Implementing a Terrestrial Timing Solution: Best Practices

Center for Alternate Synchronization and Timing (CAST)

July 2025

Prepared by:
OAK RIDGE NATIONAL LABORATORY
and
U.S. DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY

OAK RIDGE National Laboratory

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ATSC	Advanced Television Systems Committee
BPS	Broadcast Positioning System
CAST	Center for Alternative Synchronization and Timing
CVS	Common View Signal
DOCXO	Double Oven-Controlled Crystal Oscillator
ePRC	Enhanced Primary Reference Clock
GMC	Grand Master Clock
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronic Engineers
INL	Idaho National Laboratory
IP	Internet Protocol
IT	Information Technology
ITU	International Telecommunications Union
MSCVDC	Multi-Source Common View Disciplined Clock
NAB	National Association of Broadcasters
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCXO	Oven-Controlled Crystal Oscillator
ORNL	Oak Ridge National Laboratory
OT	Operational Technology
OTN	Optical Transport Network
PMA	Power Marketing Administrations
PNT	Positioning, Navigation, and Timing
PTP	Precision Time Protocol
RSU	Remote Synchronization Unit
SatCom	Satellite Communications
SCADA	Supervisory Control and Data Acquisition
SePRC	Super Enhanced Primary Reference Clock
TWSTFT	Two-Way Satellite Time and Frequency Transfer
UTC	Coordinated Universal Time
WAS	Wide-Area Synchronization

ABSTRACT

This document is an overview and guide on the concept of precision time and how an alternative terrestrial timing solution to the Global Positioning System (GPS) can be implemented. A set of recommendations and best practices, derived from research at Oak Ridge National Laboratory, across industry, and within the US government are provided to enable implementation of a system of precision timing and synchronization to support resilient operations for the US grid. Precision time is a fundamental necessity for operating the grid today, and it becomes even more important as the grid modernizes with distributed energy resources, microgrids, and precision sensors placed throughout the grid system to ensure failure-resistant operations. The Global Navigation Satellite System (GNSS), which includes GPS, is currently the primary provider of precision timing. A terrestrial-based system for time delivery and synchronization to augment GPS is outlined in this document. It provides secure time, synchronized with Coordinated Universal Time (UTC), in the event of outages or other interruptions associated with time delivery.

1. THE TIMING SYSTEM OPERATION AND ITS COMPONENTS

1.1 INTRODUCTION TO PRECISE TIME

The explicit purpose of this fit-for-use grid network is to deliver a wide-area synchronization (WAS) capability with precise traceability to Coordinated Universal Time (UTC) to US Power Marketing Administrations (PMAs), Defense Critical Electrical Infrastructure, and industry for the support of critical infrastructure and grid reliability, resilience, and security. Additionally, this work will enable the creation of a closed-loop network environment within the timing signal communications chain, reducing cyber vulnerabilities and the opportunity for man-in-the-middle attacks. Thus, the goal is to create a complementary timing capability that can support WAS across multiple geographic regions to ensure coordinated and continuous operations.

Precise time needs to be distributed to many end points in an operating utility. Many other operational technology (OT) systems supporting bulk power, distribution, and transmission rely on precise and synchronized time to perform their function at precisely the same instant, such as:

- Supervisory control and data acquisition (SCADA) systems.
- Protective relays.
- In-band and out-of-band networks supporting grid infrastructure.
- Modern and legacy smart grid sensors [1].

The inherent time synchronization and correlation ensure each time-sensitive system and device performs its function at precisely the same instant. In addition to performance, regulatory requirements for sequence-of-event recording and fault-recording equipment must be synchronized with UTC [2]. Although the Global Navigation Satellite System (GNSS) is currently the method of choice and, when functioning correctly, is a very capable source of time, an alternative source of time is necessary. GNSS devices are inherently vulnerable to jamming and spoofing activities, which present a potential disruption to reliable and safe grid operations [3]. Building and implementing alternative timing and synchronization capability will improve the resiliency of the PMAs, Defense Critical Electrical Infrastructure facilities, and the grid. The time delivery method of choice is the Institute of Electrical and Electronic Engineers (IEEE) Standard 1588: Precision Time Protocol [4].

This section presents detailed technical information on establishing and delivering precision time and discusses how an alternative terrestrial timing can be implemented. The more detail on the process of time transfer over a terrestrial network to educate and inform grid operators, the better. This detailed information will become important as operators begin the process of implementing private total time transfer in their respective networks, both internal and external, including connectivity to the substation.

1.1.1 Precise Time

Basic unit of time, the universal SI second, was created on January 1, 1970, and is defined as 1/86,400th of a day (e.g., 1 of 86,400 seconds in a 24-hour period) [5]. The signal that represents time is derived from the consistent number of transitions (9,192,631,770) of a single cesium atom when it is bombarded at a specific microwave frequency. This atom movement is captured electronically in a digital counter, and once the count totals 9,192,631,770, the digital counter produces a single pulse: the 1 pulse per second (pps) signal. The machine that performs this function is the atomic clock (more specifically, the cesium clock). The time information in the context of hours, minutes, and seconds is, in fact, metadata—formatted digital data for use by people and machines—derived from this 1 pps signal.

The US organizations responsible for the precise measurement of this time signal are the National Institute of Standards and Technology (NIST) in Boulder, Colorado, and the US Naval Observatory in Washington, D.C. These organizations, in collaboration with other Bureau International des Poids et Mesures timing centers around the world, develop UTC, a global, synchronized timing standard. As an example, the time derived from a Global Positioning System (GPS) receiver is correlated to UTC to determine its accuracy. This method ensures all GPS receiver outputs are synchronized to the same reference time base, or epoch, to create a universal time code across common industrial and commercial uses [6].

1.1.2 Network Time Protocol

Network Time Protocol (NTP) is an internet-based protocol that is used to synchronize devices connected to an Ethernet network within a few milliseconds of UTC. NTP was developed in the 1980s and is the common method used by most systems to set their clocks [7]. The NTP servers are usually geographically diverse, with a majority accessed through public/private internet connections, although in many cases NTP servers use GNSS as the source to UTC. Systems can access internet-based NTP servers by using the NTP pool project addresses or any public NTP server that is listening to requests. NTP can use authentication, which will allow the client to verify the authenticity of the NTP server. This mode provides a means to prevent synchronization with rogue NTP servers if provisioned correctly. NTP is accurate within milliseconds; however, the timing needs of the grid and event synchronization require 1 μs or better if the network is provisioned correctly for deterministic latency and if the network is end-to-end controlled.

1.1.3 Precision Time Protocol

A more accurate method of time synchronization is Precision Time Protocol (PTP), as governed by the IEEE 1588 standard [4]. This method of time transfer has been in use since 2002 and, as of this writing, is on its third upgraded version. This protocol is used in telecom, finance, power grid, industrial, and other industries to transfer precise time from its generation point to its usage or consumption point. With a properly designed transport technology, time precision in the low nanoseconds is possible because of the ability to compensate for switching delays of network devices.

The basic operation of PTP is a communication between the timing master clock, or node, and a time slave. The timing master creates the internet protocol (IP) packets (8275.2) or Ethernet frames (8275.1) that carry the time value implemented as a timestamp. The time slave receives these packets and, from the time-value timestamp, produces a digital signal of 1 pps and a clock signal of a frequency used by the receiving application. The 1 pps signal is referenced to the time base (or epoch in a substation's usage) and is measured in nanoseconds of precision relative to the original signal used by the timing master to create the PTP timestamp. The next few paragraphs explain how the PTP protocol operates and highlight critical best practices for its successful implementation.

PTP is composed of a simple communications syntax made up of synch messages (T1), delay request messages (T2), and delay response messages (T3). Figure 1 depicts this message exchange process.

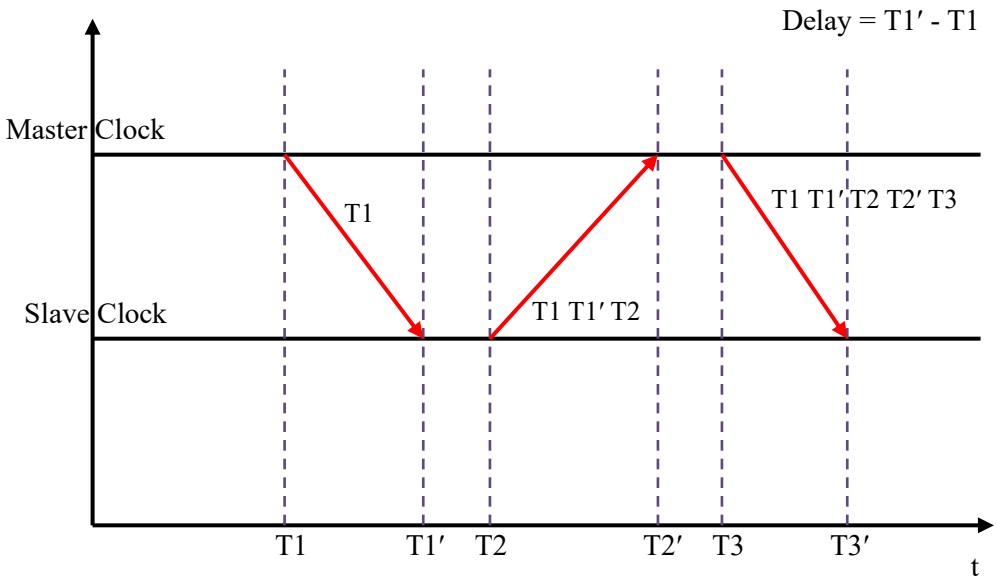


Figure 1. PTP message protocol.

