Precision Time Technology Overview

3002007843

Precision Time Technology Overview

3002007843

Technical Update, January 2017

EPRI Project Manager

D. Von Dollen

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI), prepared this report.

Principal Investigator

D. Von Dollen

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Precision Time Technology Overview. EPRI, Palo Alto, CA: 2017. 3002007843.

ABSTRACT

Precision time is growing in utilization and importance in most power systems around the world. Utilities are using precision time for a growing number of purposes including protection relays, substation metering, other intelligent electronic devices (IEDs), digital fault recording, synchrophasor measurement and IEC 61850 process bus. A range of time sources, distribution methods, standards and technologies are being deployed. As new uses for precision time are identified, new requirements such as improved reliability, device clock stability, back-up methods, time-system monitoring and cyber security are being identified and must be addressed.

This overview provides a brief summary of the current state of the art in terms of technologies and standards used to implement precision time systems that address:

- Broadcast and distribution methods for precision time
- Time sources and scales
- Physical methods for time distribution
- Time distribution protocols and signals
- Clock mechanisms at GPS receivers, eLORAN receivers or other time references
- Alternate time sources
- Cyber security considerations

Keywords
Precision time
Time sources
Time distribution
Intelligent Electronic Device (IED)

CONTENTS

LIST OF FIGURES

1
INTRODUCTION

Background

The song lyric from the band Chicago released on their April 1969 debut album Chicago Transit Authority "Does anybody really know what time it is? Does anybody really care?" poses an interesting and relevant question. Historically, sundials were more than adequate to meet people's needs regarding time when they mainly went about their daily lives within the bounds of their farm or local town life. It wasn't until the expansion of the railroads did the need for a more uniform time become a necessity.

Railway time was the standardized time arrangement first applied by the Great Western Railway in England in November 1840, the first recorded occasion when different local times were synchronized and a single standard time applied. Railway time was progressively taken up by all railway companies in Great Britain over the following two to three years. The schedules by which trains were organized and the times station clocks displayed was brought in line with the local time for London or "London Time", the time set at Greenwich by the Royal Observatory, which was already widely known as Greenwich Mean Time (GMT).

The key purpose behind introducing railway time was twofold: to overcome the confusion caused by having non-uniform local times in each town and station stop along the expanding railway network and to reduce the incidence of accidents and near misses, which were becoming more frequent as the number of train journeys increased. [1]

In a somewhat similar way the use of precision time across the electric utility grid is growing to meet the needs of increased use of grid automation technologies. This paper will provide background on the role of precision time broadcast methods, time sources and distribution protocols employed.

Precision Time

Precision time is growing in utilization and importance in most power systems around the world. Utilities are using precision time for a growing number of purposes including protection relays, substation metering, other intelligent electronic devices (IEDs), digital fault recording, synchrophasor measurement and IEC 61850 process bus. A range of time sources, distribution methods, standards and technologies are being deployed. As new uses for precision time are identified, new requirements such as improved reliability, device clock stability, back-up methods, time-system monitoring and cyber security are being identified and must be addressed.

The generic term used by governments, the military and others to describe a system that provides precision time over a wide area is a Position, Navigation and Timing (PNT) system. Technologies such as Global Positioning System (GPS) and Enhanced Long Range Navigation (eLoran) are considered part of this landscape.

An overall precision time system can be summarized as follows; a precision time source such as the International Atomic Time (TAI) scale has a defined relationship with Universal Coordinated Time (UTC)–time (UTC-time) as maintained by National Institute of Standards and Technology (NIST) and GPS-time. GPS-time is distributed globally using the GPS infrastructure including satellites and ground stations. GPS receivers function as time references for a location or a region. To complete a precision time system, the receivers connect to end devices using signals or time distribution networks that operate on the physical methods of copper or fiber cabling and may use other network components such as routers. A range of time scales are used to represent time for different applications and locations.

In recent years the breadth and criticality of the applications of precision time have grown dramatically necessitating a greater understanding of the vulnerabilities of the existing systems such as GPS and the development of suitable back-up or alternate systems. These back-up methods or Alternate Position, Navigation and Timing (APNT) systems must be selected and deployed based on a clear understanding of requirements and risk.

The selection of the appropriate technology should follow the determination of the requirements associated with the current and anticipated applications that will use the time signal and in turn the degree of criticality of the application. The tendency is to deploy technologies including precise time systems on a project basis to address a specific need. Typically project constraints such schedules and budgets make it challenging to determine let alone address system requirements beyond the scope of the project. However a broad and longer term view of requirements can contribute to an optimized deployment plan that is highly beneficial in the future.

This overview provides a brief summary of the current state of the art in terms of technologies and standards used to implement precision time systems that address:

- Broadcast and distribution methods for precision time
- Time sources and scales
- Physical methods for time distribution
- Time distribution protocols and signals
- Clock mechanisms at GPS receivers, eLORAN receivers or other time references
- Alternate time sources
- Cyber security considerations

2

BROADCAST AND DISTRIBUTION METHODS FOR PRECISION TIME

There are several methods used to broadcast or distribute precision time. These include GPS, enhanced LORAN, radio, network time distribution and public switched telephone networks. These will be describe in the following sections.

Global Positioning System (GPS)

A space-based satellite navigation system developed and deployed by the US Department of Defense that uses approximately 30 satellites (a minimum of 24) to provide accurate time and location data. [2] The time data is used by both critical and non-critical applications for military, civilian and commercial users around the world. The satellites orbit earth at an altitude of 20,200 KM and complete two orbits approximately every 24 hours (23 hours and 56 minutes). [3] The GPS system, originally called NAVSTAR, became fully operational in 1995 and was the first to achieve global coverage. Today the system is operated and maintained by the US Air Force. Time accuracy is in the range of 10-14 nanoseconds for the satellites. However the function of receiving and interpreting the time signals by GPS receivers results in additional error and produces a typical accuracy of 100 nanoseconds to one microsecond. In May 2000 Selective Availability [3], which resulted in lower accuracy for civilian use of GPS signals, was turned off.

