and time stamps to a sufficient precision defined by the standard and/or application.

End users must also understand the testing methodologies and be able to characterize their time source, networks, and clocks to define normal behavior by exporting typical traffic and analyzing the data to develop models of normal synchronization and clock behaviors. In developing the test and monitoring capabilities, it must be ascertained that the instrumented system provides the means for injection and monitoring without affecting the system to be measured and at all possible points of performance degradation. There is also a need for monitoring tools capable of determining time uncertainty and quality.

Standards to provide flagging of errors – synchronphasor communication standards have a structure to support time and time quality information, but implementation inconsistencies due to lack of conformity testing or standards ambiguities can lead to interoperability issues. Unambiguous and thorough conformance and interoperability testing is necessary to verify consistency in behaviors so the system remains synchronized within industry-defined standards.

Develop a collaborative forum and open source code base to enable end users, system integrators, time providers, researchers, and standards architects to discuss, work together, and share information and tools to be able to provide integrity assurance in a fast- evolving technology landscape.

Alternative traceable reference time propagation methods and the ability to automatically select the best source propagation medium at any given time will also be key research priorities. More discussion needed on solutions and prioritization will be held at the March 21, 2017 NIST/NASPI Time Synchronization Workshop.

In light of the workshop's presentations and discussions, the next steps for NIST standards and research development will be continuous improvement of the metrology of timing performance testing, monitoring, and anomaly detection to provide the initial steps towards integrity assurance.

NIST's initial focus will be on the conformance, interoperability, and security testing of the draft IEEE C37.238 PTP Power Profile and the draft IEEE 1588 version 2.1. IEEE C37.238; conformity and interoperability testing will transition into an industry certification process led by IEEE-SA Conformity Assessment Program (ICAP). In terms of research, NIST will continue to explore real-time measurement and monitoring capabilities to minimize uncertainty in time error measurements for end applications. The NIST Time and Frequency Division will continue to be involved in the exploration of Ethernet-based time propagation over commercial telecommunications networks and ground-based radio (WWVB) as alternative sources to GNSS.

Through collaborative understanding, research and standards development with industry, academia and government, we can envision future power systems applications having access to trusted time having all the attributes of accuracy, integrity, and resiliency, enabling unparalleled measurement, dynamic knowledge, and responsiveness to enable a more economical and resource-efficient Smart Grid.

Appendix 1. Agenda

| Time | Title | Speaker |
|---|---|--|
| 8 a.m. | Introductions and Workshop Objectives Presentation | Dave Wollman, <i>Smart Grid and CPS Program Office</i> Doug Arnold, <i>IEEE 1588 Co-Chair</i> Rudi Schubert, <i>IEEE</i> |
| Utility Perspective | | |
| 8:15 - 8:35 | Utility Keynote: Time Synchronization and the Power System | Aaron Martin, <i>Bonneville Power Administration</i> |
| 8:35-8:55 | PTP for Substation Synchronization at PG&E | Vahid Madani and Dewey Day, <i>Pacific Gas and Electric</i> |
| 8:55 - 9:15 | Timing at SCE | Brenden Russell, <i>Southern California Edison</i> |
| 9:15 - 9:35 | GPS Timing in Substations at Dominion | Robert Orndorff, <i>Dominion Virginia Power</i> |
| 9:35-9:50 | <i>Break</i> | |
| Research Perspective | | |
| 9:50-10:10 | Timing Security Assessment and Solutions | Glen Chason, <i>Electric Power Research Institute</i> |
| 10:10 - 10:30 | GPS Timing in Critical Infrastructure | Sarah Mahmood, <i>Department of Homeland Security</i> |
| 10:30 – 10:50 | Emerging Solutions in Time Synchronization Security | Karen O’Donoghue, <i>Internet Society</i> |
| 10:50 - 11:10 | <i>A DOE Perspective on Time Synchronization Needs</i> | Terry Jones, <i>Oak Ridge National Laboratory</i> |
| 11:10 - 11:30 | Testbed Capability at the Pacific Northwest National Laboratory | Jeff Dagle, <i>Pacific Northwest National Laboratory</i> |
| 11:30 | Lunch | |
| Timing Research Areas: Distribution, Anomaly Detection, Resilience | | |
| 12:30-12:50 | Time Distribution: Current Technologies and Future Visions | Marc Weiss, <i>NIST Time and Frequency Division</i> |
| 12:50-1:10 | Time Anomaly Detection | Judah Levine, <i>NIST Time and Frequency Division</i> |