PTP presumes that the paths from the time server to the target network element are identical in distance, and the times of flight of the messages are captured and measured as noted in Figure 1. This concept is referred to as called path symmetry, which guarantees the time slave can compute and replicate the value of time that the time master implemented in the timestamp it sends. The following paragraphs describe this process.

To accurately synchronize to their timing master, clocks must individually determine the network transit time of the Sync T1 messages. The transit time is determined indirectly by measuring round-trip time from each clock to its master. To measure the transit time, the clocks initiate an exchange with their master. The exchange begins when a clock sends a delay request (Delay_ReqT2) message at T2 to the master. The master receives and timestamps the Delay_ReqT2 at time T2′ and responds with a delay response (Delay_RespT3) message. The master includes the timestamp T2′ in the Delay_RespT3 message. Through these exchanges, a clock learns T1, T2, T3, T1′, T2′, and T3′.

If T1 is the transit time for the Sync message and T2 is the constant offset between master and follower clocks, then the time slave can use the timestamp placed in the T3 delay response message to calculate the offset in path flight time between the T1 and T2 paths. It then integrates this offset into its time calculation, and the clock now knows the offset during this transaction and can correct itself by this amount to bring it into agreement with the time master. This process is constantly repeated and requires almost no actual time to occur.

Clearly, the closer the downlink and uplink path flight times, the more accurate the resulting time transfer will be. In the case of grid operations and time transfer, this calculation must resolve time alignment between the time master and time slave to as close to 100 ns as possible. The time error budget for the entire grid is 1 µs, the maximum time offset from UTC allowed for synchro phaser operation.

The best practice for implementing a PTP time-transfer network between any pair of locations is to ensure that the physical frame flight times in each direction are nearly identical and, most importantly, highly deterministic. Determinism in this context means very high repeatability over time. This practice is discussed further in Section 3.3.3.

1.1.4 Time Synchronization

NTP and PTP are the mechanisms by which multiple systems can achieve time synchronization. Synchronized time supports everything, including basic alignment of information technology (IT) and OT system time operations to switches and relays operating at the precise and appropriate times, governing transactions across data-centric functions, audit support, and ensuring information assembly and recovery in logs. If clocks across the network are out of sync or if different time-dependent systems disagree by more than 1 µs, then the consequences may range from minimal impacts to mis operation of protective relaying. Synchronization happens across time hierarchical stratums, wherein Stratum 0 is the authoritative source of time and Stratums 1, 2, and so forth are distribution tiers that preserve and serve time to downstream subscribers using NTP or PTP.

1.2 BASIC EQUIPMENT NEEDED TO IMPLEMENT A NETWORK TIMING SIGNAL

1.2.1 The Source of Time

At the root, or starting point, of the PTP time transfer system is a device that produces the time base, or epoch, for the system to use. For the Center for Alternative Synchronization and Timing (CAST), this piece of equipment is a cesium clock (or atomic clock). This device creates the fundamental clock signals the timing master will eventually use to produce timestamps. The cesium clock is synchronized to an external universal time reference with traceability to UTC. Traceability means the time output from this reference can be tracked back to the time source produced by NIST in Boulder, Colorado. The cesium clock is synchronized from a signal emanating from the reference as either a frequency or a 1 pps signal. The cesium clock aligns its internal electronics to mimic exactly the time source from the reference. Because the chosen cesium clock has an extraordinary stabilization capability, after synchronization it should be capable of outputting the time replica with 100 ns of accuracy for more than 100 days. This activity is called holdover.

This precision and stability over a long timeframe provide the grid operator a source of time that can augment or replace GPS, which is complementary to a GNSS time source. The cesium clock device is an off-the-shelf and readily available commercial product and is not susceptible to jamming or spoofing activity. The recommended components and specifications are identified in Section 4. CAST continues to define, refine, test, and evaluate best practices for the use and implementation of cesium clocks to ensure their continued operation at the level required for grid applications. These best practices are discussed in Section 4.1.

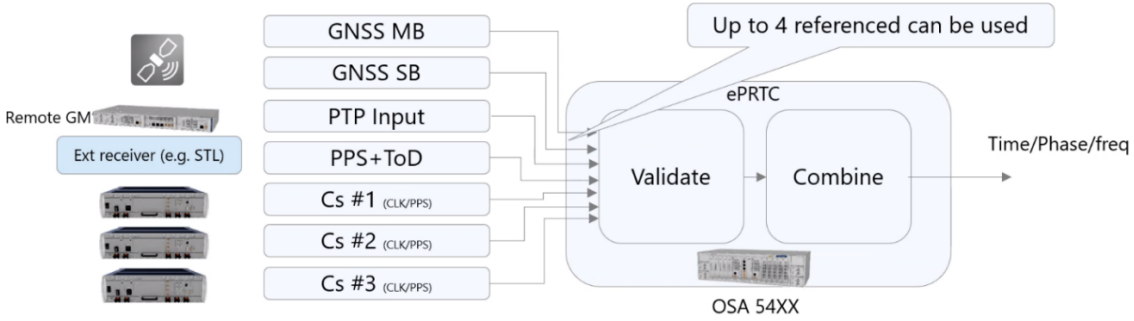


Figure 2. Example of a grand master PTP time scale.

1.2.2 The Master Source of Time Transfer Packets

This device and the associated cesium clock are implemented in the central site determined by the grid operator. The output of the cesium clocks is injected into a device called a grand master (packet) clock (GMC). This device takes the output from the cesium clocks and disciplines its internal clock to synchronize with the cesium clock. It then creates the appropriate timing packet in the manner described earlier, generates a timestamp that is equal to the frequency of its internal clock, integrates the data message and timestamp into the appropriate packet type, and launches the packet onto the network.

This device performs many other PTP functions, such as building a database of time slaves, formatting the output model to comply with whichever operating profile has been selected, performing a role in the Best Master Clock Algorithm used in a network to select the best master clock (if multiple cesium atomic clocks are used to create timestamps), and reporting performance information to the network management system. In addition, for a PTP network to operate properly, a few general network requirements need to be in place. First and foremost, the PTP synchronization process requires a bidirectional network capable of transmitting IP packets from the master clock to the slave clock and back. This capability enables all devices to receive sync, follow-up, and delay-response messages and to transmit delay requests. The master source should be able to accept inputs from three cesium clocks, algorithmically compute the standard deviation, and select the best total output time quality. This feature, combined with the extremely long holdover times of the recommended cesium clocks, provide grid operators with the capability to operate independently at well under the error budget limit for up to 6 months. The recommended components and specifications are provided in Section 4.2.

1.2.3 The Role of a Boundary Clock

A boundary clock (BC) device is deployed at remote locations selected by the grid operator, acting as intermediary points with additional sites further downstream. Occasionally called a remote synchronization unit (RSU), it receives PTP packets from the GMC and uses the PTP messages and time synchronization to train its internal clock with the GMC's timestamp. This synchronization process serves as a time slave function. The resulting time value is then passed to downstream slave devices on the network. Typically, the device relies on an internal rubidium or quartz oscillator as its local clock source. Because the PTP continuously updates the BC's time from the upstream GMC, the need for prolonged holdover is reduced, making a rubidium or quartz oscillator sufficient instead of a more precise and expensive cesium clock. Time distribution involves two-way messaging to account for network propagation delays. Some slave clock frequency-recovery algorithms leverage that bidirectional communication to enhance timing accuracy and stability; therefore, the PTP profile supports one-way and two-way operations.

PTP outlines two clock behavior types: one-step and two-step clocks. In a one-step clock, the sync messages directly carry the precise timestamp. By contrast, a two-step clock uses a follow-up message to deliver the exact timestamp of the associated sync message. Follow-up messages boost accuracy by enabling hardware-level timestamping. This approach allows the master to send the timestamp in a separate, less time-sensitive packet rather than adjusting it on the fly during sync message transmission.

A master using a one-step clock can significantly cut down on the number of PTP messages it sends. However, certain security features or design constraints might necessitate the two-step clock method. As a result, the PTP profile accommodates both options, allowing a compliant PTP master clock to operate with either a one-step or two-step approach.

1.3 BEST PRACTICES FOR INSTALLING TIMING EQUIPMENT

Several factors should be considered when choosing an installation location for timing equipment. Maintaining environmental stability around the timing system equipment is essential and includes controlling factors such as temperature and vibration, which directly affect how well the equipment operates. Equally important is having skilled and knowledgeable support staff to manage these systems. Oscillators, including cesium clocks, are particularly sensitive to changes in temperature, which can cause frequency shifts. Cesium clocks, being the core of precise timekeeping, need temperature swings to be limited to less than 1°C over 24 h for optimal performance.

The power supply also plays a big role. It needs to be steady, with AC noise filtered out to avoid issues—although this is not a concern if DC power is used instead. Unfiltered AC noise can disrupt the internal power systems, so connecting to a filtered power source with UPS backups is recommended. A DC battery setup can also work well.

The team managing a timing system should be well versed in the hardware/software configurations and should have a good understanding of IEEE 1588 PTP [4] as well as how network devices and changes affect timing. The CAST team is well suited to provide mentoring and technical support where needed to help ensure success for those wishing to set up a solid timing infrastructure.