The generic description for the GPS system is a Global Navigation Satellite System (GNSS). Currently the only other GNSS is the Russian Global Navigation Satellite System (GLONASS) however both Europe (Galileo) and China (Beidou) are expected to deploy or expand to achieve global systems by 2020.

In terms of regional systems there are both augmentation and stand-alone systems. For example India has a satellite-based augmentation system called the GPS Aided GEO Augmented Navigation (GAGAN) system that improves the accuracy of GPS and GLONASS receivers.

The total GPS consists of three primary components; the satellites, the receivers and the control segment. The GPS satellites are synchronized to each other and the ground clocks. They are equipped with atomic clocks that are very stable. True time is maintained at the ground clocks and any drift by the satellite clocks is automatically corrected. Coarse Acquisition (C/A) code is provided for the civilian GPS service (SPS) and the Precise (Y) or P(Y) code is encrypted for the military GPS service (PPS). Military GPS service utilizes two frequencies (L1 and L2) to improve accuracy by compensating for unpredictable ionospheric delays whereas civilian users initially received one frequency. [3] The latest GPS satellites now offer more frequencies for civilian users as well. The GPS receivers require line of sight access to at least four satellites to derive accurate location and time data. The receivers include clocks that are less stable than the satellites but are typically capable of an accuracy of at least 1 microsecond by computing the exact location of the receiver and the deviation from true time. The third component is the GPS Control Segment which is a distributed network of master stations (2), command and control antenna (11) and monitoring sites (15). The purpose of the Control Segment is to track the satellites, send control commands and other data, monitor and assess transmissions and analyze a range of factors.

Although research has identified some weather fronts as a possible source of positioning error, the system functions well in most terrestrial weather conditions with only minor signal attenuation. However space weather resulting from solar activity such as geomagnetic storms can significantly disturb the earth's ionosphere and interfere with the ability of the receivers to maintain lock on the satellite signal. [4] For this reason as well as the occasional need for the GPS to be taken off-line for maintenance purposes, the risk of jamming or spoofing, [5] [6] the impacts of US military testing [7] and the possibility of EMP events, GPS deployments for critical applications must incorporate back-up precision time sources and/or extended hold-over capabilities.

GPS augmentation refers to the use of additional technologies to improve accuracy, timing, availability and/or integrity. Many different augmentation systems have been developed for national and international non-military users to address a wide range of application requirements. For example NASA developed the Global Differential GPS (GDGPS) to provide highly accurate position, timing and other data for NASA science missions. A number of augmentation systems deliver higher GPS accuracy than the military GPS service. [3]

The US government has continuously invested to modernize the GPS. Generations of satellite and associated ground technologies are referred to as "Blocks" with Block IIA being launched in 1990 to 1997 and the last IIA satellite decommissioned in 2016. Following Block IIA were Block IIR, Block IIR(M) and Block IIF. The last of the Block IIF series was launched in 2016. An image of a Block IIF satellite is shown in Figure 2-1. Successive blocks provided improved performance, power, additional civilian frequencies, improved military capabilities and longer life. Beginning with Block IIR(M) additional civilian frequencies are broadcast to enable improved accuracy by allowing receivers to compensate for unpredictable ionospheric delays. Previous generations of satellites broadcast only single frequencies for civilian use. The latest generation is GPS III with launches planned starting in 2017.

Figure 2-1
Image of a Block IIF Satellite [8]

eLoran (enhanced LORAN)

A land-based navigation system that uses low frequency radio signals broadcast by transmitters at fixed positions to determine the location of stationary or moving receivers. The system was first introduced in 1943 with an objective to operate over long distances and provide highly accurate location data. Early applications included the air force and the navy during World War 2. [9] The term LORAN is short for long range navigation. The US Coast Guard changed the name to use lower-case letters when it assumed its mandate with Loran-A and changed its name to Loran-B. [10]

Years later Loran-C became the primary means of navigation in much of the Western world including the Pacific and Atlantic regions. However once civilian access to navigation satellites was permitted in the 1990s, the use of Loran-C dropped dramatically. The US and Canada turned off their Loran-C systems in 2010 and Europe followed in 2015. Just as these Loran-C systems were being de-commissioned, multiple events impacting the reliability of GPS occurred including a growing incidence of intentional and unintentional signal jamming. [5] [6] This has resulted in a new awareness of the need for a complementary back-up to GPS for critical applications and a fresh look at Loran as a possible back-up solution.

Loran operates on the principle of the difference in the time of reception of a signal from a transmitter being constant along a hyperbolic curve. In order to determine its location a Loran receiver must acquire signals from at least three transmitters. Loran systems are deployed in regional arrays or chains that include a primary station and two or more secondary stations.

At this time, industry consensus and US government guidance [11] [12] point to eLoran as the best option currently available for an APNT system. The eLoran system is suitable as a back-up mechanism because of its independent infrastructure, strong signal and difficulty in jamming. [6] [5] Investments already made in upgrading the Loran-C infrastructure will support future deployments of eLoran. [11] By further upgrading both the transmission system components and the receiver designs, eLoran provides improved accuracy and other key performance metrics. These improvements enable the performance of eLoran to approximate the performance of civilian GPS without augmentation (unaugmented).

In 2016 NIST announced its intention to fund development of a microchip version of an eLoran receiver which would facilitate easier integration into a range of system types. [13] Also in 2016 South Korea awarded a contract to deploy eLoran as an APNT system through 2019. The initiative is in response to reported GPS signal interference by the North Koreans in March 2016. [14]

Refer to Figure 2-2 for an example of a receiver that integrates GPS signals onto an eLoran monitoring system.