| Time | Title | Speaker |
|-------------------------|--|--|
| 1:10-1:30 | Clock Ensembling for Resilience | Dhananjay Anand, <i>NIST Software and Systems Division</i> |
| 1:30 - 1:50 | Reliable GPS-Based Timing for Power System Applications: A Multi-Layered Multi-Receiver Approach | Grace Gao, <i>University of Illinois Urbana Champagne</i> |
| 1:50-2:10 | Improved IEEE 1588 Synchronization Performance Bound and Attack Mitigation using Estimation Theory | Rick S. Blum, <i>Lehigh University</i> |
| 2:10-2:30 | Quantum Technologies for Secure Wide Area Time Distribution | Phil Evans, <i>Oak Ridge National Laboratory</i> |
| Industry Efforts | | |
| 2:30 -2:50 | <i>PTP Power Profile Conformity and Interoperability</i> | Bob Noseworthy, <i>UNH/IOL</i> |
| 2:50 – 3:05 | 1588 over MPLS | Mark Adamiak, <i>GE</i> |
| 3:05-3:20 | 1588 over Wide Area | Carmine Chase, <i>CenturyLink</i> |
| 3:20-3:40 | <i>Break</i> | |
| 3:40-5:00 | Round Table: <ul style="list-style-type: none"> • Application Timing Requirements Near-term and Long-Term • Time Distribution Experiences and Challenges • Potential Solutions - Standards and Technology • Future research directions | Moderated by Doug Arnold: Vahid Madani, <i>PG&E</i> Aaron Martin, <i>BPA</i> Judah Levine, <i>NIST</i> Bob Noseworthy, <i>UNH-IOL</i> Carmine Chase, <i>CenturyLink</i> |

Appendix 2. References

1. J. Amelot, J. Fletcher, D. Anand, C. Vasseur, Y. Li-Baboud and J. Moyne, "An IEEE 1588 time synchronization testbed for assessing power distribution requirements," *2010 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, Portsmouth, NH, 2010, pp. 13-18.
2. D. Anand, J.G. Fletcher, Y. Li-Baboud, and J. Moyne. A practical implementation of distributed system control over an asynchronous Ethernet network using time stamped data, *2010 IEEE International Conference on Automation Science and Engineering*, pp. 515-520. IEEE, 2010.
3. D. Anand, J.G. Fletcher, Y. Li-Baboud, and J. Moyne. "Using clock accuracy to guide model synthesis in distributed systems: An application in power grid control." *2010 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*. IEEE, 2010.
4. J. Amelot, J. Fletcher, D. Anand, C. Vasseur, Y. Li-Baboud and J. Moyne. An IEEE 1588 performance testing dashboard for power industry requirements." *Proceedings of the Workshop on Performance Metrics for Intelligent Systems*. ACM, 2012.
5. A. Goldstein, D. Anand, and Y. Li-Baboud. Investigation of PMU response to leap second. *NIST Internal Report 8077*, August 2015.
6. C. Perkins, J. Laird, R. MacEachern, R. Noseworthy, J. Amelot, Y. Li-Baboud, and K.Brady. An IEEE 1588 Power Profile Test Plan *NIST Internal Report 8002*, 2014.
7. M. Weiss, L. Cosart, and J. Hanssen. Ethernet time transfer through a U.S. commercial optical telecommunications network, *Proceedings of 2014 PTTI Meeting*, 2014.
8. M. Weiss, J. Eidson, C. Barry, D. Broman, B. Iannucci, E. Lee, K. Stanton, and L. Goldin. Time-Aware Applications, Computers, and Communication Systems (TAACCS), *NIST Technical Note 1867*, 2015.
9. D. Anand, T. Arafin, and G. Qu. Detecting GNSS spoofing using a network of hardware oscillators. *48th Annual Precise Time and Time Interval Systems and Application Meeting*, Monterey, CA, 2016.
10. A. Shrivastava, P. Derler, Y. Li-Baboud, K. Stanton., M. Khayatian, H.A. Andrade, M. Weiss., J. Eidson, and S. Chandhoke. Time in cyber-physical systems, *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*, 2016.
11. D. Anand. A set-theoretic approach to analyzing timing uncertainty within cyber-physical systems, *48th Annual Precise Time and Time Interval Systems and Application Meeting*, Monterey, CA, 2016.
12. IEEE Standard for Synchrophasor Measurements for Power Systems," in *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, Dec. 28 2011.
13. IEEE Standard Profile for IEEE 1588 precision time protocol for power systems applications, *IEEE Std C37.238*, July 2011.
14. IEC/IEEE Communication networks and systems for power utility automation: Precision time protocol profile for utility automation, *IEC/IEEE 61850-9-3*, May 2016.
15. [Reliability standards for the bulk electric systems of North America](#), NERC, Dec 2016.
16. [Security guideline for the electricity sector: Time-stamping of operational data logs](#), NERC CIP, October 2009.
17. M.S. Almas, L. Vanfretti, R.S. Singh and G.M. Jonsdottir. Vulnerability of Synchrophasor-based WAMPAC Applications' to Time Synchronization Spoofing, *IEEE Transactions on Smart Grid, Draft, October 26, 2016*.
18. IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems," in *IEEE Std 1547-2003*, pp.1-28, July 28 2003.
19. N.T. Anh, L. Vanfretti, J. Driesen, and D. Hertem. Quantitative Method to determine ICT delay requirements for wide-area power system damping controllers, *IEEE Transactions on Power Systems*, 30(4), September 2014, p. 2023-2030.
20. A. Bernstein, L. Reyes-Chamorro, J.Y. Le Boudec, M. Paolone. A composable method for real-time control of active distribution networks with explicit power setpoints. Part I: Framework. *Electric Power Systems Research*. 2015 Aug 31, pp. 254-264.
21. L. Reyes-Chamorro, A. Bernstein, J.Y. Le Boudec, and M. Paolone. A composable method for real-time control of active distribution networks with explicit power setpoints. Part II: Implementation and validation. *Electric Power Systems Research*. 2015 Aug 31, pp. 265-280.
22. D. Mills, J. Martin, J. Burbank, and W. Kasch. Network time protocol version 4: Protocol and algorithms specification, 2010.