2. INTERCONNECTING TIMING SYSTEM LOCATIONS

2.1 TWO-WAY SATELLITE TIME AND FREQUENCY TRANSFER

Two-way satellite time and frequency transfer (TWSTFT) is the appropriate method to provide NIST-based precise time to the GMC node locations [8]. TWSTFT will implement satellite communications (SatCom) between NIST Boulder and the GMC root node location(s).

This approach uses geostationary satellites to synchronize and transfer time between sites and is currently used to link NIST in Boulder, US Naval Observatory in Washington, DC, and Bureau International des Poids et Mesures in France to coordinate UTC across these locations. The signal from the satellite transponder is a precise 10 MHz frequency received by the satellite modems for comparison with locally generated 10 MHz frequency signals. The offset or correction signal is passed over the satellite link for comparison with the NIST frequency source, this corrected signal is returned, and the local satellite modem updates its local clock with the correction value. The output from the satellite modems is fed into the cesium clock ensemble as the clocks lock to this signal. A 1 pps signal can also be integrated via GPS receiver into the GMC or cesium clock to establish UTC traceable time.

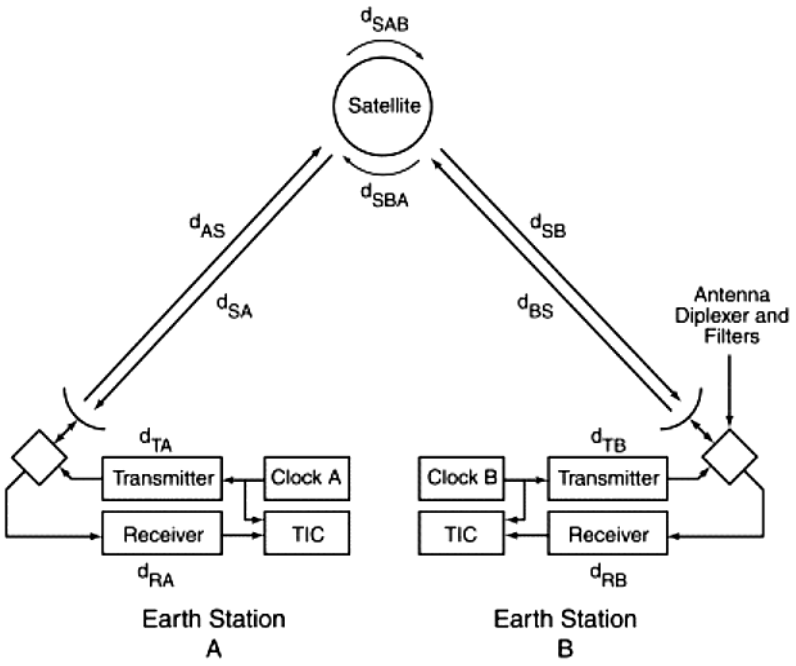


Figure 3. Two-Way Satellite Time and Frequency Transfer using a geostationary communications satellite [8].

TWSTFT has been a trusted time transfer and synchronization method for geographically wide areas for a long time. It provides good timing accuracy, usually 100 ns or less.

Oak Ridge National Laboratory (ORNL) partnered with NIST Boulder, Microchip, and Idaho National Laboratory (INL) and established TWSTFT for ORNL–NIST, ORNL–Microchip–NIST, and ORNL–INL. This setup allowed ORNL to synchronize with NIST UTC and provided a benchmark to help ORNL provide synchronization and timing to other national laboratories and serve as a ground truth reference for

evaluating PTP over wide area (e.g., ORNL-INL PTP over the Energy Sciences Network's On-Demand Secure Circuits and Advance Reservation System). The goal from this TWSTFT network is to give ORNL the facility for a resilient and reliable geo redundant network solution with the opportunity to synchronize and transfer time between ORNL and power grids.

2.2 COMMON CARRIER LEASED OPTICAL TRANSPORT NETWORK SERVICE

For transporting PTP, the recommended method is the Optical Transport Network (OTN). This networking technology enables communication within a WAS network, connecting master clocks to slave clocks, including those at substations. A common carrier-provided OTN service is like a leased line. Rather than leasing a traditional line, the client rents an optical path on a dense wavelength division multiplexing network, enhanced by a digital wrapper technology called OTN. This process adheres to the International Telecommunications Union's (ITU)-T standard G.709 [9]. The PTP protocol IEEE 1588-2019 Annex B [4] outlines how PTP is mapped onto the OTN path. National telecom operators offer this service, but it is typically available only in major metropolitan areas. For instance, the CAST project at ORNL could not secure an OTN connection to the Western Area Power Administration in Loveland, Colorado, or Sandia National Laboratories in Albuquerque, New Mexico, for experimental purposes. When OTN is not an option, the CAST team at ORNL collaborates with partners to assess alternatives, considering existing networks, expected congestion, cost of new infrastructure, and the timing system's performance requirements.

A critical factor in OTN service is ensuring that all node interconnections along the path use optical–optical–optical switching rather than the more common optical–electronic–optical approach [10], in which the PTP packets are converted from an optical signal to an electronic byte-based format for port-to-port transfer and then back to an optical signal. This process introduces a slight (but influential) delay, disrupting path symmetry and reducing the accuracy of the time output of the clocks on the edge. More details are covered in IEEE 1588 Annex B below.

[excerpted from IEEE 1588]

Transport of PTP over the Optical Transport Network (OTN)

H1.1 General
This annex specifies those portions of the PTP standard that are specific to implementations that transport messages over the Optical Transport Network (OTN), as defined in the ITU-T Recommendations G.709 Amd.1, G.709.1 Amd.2, and G.7041 Amd.1. Several types of interfaces, Optical Transport Unit-k (OTUk), Optical Transport Unit-25 (OTU25), Optical Transport Unit-50 (OTU50), Optical Supervisory Channel (OSC) and Flexible Optical Transport Network (FlexO), are considered to transport PTP by the OTN. The support of Transparent Clocks is out of scope for the transport of PTP over the OTN.

H1.2 PTP message channel
ITU-T Recommendation G.709 Amd.1 defines the OTN synchronization messaging channel (OSMC) to transport PTP messages. Clause 15.7.2.4 of ITU-T G.709 Amd.1 (12/2020) specifies one byte in the OTUk, OTU25 and OTU50 overhead as the OSMC for the OTUk, OTU25 and OTU50 interfaces, respectively (see Figure 15-12 of ITU-T G.709 Amd.1 (12/2020)). Clause 14.1 of ITU-T G.709 Amd.1 (12/2020) defines support of the OSMC for the OSC interface, and Figure 15-1 of ITU-T G.709 Amd.1 (12/2020) shows that the OSMC is carried by the OSC payload. ITU-T Recommendation G.709.1 Amd.2 defines the OSMC to transport PTP messages for the FlexO interface. Clause 9.2.10 of ITU-T G.709.1 Amd.2 (12/2020) specifies two bytes in the FlexO overhead as the OSMC (see Figure 9-7a of ITU-T G.709.1 Amd.2 (12/2020)).

H1.3 PTP message encapsulation
ITU-T Recommendation G.7041 Amd.1 defines a Generic Framing Procedure, frame-mapped (GFP-F). This is used to encapsulate PTP messages as specified in clause 7.10 of ITU-T G.7041 Amd.1 (08/2019). To transport PTP over OTUk, OTU25, OTU50, and FlexO interfaces, the PTP messages shall be encapsulated into the GFP-F frames as specified in clause 7.10 of ITU-T G.7041 Amd.1 (08/2019). The GFP-F frames shall be inserted into the OSMC as specified by the normative references cited in H1.2 and H1.4. To transport PTP over the OSC interface, the encapsulation of PTP messages is implementation specific.

H1.4 Timestamp generation
To transport PTP over OTUk, OTU25, and OTU50 interfaces, the message timestamp generation shall be as defined in clause 15.7.2.4.1 of ITU-T G.709 Amd.1 (12/2020). To transport PTP over the FlexO interface, the message timestamp generation shall be as defined in clause 9.2.10.1 of ITU-T G.709.1 Amd.2 (12/2020). To transport PTP over the OSC interface, the message timestamp generation is implementation specific.

2.3 USING ETHERNET POINT-TO-POINT MICROWAVE RADIO

Another method, but not preferred, for transferring the PTP-based time packets is the use of point-to-point high-frequency Ethernet radio systems [11]. The systems are common and are already used in the grid to transfer data and control messages between locations. These systems suffer from operational issues, which operators need to be aware of before using them to transfer time via PTP.

Because these systems use the free-space environment (line of sight) between radio towers, they are susceptible to environmental disruptions such as fog, rain, and high winds. These systems have mitigation methods to ensure some data passes between radio locations in all these circumstances. The typical method used is controlled fade, a mechanism by which the radio reduces its data transfer rate until the measured error rate drops to an acceptable level. This process is fine for normal data. However, for PTP, which is very sensitive to path symmetry, if the transfer rate changes to a lower value, then the PTP algorithm will conclude that the path between the radios suddenly got longer. In such a circumstance, the GMC will begin the process of recalibrating the timestamp flight times; consequently, the resolution accuracy between the PTP nodes at each end of the radio will degrade. Once the environmental condition

returns to normal, the PTP algorithm will normalize, and the desired precision can be recovered. The operator must understand this operating paradigm before implementing this type of system.