Figure 2-2
Example eLoran Monitoring System that Integrates GPS Signals

Standard Radio (WWV, WWVB, CHU)

Short-wave and long-wave radio stations have existed since the 1920s in the US and Canada for the purpose of disseminating time information. In the US, stations with the call letters WWV (short-wave), WWVH (Hawaii) and WWVB (long-wave) are operated by NIST. The stations broadcast frequency and time data using carrier frequencies such as 2.5, 5, 10, 15 and 20 MHz as well as voice for time (only). The NIST stations are located in Fort Collins, CO and use atomic clocks that are linked to NISTs primary time standard in Boulder, CO. Similar stations and capabilities exist in Canada (CHU) and Germany (DCF). [15]

These radio signals are not used by power utilities or other applications that require accurate time as the signals are not compensated for transmission path delays. In addition the signals are significantly impacted by the corona noise present near high-voltage equipment and signals in the High Frequency (HF) bands which are also subject to space weather (ionospheric) impacts.

Network Time Distribution

Another broadcast method for precision time is an Ethernet network that delivers the time and frequency data using one of a number of time distribution protocols such as Network Time Protocol (NTP) or IEEE 1588-2008 Precision Time Protocol (PTP). These protocols are described in a separate section of this report. Another network option uses Time Division Multiplexing (TDM) based on Synchronous Optical Network (SONET). The time itself originates from a single or multiple highly accurate and stable clocks such as NIST's F2 cesium atomic [16] clock in Boulder, CO and uses a time scale such a UTC.

There are numerous advantages cost savings that come from using a network for time distribution. Multiple time sources can be integrated and at the same time fewer clocks are required. The time network will likely run on hardware and cabling that already exists with the result that devices can be time synchronized and communicate using a single Ethernet cable. Even if one time source such as GPS is lost, the specific time distribution system itself will be able to remain synchronized although there may be errors relative to absolute time. Another important aspect is the immunity to vulnerabilities associated with radio signals including weather (terrestrial or space), jamming or spoofing.

In order for an Ethernet network to distribute time information, precise time managed switches are used to provide important features such as network data prioritization (QoS), traffic management (VLAN) and overload avoidance (IGMP snooping). These types of features are already included in the Ethernet switches for typical substation networks so new hardware may not be needed. User Datagram Protocol (UDP) is the network protocol used by NTP and PTP due to its ability to keep data flowing albeit with the periodic loss of packets. In the case where PTP is used there are two options; software-only and hardware-aided. Hardware-aided PTP deployments are able provide accuracies of 20 to 100 nanoseconds but require the use of additional components including a PTP Grandmaster, PTP Switches (with transparent clock) and PTP Switches (with boundary clock). Figure 2-3 shows a small time distribution network using PTP. The software-only option can operate on a typical network without additional hardware and provide an accuracy of 10 to 100 microseconds.

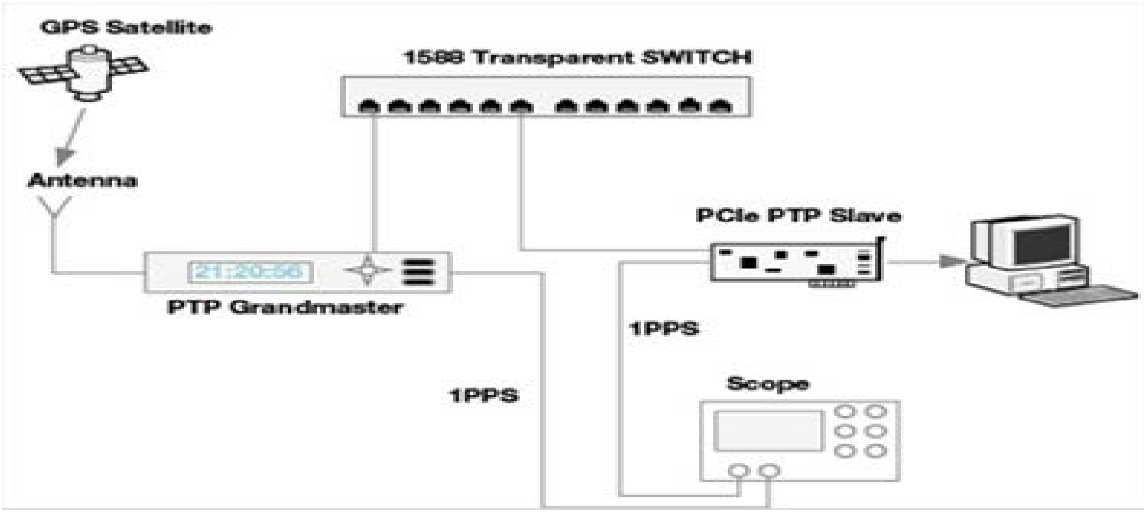

Figure 2-3
A Small PTP Distribution Network [17]

Public Switched Telephone Network, Voice (PSTN Voice)

Time information is provided using conventional dial-up telephone services as tone signals or voice announcements or both. Accuracy is impacted by the lack of determinism and the method of broadcasting information without path delay measurement and correction. Typical accuracies are 30 milliseconds for calls within North America and 250 milliseconds for international calls. Computer hardware/software and dial-up modems are needed with this approach.

Public Switched Telephone Network, Data (PSTN Data)

This system provides time information using tone signals similar to the PSTN Voice system mentioned above. Typical accuracies without interaction are 30 milliseconds for calls within North America and 250 milliseconds for international calls. By implementing an interactive capability multiple time messages can be used to measure path delay and calculate the needed correction. In addition the communications paths are often repeatable in the short-term. These differences can result in accuracy improvements to 15 milliseconds. Computer hardware/software and dial-up modems are needed with this approach.

3

TIME SOURCES AND SCALES

Extremely accurate and stable time sources provide the single central origin of time that is distributed across a precision time system. The central source enables time to be accurately correlated and compared across a local or wide area system. The global time community is led by the International Bureau of Weights and Measures (BIPM) [18] which is based in Sevres, France and which developed and maintains the TAI scale. The TAI system is comprised of approximately two hundred networked atomic clocks around the world that are maintained by national standards labs such as National Institute of Standards and Technology (NIST), the United States Naval Observatory (USNO), and the National Research Council (NRC) in Canada. The long-term stability of TAI is established by careful weighting of the networked clocks. GPS-time is managed by the USNO while NIST manages UTC (NIST). The USNO and NIST have an agreement to ensure that the difference between GPS-time and UTC (NIST) is less than 100 nanoseconds. [19] NIST's time standard clock is located in Boulder, Colorado.