23. IEEE Standard for a precision clock synchronization protocol for networked measurement and control systems," in *IEEE/IEC 61588:2009*, Feb. 2 2009.
24. [Precision time protocol telecom profile for frequency synchronization](#), *ITU Recommendation G.8265.1*, July 2014.
25. [Precision time protocol telecom profile for phase/time synchronization](#), *ITU Recommendation G.8275.1*, June 2016.
26. IRIG Standard 200-04 Serial Time Code Formats, September 2004.
27. [Radio Station WWVB](#), *NIST Time and Frequency Division*.
28. [Time Measurement and Analysis Service \(TMAS\)](#), *NIST Time and Frequency Division*.
29. T. Mizrahi. RFC 7384 Security requirements of time protocols in packet switched networks. 2014.
30. K. O'Donoghue. "Emerging solutions for time protocol security." *Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), 2016 IEEE International Symposium on*. IEEE, 2016.
31. [Framework for Cyber-Physical Systems](#), Release 1.0, *Cyber-Physical Systems Public Working Group*, May 2016.
32. [Cybersecurity Capability Maturity Model \(C2M2\)](#), Version 1.1, *Department of Energy*, February 2014.
33. IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Transmission and Distribution Facilities, *IEEE Std 1613.1*, Dec. 2013
34. Jiecheng Zhao, Jin Tan, Ling Wu, Lingwei Zhan, Yilu Liu, Jose R. Gracia, Paul D. Ewing. Impact of Measurement Error on Synchrophasor Applications. ORNL Technical Report.
35. Best practices for improved robustness of time and frequency sources in fixed locations. DHS US-CERT, January 6, 2015.
36. S. Bhamidipati, Y. Ng, and G. Gao, Multi-receiver GPS-based direct time estimation for PMUs, *Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2016)*, Portland OR, Sep. 2016.
37. Y. Ng and G. Gao. Advanced multi-receiver position information-aided vector tracking for robust GPS time transfer to PMUs, *Proceedings of the Institute of Navigation GNSS+ conference*, Tampa FL, Sep. 2015.
38. L. Heng, D. Work, and G. Gao. Reliability from unreliable peers: Cooperative GNSS authentication, *Inside GNSS Magazine*, Sep.-Oct. 2013.
39. P. Pradhan, K. Nagananda, P. Venkatasubramaniam, S.Kishore and R.S. Blum, "GPS Spoofing Attack Characterization and Detection in Smart Grids," *IEEE Conference on Communications and Network Security*, 2016.
40. J. Zhang, R.S. Blum, X. Lu, and D. Conus. Asymptotically optimum distributed estimation in presence of attacks, *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1086-1101, March 2015.
41. A. Karthik and R. Blum. Estimation theory based robust phase offset estimation in presence of delay attacks, arXiv preprint arXiv:1611.05117. 2016 Nov 16.
42. A. Smith, P. Evans, B. Williams, and W. Grice. Provably secure time distribution for the electric grid. *SPIE Sensing Technology and Applications* May 21, 2015.
43. [Best practices for leap second event occurring on 31 December 2016](#), DHS US-CERT, October 2016.
44. [NASPI leap second webinar](#), December 2016.
45. B. Noseworthy. Network-based application-independent time-error and direct port latency measurement. *IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, Sep 2016, pp.1-6.
46. 1588 Revision: Tool box for monitoring, <https://ieee-sa.imeetcentral.com/1588/file/43739452>.