2.4 EMERGING ALTERNATIVE SOURCES OF TIME AND SYNCHRONIZATION

2.4.1 Digital Television Transmission

The National Association of Broadcasters (NAB) has released the new broadcast standard Advanced Television Systems Committee (ATSC) 3.0 [12]. Although this standard is not yet fully implemented, it has the capability to carry a nanosecond-level timestamp and the geolocation data of the transmitter. When these are received, the timestamp can be used to correct the local clock. After several copies are received, the receiver can calculate the rate of change in the timestamp, which is directly related to the timestamp clock frequency. Using the timestamped geolocation data from other transmitters combined with the receiver's own geolocation data, the direction and distance to each transmitter can be calculated. Once the local timestamp clock rate of change is aligned to the transmitter timestamp clock, the difference in received timestamp values represents the flight time of the received packet, which is used to advance the local timestamp clock to match the timestamping event time of the transmitter as well as the flight time of the packet. According to NAB engineers, these combined signals allow the receiver and transmitter to correlate to approximately 50 ns of alignment.

NAB and NIST have conducted measurements of their terrestrial beacon approach to alt-GNSS: Station KWGN in Denver, Colorado, has been broadcasting the Broadcast Positioning System (BPS) timing signal on ATSC 3.0. Initial results look promising: noise added by a BPS transmitter and receiver seems bounded to a few nanoseconds over 100 km distances. The United States has more than 1,700 existing TV transmitter towers, and NAB is actively searching for more partners to test deployment of ATSC 3.0 and BPS.

NAB is investigating GNSS-independent time sources such as UTC-NIST dark fiber or TWSTFT but has not yet installed those time delivery methods because they are expensive. Low Earth orbit satellites and enhanced long-range navigation have also been cited as GNSS-independent timing sources. Although the above-mentioned sources would have made our timing system truly independent of GNSS, using GNSS as a reference still enabled us to characterize BPS time transfer capabilities using the KWGN signal.

2.4.2 Multi-Source Common View Disciplined Clock

A future development of connecting multiple master clocks, the multi-source common view disciplined clock (MSCVDC) is a technique for synchronizing earthbound endpoints to a common clock without the requirement for large infrastructure investments or specialized personnel skill sets. MSCVDC is a recent NIST invention designed to support critical infrastructure timing systems that require a verifiably accurate and fail-safe clock [13]. Lombardi [13] introduces the MSCVDC, provides a technical description of how it works, and discusses its reliability, redundancy, security, and performance.

The technology background for MSCVDC is based on the NIST-developed common view signal (CVS) approach of synchronizing time at two different physical locations with high correlation precision. The original system used high-accuracy GPS receivers with rubidium oscillator companions. In this original embodiment, the two endpoints each received the 10 MHz and 1 pps clocks from a single satellite, the same for both ends. They would then compare themselves to these signals and, via a simple data exchange mechanism, exchange their local clock values.

The initial implementation of MSCVDC uses GPS as the CVS source. Other CVS sources are available, as noted in Table 1, which provides a partial list of direct broadcast satellites that deliver digital television signals to all 50 states and that could potentially provide a CVS source (sorted by longitude).

Table 1. CVS sources to support MSCVDC

Satellite	Year launched	Longitude	Operator
T11 (DIRECTV 11)	2008	99° W	AT&T
T14 (DIRECTV 14)	2014	99° W	AT&T
T16 (DIRECTV 16)	2019	101° W	AT&T
T10 (DIRECTV 10)	2007	103° W	AT&T
T12 (DIRECTV 12)	2009	103° W	AT&T
T15 (DIRECTV 15)	2015	103° W	AT&T
EchoStar 105 (SES-11)	2017	105° W	EchoStar
EchoStar X	2006	110° W	Dish Network
EchoStar XIV	2010	119° W	Dish Network
EchoStar IX	2003	121° W	EchoStar

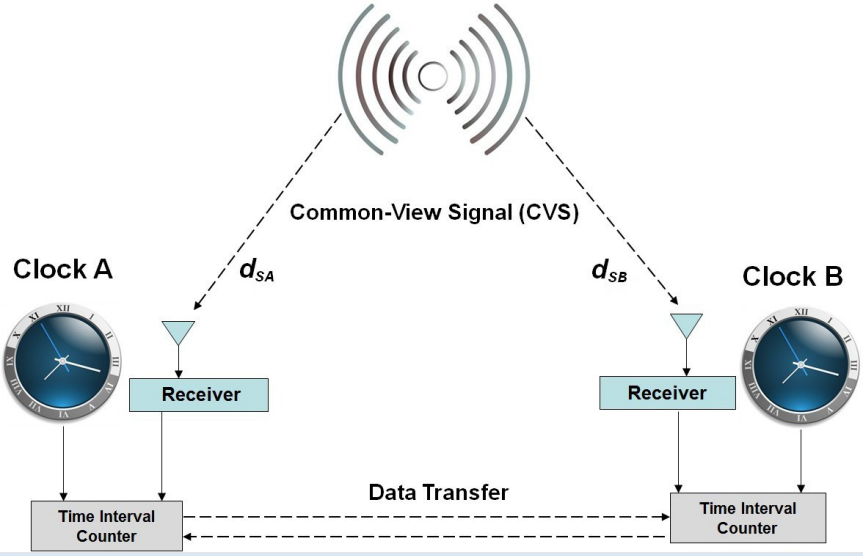
If the MSCVDC approach is of interest to a PMA, then they should contact NIST Boulder. This technology can be rented from NIST for a nominal fee. The MSCVDC system could also be purpose-built for the US Department of Energy.

The following excerpt has been adapted from the above-referenced NIST publication for clarity [13]:

[excerpted from Lombardi, 2022]

A common-view comparison can be arranged if there is a signal that can be simultaneously observed both in Chicago and in Boulder. If such a common-view signal (CVS) exists, then the clocks in Chicago and Boulder can each be simultaneously compared to the CVS. The difference between the two "indirect" comparisons effectively substitutes for a direct comparison and reveals the time difference between the Chicago clock and UTC (NIST). Even though the CVS signal originates from its own clock, the time signal it delivers does not have to be accurate, because it is cancelled out when the two indirect comparisons are subtracted from each other, if the propagation times are equal or if the differences in propagation time can be measured and corrected. In a common-view comparison, the CVS is not the reference clock used for synchronization, but instead just a vehicle that relays time information from one site to another.

The following figure shows a common-view time transfer system where a transmitter produces the CVS, and where the CVS is received at sites *A* and *B*. Both sites have a local clock and a receiver that each produce a 1PPS signal. At each site, the time difference between the received and local 1PPS signals is measured with a time interval counter (TIC). The site *A* measurement compares the CVS received over the path *dSA* to Clock A, producing the time difference *Clock A – CVS*. The site *B* measurement compares the CVS received over the path *dSB* to Clock B, producing the time difference *Clock B – CVS*.



2.5 SUGGESTED WIDE-AREA SYNCHRONIZATION NETWORK

The technologies described above can be used to transport time between devices and across networks, ensuring synchronized operations. Time transport is architected in a hub-and-spoke model, where a source of reference time (a master clock, synchronized to an authoritative time source) delivers time to a secondary receiver clock (a slave clock, or BC), which then further cascades the time to other clocks, independent devices, or systems. This process typically uses terrestrial connectivity, such as OTN, leased lines (T-1), or microwave hops. Some synchronization systems may have only one spoke coming from the hub (a single chain of time transport), whereas others may have many spokes with further branching at each boundary/slave clock node.

To achieve a WAS network, multiple master clock nodes must be connected and synchronized. Master clocks are typically geographically dispersed, or purposely independent of one another for security or business purposes. Historically, GPS has been the wide-area source for synchronizing dispersed clocks to a common reference. Although GPS is technically sufficient, resilient synchronization outside of GPS can

be achieved via either secure terrestrial or over-the-air communications methods. For master clocks to synchronize to UTC, only dark fiber (dedicated private fiber connectivity), OTN, or TWSTFT will meet the accuracy requirements (<100 ns). Connecting and synchronizing these various master nodes, each with their independent and cascading spokes, will achieve WAS. However, constant calibrations for path delay, signal asymmetry, and clock error will need to be performed to ensure devices at opposite ends of this synchronization network reflect the same time with precision and accuracy. This capability is critically important for power grid equipment as well as message/event handling during the analysis phase because nanosecond accuracy must be maintained in the timing and event logs. Figure 4 highlights an example tiered WAS network for timing, which could be established across the PMAs, regional utilities, and their respective infrastructures.