TAI is a highly stable and consistent time scale which by definition does not keep in step with the slightly irregular rotation of the earth, measured as astronomical or mean solar time. However for practical reasons we need a scale that does keep in step with the earth's rotation. Coordinated Universal Time (UTC) upon which civil time is based is the primary global scale that addresses these practical needs. UTC tracks the TAI except that a leap second is added as necessary to ensure alignment within one second of the earth's rotation on an average annual basis. As of July 2015 UTC is 36 seconds behind TAI. [20] Since UTC was established first it is further behind TAI than the other time scales. GPS and Loran time are also set as fixed values relative to TAI.

During periods when leap seconds are added to UTC, GPS receivers may show an incorrect UTC time until they receive the new UTC offset message. This can also affect new receivers which must receive an offset message before operating. Currently UTC is 17 seconds behind GPS time. Protocols for communicating time such as PTP (based on IEEE STD 1588v2) can be used to distribute both TAI and UTC time however native time for 1588 is TAI.

Local precise time is based on UTC but adjusted to the local time zone and may include adjustments for daylight savings time as well. Although the time may be accurate the time zone adjustments make wide-area time correlations more difficult as a result working groups with the IEEE PSRC recommend the use of UTC without local time adjustments for utilities. [21] NERC is less specific but PRC-018-1 implies the best approach is UTC without local time adjustments. [22]

4

TIME DISTRIBUTION PROTOCOLS AND SIGNALS

The role of time distribution protocols and signals is to deliver time data and messaging to the end devices in the time distribution system. An overall precision time system can be summarized as follows; a precision time source such as TAI has a defined relationship with the NIST UTC-time and GPS-time. GPS-time is distributed globally using the GPS infrastructure including satellites and ground stations. GPS ground stations become time references for the satellite clocks which are also extremely stable. GPS receivers function as time references for a location or a region. To complete a precision time system, the receivers connect to end devices using signals or time distribution networks that operate on the physical methods of copper or fiber cabling and may use other network components such as routers. A range of time scales are used to represent time for different applications and locations.

Three categories of protocols and signals can be identified:

- Non-network time signals and protocols
- Network time protocols
- Time synchronization features of SCADA protocols (may be serial or network)

Non-network Time Signals and Codes

- **One Pulse per Second (1PPS) signal** [15] – capable of providing an accuracy of ~100 nanoseconds. The first distribution method available for precision time. The 1PPS signals only include time data so a secondary communications channel is needed to provide time of day and date.
- **Inter-Range Instrumentation Group time code (IRIG) – Code B – Modulated –** capable of providing an accuracy of ~10 microseconds to 1 millisecond. Code includes time of day and an "on-time" mark.
- **Inter-Range Instrumentation Group time code (IRIG) – Code B – Unmodulated –** capable of providing an accuracy of ~10 nanoseconds to 1 microsecond. Code includes time of day and an "on-time" mark.
- **Inter-Range Instrumentation Group time code (IRIG) – Code B – Modified Manchester Modulation** – also referred to as the IRIG-B High Precision Time Code Format [23] – capable of providing an accuracy of ~10 nanoseconds to 1 microsecond. Code includes time of day and an "on-time" mark.
- **IEEE STD 1344-1995 defined extensions to IRIG-B** [15] – extension to the IRIG-B code to provide local offset, time quality, leap second, year and seasonal time changes. The extension also defined a "modified" Manchester encoding method. Many of these capabilities have since been added to the IRIG-B standard.

Network Time Protocols

- **Network Time Protocol (NTP) –** capable of providing an accuracy of ~1 millisecond to 50 milliseconds. Better accuracies may be possible with small local networks. Systems consist of time reference sources and one or more time servers on the network. Servers may also exist elsewhere on the network. Figure 4-1 shows a simplified system of time distribution using NTP or SNTP.

- **Simple Network Time Protocol (SNTP)** – runs on the same time network using the same time packet as NTP. The "simple" in SNTP refers to the algorithm running on the remote platform. An SNTP time algorithm uses a much simpler method for error checking and clock speed adjustments. The expected accuracy is less with SNTP than with NTP.
- **IEEE STD 1588 – 2008 – IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems –** also known as Precision Time Protocol Version 2 (PTPv2). Defines software-only and hardware-augmented methods that operate on an Ethernet network. Software-only deployments are capable of providing an accuracy of ~10 microseconds to ~100 microseconds. Hardware-aided deployments are capable of providing an accuracy of ~20 nanoseconds to ~100 nanoseconds and require the use of a PTP Grandmaster clock, PTP Switches (with transparent clock) and PTP Switches (with boundary clock). Figure 4-2 shows time distribution using PTP.
- **IEEE STD C37.238-2011** – **IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications –** a defines a selection of the capabilities of IEEE STD 1588-2008 for precise time applications for power systems. Also adopted as a dual-logo standard by the IEC using the designation 61850-9-3.

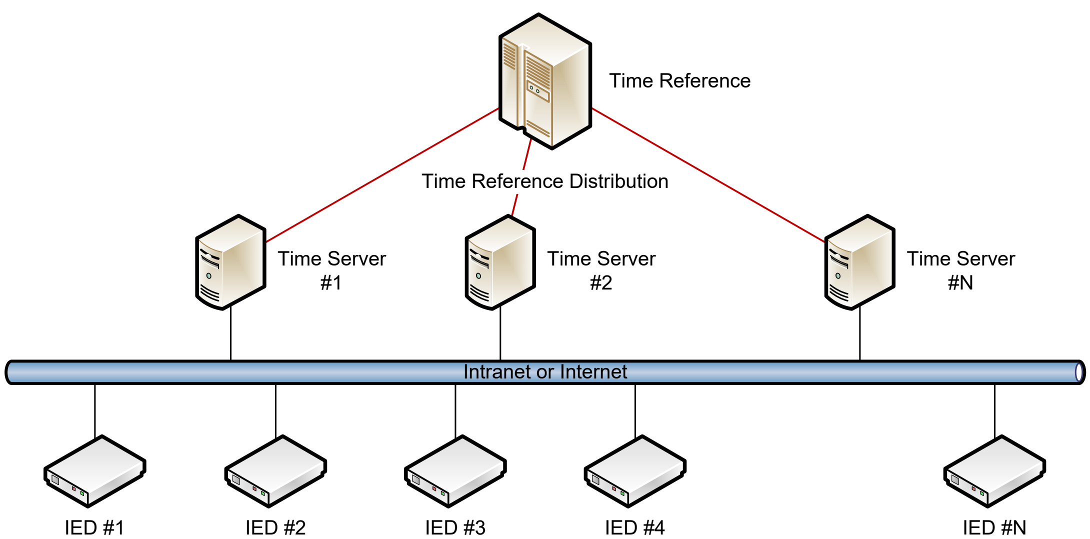

Figure 4-1
Time Distribution using NTP or SNTP [19]

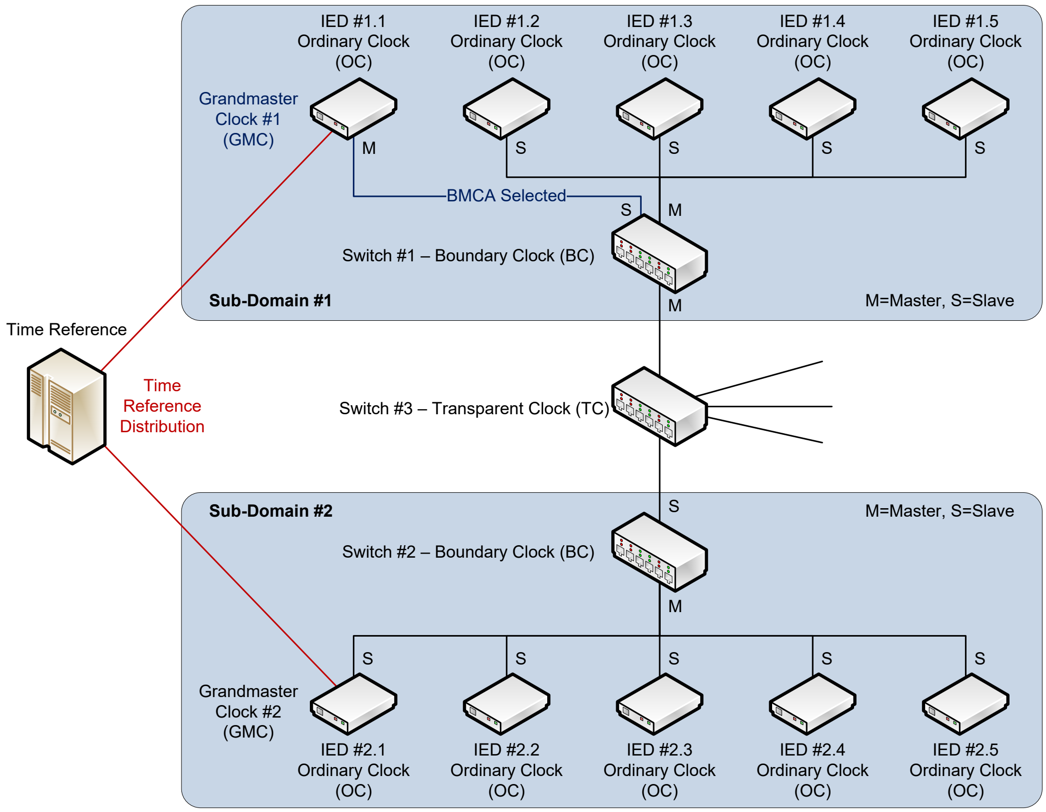

Figure 4-2
Time Distribution using PTP (IEEE STD 1588) [19]

- **IEEE STD C37.118-1 – 2005** – incorporates the extensions to IRIG-B defined in IEEE STD 1344-1995 plus a change in the sign for the local time offset. [23] Standard supports serial and network implementations although network methods are most common. [24]
- **IEEE STD C37.118-1 – 2011** – incorporates the extensions to IRIG-B defined in IEEE STD 1344-1995 plus a change in the sign for the local time offset plus a continuous time quality code. [23] Standard supports serial and network implementations although network methods are most common. [24]
- **IEC 61850 methods for precision time** – initially NTP was specified for time distribution. However NTP did not meet the requirements for precision as stated in IEC 61850-5, IEC 61850-9-2 and IEC 61869-9. PTP is now the specified solution for precision time (IEC 61850-9-3 published May 2016).

Time Synchronization Features of SCADA Protocols

- **IEEE STD 1815 – 2012 (DNP3)** – supports serial and network implementations. Has been using UTC time since January 1, 2008. Capable of providing an accuracy of ~1 millisecond to 10 milliseconds depending on the consistency of the outbound and inbound path delays and the stability of the local clock. Requires that the master station has access to a reference source for time and is communicating using DNP3.

5
CLOCK MECHANISM(S) AT GPS RECEIVERS, ELORAN RECEIVERS AND OTHER TIME REFERENCES

Precision time references function as the local or regional representation of time that originates from a central source such as NIST – UTC which is linked to TAI. These time references may be GPS receivers, eLoran receivers, integrated GPS and eLoran receivers or receivers of other time signals. By far the most common are GPS receivers receiving GPS-time which is administered by the USNO.