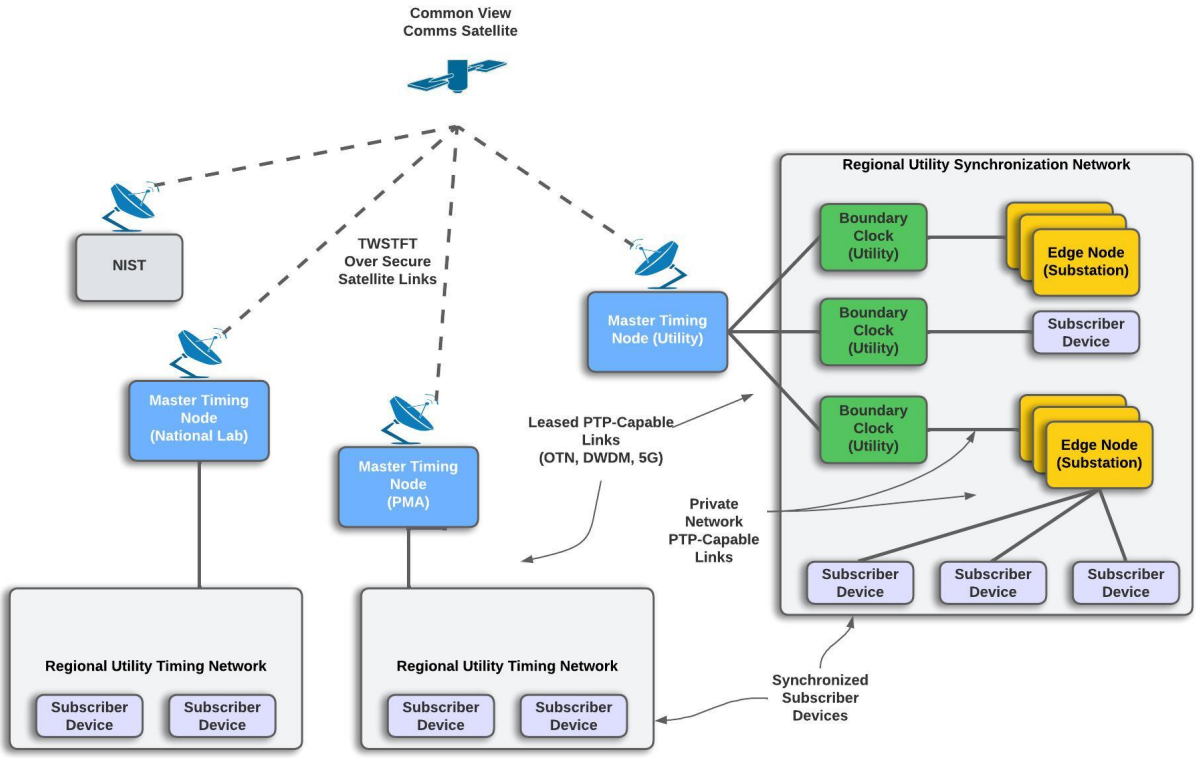


Figure 4. Example wide-area synchronization network for inter-regional time synchronization.

3. OPERATING, MONITORING, AND SECURING TIMING SYSTEMS

Operating, monitoring, and securing timing systems are critical aspects of ensuring that these systems function reliably and securely, especially in critical infrastructure environments such as the power grid. This section provides best practices for operating, monitoring, and securing timing systems. Section 3.1 highlights the establishment of a timing signal, key protocols, architectures, and the GPS/timing data traverse path through the system for device synchronization. Section 3.2 highlights best practices for deploying NTP and PTP and provides recommendations for leveraging NTP internally when architectures require it or when devices are not PTP-enabled. Section 3.3 examines various tools and methods that can be used to monitor and secure multiple aspects of NTP/PTP operation and performance. Special attention is paid to the effects of network path routing automation on time synchronization precision. Finally, IT considerations for operational timing systems are presented.

3.1 ESTABLISHING A TIMING SIGNAL FOR DEVICE SYNCHRONIZATION

A timing signal can be established for device synchronization in many ways, including using legacy GPS, TWSTFT, PTP through fiber, and connecting an atomic clock to GMCs and BCs. For establishing a timing signal, CAST presently maintains multiple GMCs at the ORNL lab, receiving GNSS/GPS signals as the timing reference input. The trusted timing source, such as NIST time or GNSS/GPS, serves as the authoritative timing reference for the initial calibration of GMCs. A timing device that is configured as a GMC can receive authoritative time reference on one of its interfaces while delivering, on the other inward interfaces, timing and synchronization to the time service subscribers. A cesium atomic clock is also connected to the GMCs, delivering the accurate phase and frequency and serving as oscillator reference for GMCs. So, when the trusted timing reference is disconnected or becomes unavailable for whatever reason during the actual deployment operation, GMCs will continue to keep time with extremely high accuracy using the reference provided by the high-frequency cesium clock. This configuration achieves a true terrestrial timing/synchronization alternative solution. The length of the GMC's ability to maintain accurate timing in absence of external reference is defined as holdover. Figure 5 shows an example for establishing a time signal using different synchronization methods.

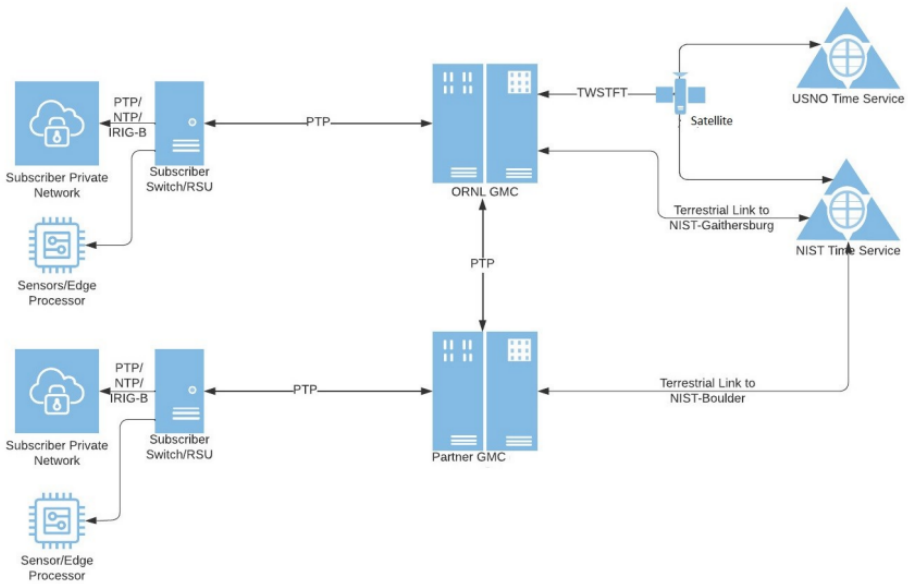


Figure 5. An illustrative example for establishing a time signal using different methods for synchronization.

GMCs deliver timing service to subscribing customer enterprises via secure PTP traffic. At the entry point of the CAST PTP traffic, a subscriber's boundary RSU device can be configured in the following ways based on the subscriber's requirements:

- As an ordinary clock that runs PTP on only one of its interfaces receiving CAST timing service. An OC is typically an end device such as an edge processor or a sensor that needs its time synchronization.

- As a BC on one end acting as a slave clock receiving CAST PTP traffic to synchronize. On the other end, often through multitude of interfaces, acting as a master clock provisioning inward synchronization service to internal clocks in either PTP or NTP traffic. A BC residing between a GMC and a multitude of slave clocks offers scalability benefits by reducing the direct communication load on the GMC. A BC also acts as a repeater that refreshes the PTP signal when long network paths are in play. Furthermore, a BC sitting at the boundary of a subscriber's internal network also provides security because it enables internal network synchronization and reduces the number of connections to external timing sources and their associated vulnerabilities.

- As a transparent clock that passes through CAST PTP traffic inward to the specific destinations within the subscriber's private enterprise. These destinations could be additional network segments containing multiple ordinary clocks to be synchronized for a broader coverage. Transparent clock RSUs can compensate for their own queuing delays but cannot function as time references. Essentially, transparent clocks function as PTP traffic switches.

3.2 DEPLOYING INTERNAL NTP AND PTP

Wide-area time distribution is critical for synchronizing devices across power generation, transmission, and distribution systems, traditionally relying on GNSS and NTP. NTP, widely supported in commercial grid components since its introduction in 1980 and standardization in 1988, synchronizes devices to UTC via public internet sources such as NIST or Google. However, NTP's reliance on internet-based timing leaves it vulnerable to cyberattacks, including man-in-the-middle attacks (where attackers intercept and alter signals), distributed denial-of-service attacks, and masquerade attacks (where attackers pose as legitimate time sources), potentially disrupting operations or masking malicious attacks.

To address GNSS vulnerabilities and enhance timing resilience, CAST is researching alternatives, including PTP (IEEE 1588), which offers more precise and secure synchronization but is less integrated into grid hardware. Although NTP follows the best practices outlined in [14] (e.g., keeping software updated, using multiple diverse time sources, monitoring for issues, etc.), its internet dependency poses risks. Organizations can mitigate these risks by deploying internal authoritative time sources such as GMCs, which use GNSS but include spoofing detection and can operate in holdover mode for weeks. PTP reduces internet-based attack risks by using secure, internal point-to-point synchronization, closing firewall vulnerabilities associated with NTP. For systems that are not PTP capable, it is recommended to configure a GMC to not only provide secure PTP but to also be an internal source for secure NTP that is not susceptible to attacks like a public NTP source over the internet (see Figure 6).