GPS receivers communicate with multiple (minimum of 3) satellites which themselves contain extremely accurate atomic clocks. By acquiring time estimates using multiple satellites and correction estimates from GPS ground stations, the receiver is able to determine time within a specified accuracy. This time is then used to discipline an integrated oscillator which becomes the local time reference. Therefore the stability of the integrated oscillator is an important determinant in the stability and accuracy of the GPS receiver in the event of loss of the GPS signal. The term “hold-over” specifies the ability of the oscillator in the GPS receiver to hold accurate and stable time upon this signal loss.

Types of integrated oscillators (approximately) in order of increasing stability and cost:

- Quartz crystal oscillator (XO)
- Temperature compensated oscillator (TCXO)
- Oven (temperature) controlled oscillator (OCXO)
- Rubidium (atomic) oscillator
- Cesium (atomic) oscillator

6 ALTERNATE (APNT) TIME SOURCES

In recent years the breadth and criticality of the applications of precision time have grown dramatically driving a better understanding of the vulnerabilities of the existing systems such as GPS/GNSS and the development of suitable back-up or alternate systems. These back-up methods or Alternate Position, Navigation and Timing (APNT) systems must be selected and deployed based on a clear understanding of requirements and risk. An over-arching principle is avoiding the risk of a single point of failure which is a basic and common requirement for critical systems.

The need for and type of APNTs is determined by the degree and nature of risk to be mitigated. Risk can be defined as the multiple of the degree of impact of a failure and the probability of such an occurrence. In the context of a PNT, system risk[1] can be assessed at a minimum by:

- The degree of criticality of the application considering the impact of a timing error or an outage of a given duration.
- The probability of an outage or error event which is based on the vulnerabilities and their nature.

If the risk assessment concludes that investment in APNT technology is or may be warranted then gaining a deeper understanding of the requirements, the available technologies and their vulnerabilities is a logical next step. A good APNT solution will exhibit complementary strengths and vulnerabilities. Other mitigation approaches should also be considered. For example devices that use time can monitor the rate of time adjustments over time to detect possible spoofing. Another example might be to use higher quality oscillators in the local time references to extend the hold-over capability in the event of loss of the time source signal.

Example Vulnerabilities and Challenges with GNSS

- "GPS is prone to errors caused by such issues as atmospheric refraction, multipath, shifts in satellite orbits (ephemeris error), satellite geometry effects, satellite clock errors and calculation errors. Ground stations throughout the world monitor the satellites to ensure that these errors are minimized. Most errors can be calculated and eliminated (or at least greatly minimized) once a receiver is tracking at least four satellites." [19]
- Space weather such as X-ray emissions from the sun can significantly disturb the earth's ionosphere and interfere with the ability of the receivers to maintain lock on the satellite signal. [4]
- Antenna location and sky-view obstruction issues
- RF interference from nearby transmitters such as cell towers

[1] For additional information consider EPRI reports 1024422: "Draft Risk Assessment Processes" and 10424423 "Risk Mitigation Strategies."

- Ambiguity in time due to leap second adjustments. This occurs for a short period every few years. Impact is negligible for many applications but a one second error would have a serious impact for synchrophasor applications.
- Occasional need for the GPS to be taken off-line for maintenance purposes
- Risk of jamming or spoofing [5] [6]
- Impacts of US military testing [7]
- Possibility of an EMP event
- Kinetic or laser attacks on satellites [25]
- Collisions with space debris
- An example of a GPS timing error occurred in January 2016. The US Air Force reported the following:
  - "This change occurred when the oldest vehicle, SVN 23, was removed from the constellation [of GPS satellites orbiting Earth]……….investigation revealed an issue in the global positioning system ground software ……..," a spokesperson for the USAF 50th Space Wing at Schriever Air Base, Colorado said.
  - "………….. the coordinated universal time (UTC) timing signal was off by 13 microseconds which exceeded the design specifications. …………global users may have experienced GPS timing issues for several hours." [26]

Complementary APNT Technologies

- **Network time distribution –** If one time source such as GPS is lost, the specific time distribution system itself will be able to remain synchronized even if there is error relative to absolute time. In addition, network distribution is immune to some of the vulnerabilities associated with radio signals including weather (terrestrial or space), jamming or spoofing. Note however that PTP does not currently define a normative cyber security requirement or method. Several proposals are being considered by the IEEE working group that is updating IEEE STD 1588-2008.
- **eLoran –** At this time, industry consensus and US government guidance [11] [12] point to eLoran as the best option currently available for a complementary wide area APNT system. eLoran is suitable as a back-up mechanism because of its independent infrastructure, strong signal and difficulty in jamming. [5] In 2016 South Korea awarded a contract to deploy eLoran as an APNT system through 2019. The initiative is in response to reported GPS signal interference by the North Koreans.

7
CYBER SCURITY CONSIDERATIONS

The use of PNT systems has grown to the point where as of 2016 there were an estimated 3.5 to 4 billion users around the world (growing approximately 800 million per year). [27] [28] The range of user types has also increased substantially, growing beyond the original military applications to include many industries such as utilities, telecommunications, air transportation and agriculture as well as 100's of millions of smart phone users. Civilian applications range from the simple to the sophisticated such as synchrophasor measurement and from the cursory to the critical such as aircraft landing systems. In the midst of this growth there are increasing incidents of both intentional and unintentional interference with PNT systems, especially GNSS, which can block access to precision time data. The probability of cyber incidents is also on the rise for network distribution of time however this has been less common.

A new threat for GNSS systems is signal interference by small GPS-Jammers that are inexpensive and easily obtainable yet powerful enough to disrupt GPS signals for up to 16 KM. [6] Small jamming devices like this disrupted GPS (augmentation) signals at the Newark airport in 2010 and 2012. [27] An example of intentional jamming occurred when the North Koreans toward the South which has occurred multiple times in recent years. In March 2016 GPS jamming signals originating from five locations along the South/North Korean border, interrupted signal reception by an estimated 110 South Korean ships and aircraft. In response South Korea are investing in a large eLoran system to function as an APNT. [14] [6] It is reasonable to assume that interference issues will become more common as more devices capable of signal interference become publicly available.

Example Vulnerabilities for PNT Systems

- Spoofing – is the intentional transmission of a false GNSS signal at a somewhat higher power to deceive the GNSS receiver into locking onto the false signal. The false signal is then gradually adjusted to provide incorrect position, navigation or time data. [29] A spoofing attack can be difficult but not impossible to detect.
- Jamming – is signal interference (intentional) of a GNSS satellite signal.
- Meaconing – is the intentional capture, delay and retransmission of a GNSS signal for the purpose of introducing errors to a GNSS receiver.
- Older versions of NTP nor SNTP do not define security mechanisms.
- PTPv2 does not currently define a normative cyber security requirement or method. Several proposals are being considered by the IEEE working group that is updating IEEE STD 1588-2008. The "experimental" content in Annex K of the standard is considered to be inadequate.
- Networks carrying time messages can be severed or hacked.

Example Technology Solutions

The focus of this section is technologies and standards solutions to address cyber security related vulnerabilities. In addition there is increasing engagement by policy makers and law enforcement officials.

- Interference resistant GNSS receivers.
- Multi-GNSS receivers which have the capability of receiving GNSS signals in addition to GPS. Examples are GLONASS (Russia), Galileo (Europe) and BeiDou (China). [28] It is far more difficult to spoof a multi-GNSS receiver. Another term used for this is Global PNT System-of-Systems (GPSS).
- GNSS interference detection, location and reporting system. May use fixed or portable instruments.
- RF environment monitoring around key GNSS receivers.
- APNT such as eLoran.
- Receivers that integrate GPS and eLoran signals. Refer to Figure 2-2 for an example of this.
- Local APNT solutions such as Locata.
- Network circuit isolation. IEC 62351-6 recommends that VLANs be used to provide confidentiality for information exchange. The requirement for IEEE Standard C37.238 messages to be IEEE Standard 802.1Q compliant enables this approach.
- The following is an abbreviated list of recommended standards for cyber security that apply to network communications for power utilities:
  - IEC 62351 describes recommended security profiles for various communications media and protocols.
  - IEEE STD 1815-2012 (DNP3) – secure authentication version 5
  - NERC CIP 002-009 establishes NERC cyber-security standards
  - IEEE STD 1686-2013 describes security measures from the perspective of an IED (intelligent electronic device)
  - IEEE STD C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection and Control Systems.
  - IEEE STD 1402-2000 (reaffirmed in 2008 and now being updated) - IEEE Guide for Electric Power Substation Physical and Electronic Security
  - IEEE 802 series – applicable parts
  - IEC 62443 on security for industrial process measurement and control
  - NIST Special Publication (SP) 800-53 are guidelines for federal information systems
  - FIPS 199 and FIPS 200 are the foundation of system classifications
  - NIST FIPS 140-2 Cryptographic Security
  - IETF RFC 6272 Internet Protocols for the Smart Grid

8
CONCLUSIONS

Uniform time has had an important role since the earliest scheduled railway operations in England began to use a single standard time and different local times that were synchronized. Fast forward to today and we have GNSS offering precise time with microsecond resolution that is used by billions of people in every corner of the globe.

Precision time has many purposes in the modern electric utility including protection relays, substation metering, other IEDs, digital fault recording, synchrophasor measurement and IEC 61850 process bus. A range of time sources, distribution methods, standards and technologies are being deployed. As new uses for precision time are identified, new requirements such as improved reliability, device clock stability, back-up methods, time-system monitoring, APTNs and cyber security are being identified and must be addressed.

An overall precision time system can be summarized as follows; a precision time source such as TAI has a defined relationship with the NIST UTC-time and GPS-time. GPS-time is distributed globally using the GPS infrastructure including satellites and ground stations. GPS ground stations become time references for the satellite clocks which are also extremely stable. GPS receivers function as time references for a location or a region. To complete a precision time system, the receivers connect to end devices using signals or time distribution networks that operate on the physical methods of copper or fiber cabling and may use other network components such as routers. A range of time scales are used to represent time for different applications and locations.

Much has been accomplished with today's broad and rapid utilization of precision time. However we have reached the point where PNT systems are a critical albeit less visible infrastructure that is taken for granted. Military technology specialists and industry participants are now keenly aware that even a temporary loss of a portion of this infrastructure can cause significant disruption in critical applications. Longer and/or broader interruptions could impact many areas of our economy. The increasing occurrence of GNSS jamming and a recent demonstration of GPS spoofing have brought focus on cyber security needs. From a system perspective, a GPS receiver often presents a single point of failure. This awareness coupled with inherent vulnerabilities of GNSS such as space weather is driving a push for APNT systems.

9
REFERENCES

[1] “Railway time,” Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Railway_time. [Accessed 22 06 2016].

[2] “What is a GPS?,” Library of Congress, [Online]. Available: http://www.loc.gov/rr/scitech/mysteries/global.html. [Accessed 18 May 2016].

[3] “GPS.gov,” US Air Force, [Online]. Available: http://www.gps.gov/systems/gps/. [Accessed 02 June 2016].

[4] “Space Weather and GPS Systems,” NOAA (US National Oceanic and Atmospheric Administration), [Online]. Available: http://www.swpc.noaa.gov/impacts/space-weather-and-gps-systems. [Accessed 18 May 2016].

[5] J. Palmer, “Sat-nav systems under growing threat from 'jammers',” BBC News, 23 02 2010. [Online]. Available: http://news.bbc.co.uk/2/hi/science/nature/8533157.stm. [Accessed 27 05 2016].

[6] National Space-Based Positioning, Navigation and Timing (PNT) Advisory Board, “Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures,” National Space-Based Positioning, Navigation and Timing (PNT) Advisory Board, 04 11 2010. [Online]. Available: http://www.gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf. [Accessed 28 05 2016].