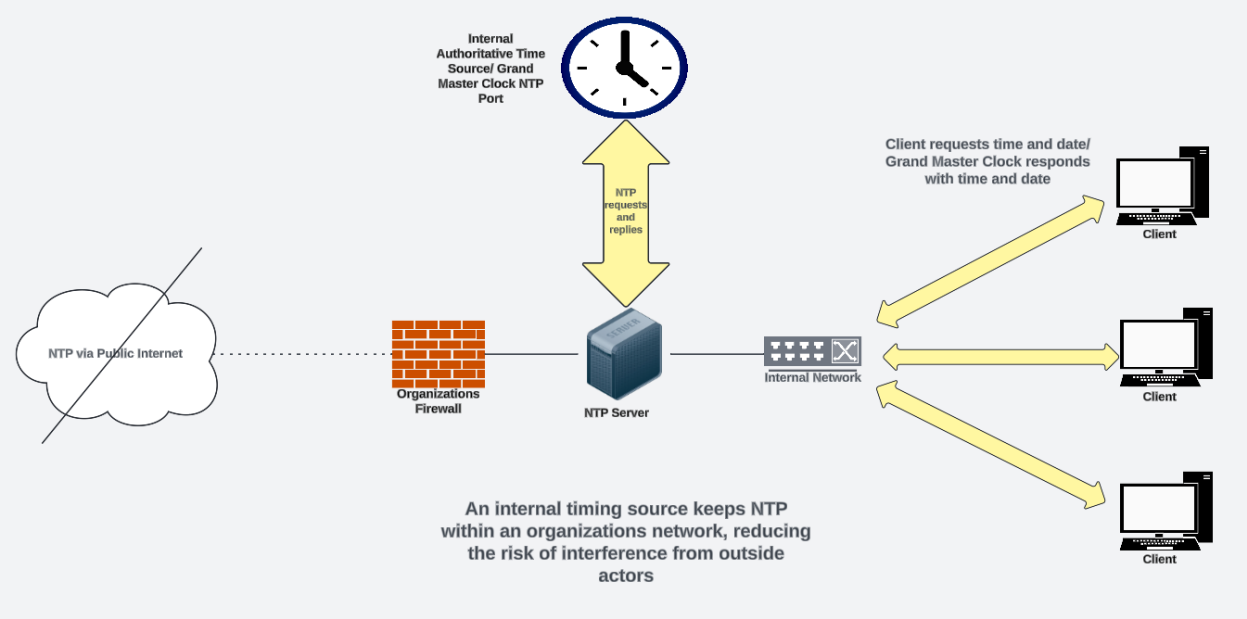


Figure 6. An illustrative example of how an internal NTP configuration secures network timing by closing the vulnerable path through the firewall that is needed for external NTP.

In summary, although NTP has been a reliable synchronization tool, its vulnerabilities necessitate fortified solutions, including PTP and internal timing, for critical infrastructure such as the power grid.

3.3 MONITORING AND SECURING NTP AND PTP SIGNALS

CAST provides an alternate timing synchronization solution to ensure accurate alignment of clocks on the devices across national critical infrastructures, including the power grid. However, if the CAST network itself is not properly secured, then the intended timing service, along with the underlying synchronization protocols (PTP/NTP), could become vulnerable to cyberattacks. Such attacks have realistic potential to generate security compromises such as timestamp manipulation that could undermine system operation, access control, forensics, and consequently the overall synchronization capability. The potential vulnerability is not limited to PTP/NTP attacks. The attack surface spans the entire networking infrastructure and systems that CAST operates upon. A broad array of operation anomalies, such as incorrect device/software configurations or network traffic congestion, could also lead to unspecific unmalicious faults/disturbance within the CAST infrastructure. Malicious attacks and unmalicious faults both contribute to CAST security compromises, in terms of timing information integrity and service availability. Consequently, sound cybersecurity constructs in CAST design, configurations, operation, and maintenance are crucial to the intended alternate synchronization solution mission.

3.3.1 GNSS/GPS Cybersecurity

Satellite-based navigation/timing signals from the space are precariously weak. These signals can easily be obstructed, damaged, or compromised by a variety of malicious and unmalicious activities. GNSS/GPS vulnerabilities pose significant cybersecurity threats. To achieve signal spoofing, malicious actors can send false GNSS/GPS signals to trick the GMCs to intake an erroneous authoritative timing reference. Malicious actors can also send a relatively powerful radio signal to jam/interfere with the authentic GNSS/GPS signals, causing the signals to be lost or distorted. The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency has classified GNSS/GPS-based positioning, navigation, and timing (PNT) vulnerabilities as cybersecurity threats. Within the CAST context, GPS

infrastructure resiliency is partially addressed by connecting the cesium atomic clock to the GMC to deliver accurate phase and frequency and using it as the oscillator reference for GMC. When a trusted GPS timing reference is disconnected, disrupted, or becomes unavailable during the actual deployment operation, GMC will continue to keep time with high accuracy using the reference provided by the high-frequency cesium clock. The US Department of Homeland Security provides a reference on resilient GNSS/GPS architecture [15].

Figure 7 illustrates GNSS/GPS threats/vulnerabilities and countermeasures. On the left side is the DHS architecture diagram [15] showing possible threats and disruptions for GNSS/GPS signals. Such threats include attacker-initiated jamming, spoofing, or signal delay, as well as naturally occurred RF interference from buildings, weather elements, or solar activities. GPS receivers themselves are also single points of failure, and insecure communication links could expose the communication to man-in-the-middle attacks. On the right side of Figure 7 is a DHS list of possible countermeasures against these threats. Multiple techniques are often employed to address a single threat. For example, to mitigate risks such as jamming, systems may incorporate multiple independent timing sources—such as a local cesium clock or a terrestrial alternative—to "diversify" the timing inputs, and to "verify" and "limit" reliance on external, potentially untrusted GNSS/GPS signals. Additionally, using GPS receivers equipped with anti-jamming antenna can improve overall resilience.

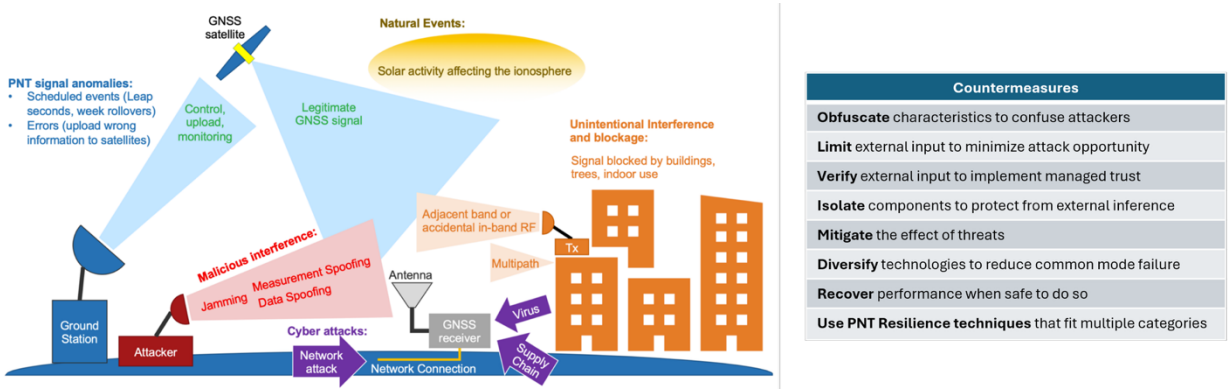


Figure 7. GNSS/GPS threats/disruptions and countermeasures [15].

3.3.2 CAST Operation and PTP/NTP Cybersecurity

CAST delivers timing service over PTP/NTP on top of infrastructure-comprising networks, time servers, firewalls, and various devices such as storage. Security compromises on the infrastructure components lead to operational anomalies that could indicate either attacks or faults. Correct configuration management over all infrastructure devices, coupled with vigilant monitoring—on the infrastructure itself with PTP/NTP operation conditions—are crucial to achieve the cybersecurity level required for service delivery.

CAST GMCs are located within the ORNL infrastructure, so the infrastructure cybersecurity management largely falls under ORNL system administration. Beyond that, some CAST-specific cybersecurity aspects require particular attention. GMC configuration management and the associated service connectivity management as well as GMC server access control, such as application (e.g., telnet, ssh, ftp) authentication and authorization. Then, there is default port configuration and account/password management against attacks. These practices must be part of the regular operation process because

activities such as software/hardware revisions could result in default port/accounts/passwords reset, thus renewing the attack surfaces. The focus is a rigorous cybersecurity guideline embedded in regular CAST production operation processes.

On top of the standard system/network cybersecurity, PTP/NTP operation monitoring is also crucial for overall CAST cybersecurity. NTP monitoring can be segmented into three main areas: server monitoring, traffic monitoring, and monitoring data analytics.

- NTP server monitoring primarily focuses on the availability, dependency, and operational status of the server. NTP server monitoring provides a window to trigger NTP server adjustment/maintenance/repair actions when precursors of NTP operational anomalies, from either malicious cyberattacks or unmalicious system failures, are observed. Example tools include public-domain/open-source tools such as NTP daemon and NTPmon as well as commercial tools such as SolarWinds and Paessler Router Traffic Grapher.

- NTP network traffic monitoring provides a holistic perspective of the NTP subscription network operational status in the context of overall combined timing traffic flow. For example, network traffic monitoring could reveal distributed denial-of-service attacks against NTP-dependent User Datagram Protocol 123 port bidirectional traffic. NTP network traffic monitoring tools, such as SonicWall and Wireshark, are also available.

- NTP monitoring data analysis can be conducted either online or offline with the help of advanced data analysis tools—potentially with the aid of AI and ML—to detect operational anomalies such as significant NTP traffic pattern and volume deviation against malicious cyberattacks and unmalicious faults.

CAST utilizes IEEE 1588 PTP as the primary synchronization backbone for timing packet delivery over long-distance terrestrial networks. Once deployed, accurate and efficient CAST PTP operation will become an important mandate for the depending critical infrastructures. This capability requires CAST to have a comprehensive and reliable anomaly-monitoring operation watching over PTP network traffic, time server status, and various operational performance and system health parameters. PTP monitoring can similarly be segmented into three general areas: server monitoring, traffic monitoring, and monitoring data analytics.

- PTP server monitoring: Monitoring PTP server controls is an important first step in ensuring accurate and secure time distribution. Server data and configuration details can be retrieved through traditional management console commands, and regular configuration compliance and control checks should be performed. An example of such a PTP server-monitoring tool is Dataminer PTP monitoring.

- PTP network traffic monitoring: Monitoring PTP network traffic provides visibility into the timing signal flow over a network. PTP network traffic typically runs over IP. PTP V1 (IEEE 1588-2002) runs exclusively on IPv4 in multicast messaging mode only, while PTP V2 (IEEE 1588-2008) and PTP V2.1 (IEEE 1588-2019) run on IPv4 or IPv6, in both multicast and port-to-port unicast messaging modes. Network traffic data can be captured using traditional monitoring tools, as well as tools designed specifically for timing data, allowing for data analysis and anomaly detection. Meinberg PTP Track Hound is one example of a PTP network traffic monitoring tool.

- Offline analysis of PTP monitoring data: Advanced techniques such as AI can be used to detect malicious violations such as man-in-the-middle attacks, impersonation attacks, protocol/algorithm

manipulation attacks (e.g., best master clock attack), denial-of-service attacks, or unmalicious faults such as clock drift, network latency/jitter, asymmetric path delays, packet loss, hardware failure, and misconfigured PTP settings.

3.3.3 NTP/PTP Monitoring and Network Operation Anomalies

The ability to monitor NTP and PTP synchronization performance metrics across the network is crucial for identifying network operation issues that would otherwise go undetected. For example, typical network paths from GMC to BC may involve many network segments that are maintained and operated by different entities. For certain OSCARS (On-Demand Secure Circuits and Advance Reservation System)–provisioned network segments, if anything along the path does not meet certain quality of service thresholds, then the circuit will automatically reroute, as a failover measure, to any other available path, thus disrupting network synchronization and noticeably increasing latency.

The bidirectional communication between clocks provides visibility into communication networks, enabling the calibration of network effects to achieve timing symmetry between nodes. Monitoring these signals and their performance provides insights into the quality and security of the communication networks supporting the grid. Specifically, this monitoring allows the team to detect automatic rerouting and assess its effect on quality-of-service metrics, offering valuable information about network behavior and performance changes.

3.4 IT CONSIDERATIONS FOR OPERATIONAL TIMING SYSTEMS

When deploying PTP and NTP in operational timing systems, IT infrastructure must be designed to support high-precision synchronization, fault tolerance, and security. Below are key technical best practices:

- Network Architecture and Infrastructure
    - Deploy dedicated timing networks or VLANs to reduce latency and minimize packet jitter.
    - Utilize network hardware with IEEE 1588 support, including boundary clocks and transparent clocks, to improve synchronization accuracy.
    - Optimize quality-of-service policies to prioritize timing packets over general traffic.
    - Ensure network switches and routers support hardware-based timestamping for PTP to minimize timing drift.
    - Use redundant network paths to prevent single points of failure in timing distribution.

- Time Synchronization Servers and Clients
    - Configure highly stable PTP grandmaster clocks with Stratum-1 time sources such as GPS-disciplined oscillators or atomic clocks.
    - Implement fallback strategies with NTP servers in case of PTP failures, ensuring seamless synchronization across distributed systems.
    - Deploy multiple redundant grandmaster clocks using Best Master Clock Algorithm to facilitate automatic failover.
    - Ensure that critical systems, including database servers, application servers, and industrial control systems, operate within a unified timing domain.

- Type 1 Hypervisors, Virtual Machines, and Containers

    - Use Type 1 hypervisors (e.g., VMware ESXi, XCP-NG, Proxmox) with direct access to hardware-assisted PTP/NTP synchronization.
    - Configure guest VMs to synchronize with the hypervisor's clock rather than external NTP sources to minimize drift.
    - Implement PTP-aware virtual NICs and enable precision timing features in hypervisor settings.
    - For containerized environments (e.g., Kubernetes, Docker), ensure that host nodes are accurately synchronized and leverage PTP/NTP synchronization within containerized workloads where required.

- Security and Access Control
    - Implement network segmentation and firewall policies to isolate timing traffic from general network traffic.
    - Enforce cryptographic integrity checks (e.g., NTP Autokey, IEEE 1588 security extensions) to prevent timing spoofing attacks.
    - Deploy role-based access controls to restrict modifications to time synchronization configurations.
    - Conduct regular security audits to detect anomalies, unauthorized PTP/NTP traffic, or configuration drift.

- Monitoring, Diagnostics, and Maintenance
    - Deploy monitoring solutions (e.g., PTP monitoring tools, NTPstat, Chrony tracking) to continuously assess synchronization accuracy.
    - Configure logging and alerting mechanisms for deviations beyond predefined thresholds.
    - Utilize packet capture tools to analyze PTP/NTP timing packets and detect jitter or propagation delays.
    - Perform periodic recalibration and firmware updates for timing hardware to maintain optimal precision.

- Interoperability and Compliance
    - Validate compatibility between multi-vendor PTP/NTP implementations to prevent synchronization conflicts.
    - Ensure adherence to industry standards such as IEEE 1588-2019 (PTP) and RFC 5905 (NTPv4) for compliance with regulatory frameworks.
    - Maintain alignment with industry-specific timing accuracy requirements (e.g., IEC 61850 for power systems, 3GPP for telecom networks, and MiFID II for finance).

By following these best practices, one can ensure precise, resilient, and secure time synchronization across bare-metal, virtualized, and containerized environments, optimizing operational efficiency and compliance with stringent timing requirements.

4. GRAND MASTER CLOCK HARDWARE RECOMMENDATIONS

This section outlines three tiers of recommendations for a grand master time scale, ranging from a highly available and highly accurate solution to a basic, nonredundant option. Each tier includes specific hardware and configuration details to meet varying accuracy and fault-tolerance needs.

- **Highly Available and Highly Accurate Grand Master**

  Overview: This solution provides maximum availability, fault tolerance, and precision using advanced optical cesium clocks and ensemble voting.

  Hardware Requirements:

  1. Three optical cesium clocks meeting the Super Enhanced Primary Reference Clock (SePRC) standard, each equipped with four 1pps outputs and one 10 MHz frequency output.

  2. Two grand master PTP clocks supporting majority voting (ensembling), each with a minimum of two 1 pps inputs and two 10 MHz inputs.

  3. NIST MSCVDC and/or TWSTFT hardware components.

  Additional Recommendations:

  1. Equip grand master PTP clocks with dual power supplies compatible with the target location's power type (AC/DC).

  2. Use 10 Gb small form-factor pluggable optics for Ethernet connections to avoid framing issues.

  3. Isolate timing transmission paths from other network traffic where possible.

- **Fault-Tolerant Mid-Level Accuracy Grand Master**

  Overview: This solution offers fault tolerance with moderate accuracy, suitable for applications requiring reliability without the highest precision.

  Hardware Requirements:

  1. Two optical cesium clocks meeting the Enhanced Primary Reference Clock (ePRC) standard, each with four 1 pps outputs and one 10 MHz frequency output.

  2. Two grand master PTP clocks supporting multisource combining, each with a minimum of two 1 pps inputs and two 10 MHz inputs.

  3. NIST MSCVDC and/or TWSTFT hardware components.

  Additional Recommendations:

  1. Include dual power supplies and 10 Gigabit small form-factor pluggable optics as described above.

2. Ensure isolated timing paths for optimal performance.

- **Nonredundant Grand Master with Basic Accuracy**

  Overview: This basic solution provides a cost-effective option with no fault tolerance, suitable for less critical applications.

  Hardware Requirements:

  1. One optical cesium clock meeting the ePRC standard, with four 1 pps outputs and one 10 MHz frequency output. An alternative for using GNSS as a Reference, a rubidium clock may be setup that receives 10 MHz from the Cesium clock as a Reference.

  2. One grand master PTP clock supporting one 10 MHz or one 1 pps input.

  3. NIST MSCVDC and/or TWSTFT hardware components. This is another alternative for not relying on 1 pps from GNSS, so we may use GMC Steered by TWSTFT as a Reference.

  Additional Recommendations:

  1. Consider dual power supplies and 10 Gb small form-factor pluggable optics for improved reliability.
  2. Isolate timing paths if feasible.

4.1 CESIUM REQUIREMENTS

A cesium clock combined with GNSS can form a GMC. A typical implementation with output options is shown in Figure 8.