[7] G. Matt Novak, “Cancelled? FAA Warns of GPS Outages This Month...............,” Resilient Navigation and Timing Foundation, [Online]. Available: http://rntfnd.org/2016/06/08/faa-warns-of-gps-outages-this-month-during-mysterious-tests-on-the-west-coast-gizmodo/. [Accessed 10 06 2016].

[8] “Boeing Image Gallery,” Boeing, [Online]. Available: http://boeing.mediaroom.com/image-gallery?s=20291&searchform=2&mode=gallery&view=search&cat=&keywords=gps. [Accessed 02 06 2016].

[9] D. a. W. Halford, in *History of LORAN*, MIT Radiation Laboratory, pp. 19-23.

[10] US Coast Guard, “LORAN-C General Information,” 04 08 2010. [Online]. [Accessed 01 06 2016].

[11] GPS.gov, “LORAN-C Infrastructure & E-LORAN,” GPS.gov, [Online]. Available: http://www.gps.gov/policy/legislation/loran-c/. [Accessed 28 05 2016].

[12] D. A. Davis, “PNT ExCom Backs eLoran as a Step to Full GPS Backup System,” Inside GNSS, 10 12 2015. [Online]. Available: http://www.insidegnss.com/node/4760. [Accessed 28 05 2016].

[13] NIST, “Will Fund eLoran on a Chip - NIST,” Resilient Navigation and Timing Foundation, 11 02 2016. [Online]. Available: http://rntfnd.org/2016/02/11/will-fund-eloran-on-a-chip-nist/. [Accessed 10 06 2016].

[14] BBC News, “North Korea 'jamming GPS signals' near South border,” BBC News, 01 04 2016. [Online]. Available: http://www.bbc.com/news/world-asia-35940542. [Accessed 16 06 2016].

[15] Dickerson, “Substation Time Synchronization,” *PAC World,* no. Summer 2007, 2007.

[16] NIST, “NIST Launches a New U.S. Time Standard: NIST-F2 Atomic Clock,” NIST, 03 04 2014. [Online]. Available: http://www.nist.gov/pml/div688/nist-f2-atomic-clock-040314.cfm. [Accessed 30 05 2016].

[17] M. Korreng, “IEEE-1588 precision time protocol synchronisation,” End Run Technologies, [Online]. Available: http://www.iebmedia.com/index.php?id=9752&parentid=63&themeid=255&hft=78&showdetail=true&bb=1. [Accessed 02 06 2016].

[18] BIPM, “International Atomic Time,” BIPM - International Bureau of Weights and Measures, [Online]. Available: http://www.bipm.org/en/bipm/tai/tai.html. [Accessed 10 06 2016].

[19] IEEE PES Substations Committee, “IEEE P2030.101 Draft 9 - Guide for Designing a Time Synchronization System for Power Substations,” IEEE Standards Assocation, Piscataway, NJ, 2016.

[20] IERS, “Overview of the IERS,” IERS - International Earth Rotation and Reference Systems Service, [Online]. Available: https://www.iers.org/IERS/EN/Home/home_node.html. [Accessed 10 06 2016].

[21] IEEE PES PSRC WG I11, “Event Reconstruction Using Data from Protection and Disturbance Recording IEDs,” IEEE PES PSRC, 09 04 2008. [Online]. Available: www.pes-psrc.org/Reports/I11_Report_FINAL_080409.doc. [Accessed 01 06 2016].

[22] NERC, “Project 2007-11 Disturbance Monitoring,” NERC, 13 11 2014. [Online]. Available: http://www.nerc.com/pa/Stand/Pages/Project_2007-11_Disturbance_Monitoring.aspx. [Accessed 02 06 2016].

[23] IEEE, “IEEE Std C37.118.1-2011 IEEE Standard for Synchrophasor Measurement for Power Systems,” IEEE, Piscataway, NJ, 2011.

[24] IEEE, “IEEE Std C37.118.2-2011 IEEE Standard for Synchrophasor Data Transfer for Power Systems,” IEEE, Piscataway, NJ, 2011.

[25] M. a. Kaag, “Threats to Global Navigation Satellite Systems,” Marine Link, 05 2015. [Online]. Available: http://magazines.marinelink.com/Magazines/MaritimeReporter/201505/content/navigation-satellite-systems-491869. [Accessed 06 2016].

[26] J. Saarinen, “Satellite failure caused global GPS timing anomaly,” itnews, 28 01 2016. [Online]. Available: http://www.itnews.com.au/news/satellite-failure-caused-global-gps-timing-anomaly-414237#ixzz3yalTVL1Y. [Accessed 26 05 2016].

[27] B. Parkinson, “Assured PNT for our Future: PTA,” GPS World, 01 09 2014. [Online]. Available: http://gpsworld.com/assured-pnt-for-our-future-pta/. [Accessed 06 2016].

[28] D. Jewell, “In defense of PNT: Multi-GNSS to the rescue,” GPS World, 11 05 2016. [Online]. Available: http://gpsworld.com/in-defense-of-pnt-multi-gnss-to-the-rescue/. [Accessed 06 2016].

[29] Q. 3. U. T. Lin and Qing, “GPS Spoofing,” in *DEF CON 23* , Las Vegas, NV, 2015.

[30] NIST - Amelot et al., “Towards Timely Intelligence in the Power Grid,” in *44th Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting*, Gaithersburg, MD, 2013.

[31] NIST - Weiss et al., “NIST Technical Note 1867 - Time-Aware Applications, Computers, and Communication Systems (TAACCS),” NIST, Gaithersburg, MD, 2015.

[32] UrsaNav, “eLoran,” UrsaNav, [Online]. Available: http://www.ursanav.com/solutions/technology/eloran/. [Accessed 27 05 2016].

[33] LeapSecond.com, “LeapSecond.com - GPS Clock,” LeapSecond.com, [Online]. Available: http://www.leapsecond.com/java/gpsclock.htm. [Accessed 20 06 2016].

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002007843

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com