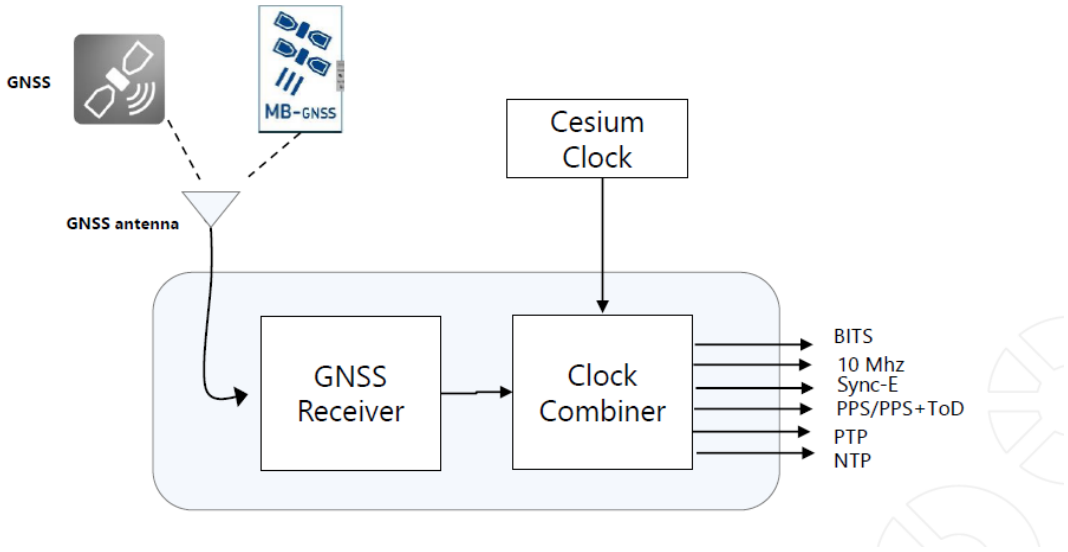


Figure 8. Typical cesium clock implementation [16].

Cesium clock requirements focus on ensuring its ePRC capabilities comply with ITU-T G.811.1 as well as its ability to maintain short- and long-term stability. SePRC leverages the optical pumping technology

to deliver full high-performance frequency stability. When used with enhanced primary reference time clocks, it delivers a holdover of 100 ns for a minimum of 45 days (typically 55 days). To achieve the same performance with the market's current solutions, users would need multiple magnetic cesium clocks. SePRC provides optimum stability for 10 years, a substantially longer lifespan compared with all other high-performance magnetic cesium clocks. Figure 9 shows the requirements for two types of optical cesium clocks.

	ePRC+ standard	SePRC Option
Frequency stability (ADEV)	**Feature**	**Feature**
1s	≤ $5x10^{-12}$	≤ $5x10^{-12}$
10s	≤ $3.5x10^{-12}$	≤ $3.5x10^{-12}$
100s	≤ $8.5x10^{-13}$	≤ $8.5x10^{-13}$
1'000s	≤ $2.7x10^{-13}$	≤ $2.7x10^{-13}$
10'000s	≤ $8.5x10^{-14}$	≤ $8.5x10^{-14}$
100'000s	≤ $2.7x10^{-14}$	≤ $2.7x10^{-14}$
5 days	NA	≤ $1x10^{-14}$
14 days	≤ 1x10-14	
30 days	NA	≤ $1x10^{-14}$
Floor	NA	≤ $1x10^{-14}$
Phase Noise 10MHz Output		
1Hz	-90 dBc/Hz	-90 dBc/Hz
10Hz	-120 dBc/Hz	-120 dBc/Hz
100Hz	-135 dBc/Hz	-135 dBc/Hz
1'000Hz	-145 dBc/Hz	-145 dBc/Hz
10'000Hz	-145 dBc/Hz	-145 dBc/Hz
100000Hz	-145 dBc/Hz	-145 dBc/Hz

Figure 9. Cesium stability and noise threshold requirements for grid-centric terrestrial synchronization operations [17].

4.2 GRAND MASTER REQUIREMENTS

The GMCs propagate the synchronization/timing signal to the rest of the clocks in the network. These clocks must continuously maintain stable and accurate timing signal while locked to the cesium clock and GNSS. GMCs are set to higher standards and are essential for providing standard time information to other clocks across the network. GMCs need to maintain accurate and stable synchronization whether locked to GNSS or in holdover mode when satellite signals are lost. They are usually built with high quality clocks connected to a cesium clock through 10 MHz and GNSS in enhanced primary reference time clock mode to achieve 10 ns or better accuracy, and the requirements vary based on the clock manufacturer selections. Figure 10 shows a typical GMC setup with a cesium clock and GNSS.

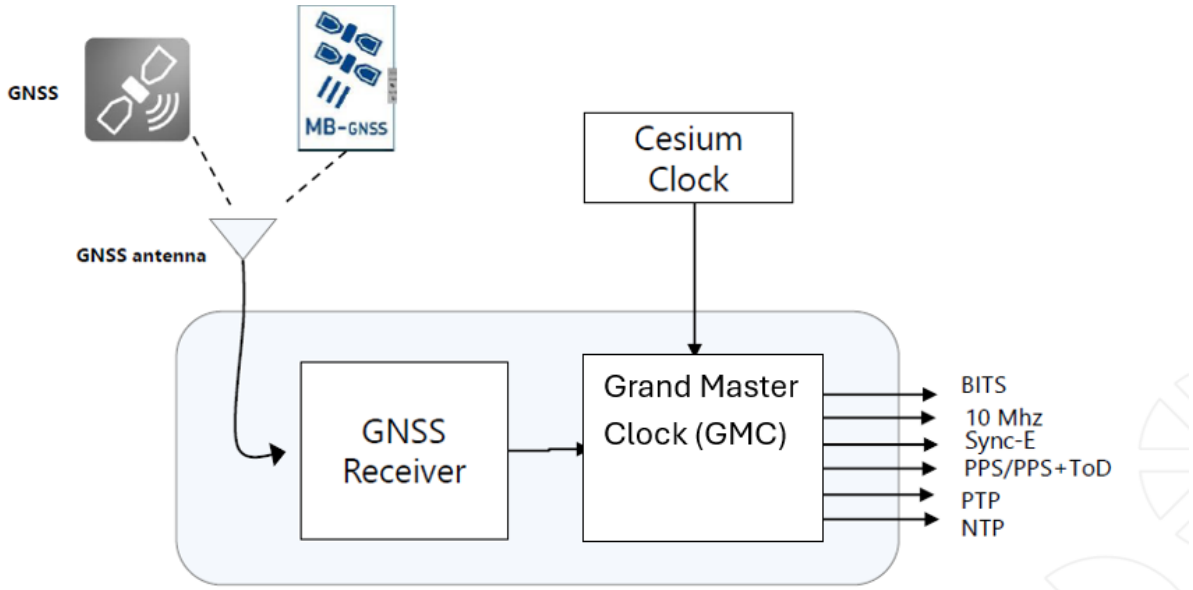


Figure 10. Typical GMC setup with cesium clock and GNSS.

The following are the requirements for GMCs:

1. Multiband GNSS: Required if measuring accuracy is a priority. GNSS is not part of the time scale.
2. Rubidium (Stratum 2) oscillator: Must be able to maintain accuracy for up to 10 µs of accuracy for 12 days or 16 parts per billion for 5 years.
3. GUI: A user-friendly interface to facilitate easier management and operation.
4. Timing accuracy probes: Built into the GUI for real-time monitoring of timing accuracy.
5. 10 MHz frequency: Sourced from a cesium clock.
6. Power source redundancy: The GMC must remain operational and not losing power.
7. Ability to access the GMC URL remotely for troubleshooting when necessary.
8. Ability to set alarms when the accuracy of the GMC degrades below a specified threshold.
9. Long duration of holdover periods with minimal offset when satellite signals are lost.
10. Stable and accurate, with standard holdover minimum of 14 days, when satellite signals are lost.

4.3 UNDERSTANDING HOLDOVER PERFORMANCE

The main challenge when attempting to maintain accuracy in timekeeping sources, or clocks, is that any independent clock will experience some amount of drift over time compared with a stable reference source. Clock drift is caused by several factors, including ambient environmental changes, thermal noise, and the precision of the clocks themselves [18]. To correct this natural drift over time, the clock can be

synchronized to a stable reference source through radio frequency, IP, or by connecting directly to the source's reference output. When a stable reference source is not available for synchronization, the drifting clock is said to be in a state of holdover. Once a clock enters holdover, the amount of drift will continue to accumulate and has no upper bound if the state of holdover endures [19]. Nevertheless, the total drift can be minimal if the clock is extremely accurate.

Commercial off-the-shelf clocks usually rely on an internal or external oscillator to improve their accuracy while in a state of holdover. Typical oscillators used to discipline commercial clocks include, in order of increasing accuracy, oven-controlled crystal oscillators (OCXOs), double oven-controlled crystal oscillators (DOCXOs), rubidium oscillators, and cesium oscillators. Although oscillators can all be an effective way to minimize total drift in a state of holdover, their price and accuracy can vary dramatically. Therefore, each oscillator should be examined individually and compared with the timing requirements of the specific application before it is selected.

OCXOs and DOCXOs are the cheapest and least accurate of the listed oscillators. Both use a quartz crystal to keep time, much like a wristwatch or a wall clock. However, these oscillators are orders of magnitude more accurate than a wristwatch or a wall clock because their crystals are encased in a low-temperature oven. When the encased crystal is kept at a high temperature (relative to room temperature) with little variation, its accuracy improves enough to maintain nanosecond-level holdover performance for a few hours [20] [21].

A rubidium oscillator, which is nearly always more accurate than an OCXO [20], is the entry-level oscillator in the world of atomic timekeeping. Rubidium oscillators work by observing the frequency of transitions between energy levels in rubidium atoms and then matching an internal quartz oscillator to that frequency [22]. Although a rubidium oscillator is more expensive than an OCXO, it is accurate enough to maintain nanosecond-level holdover performance for several days [20].

Cesium, the most expensive of the listed oscillators, is also the most accurate. These oscillators function the same way as rubidium oscillators, although they are more accurate because cesium has several ideal characteristics. For example, cesium has a high vapor pressure and is easy to vaporize, so cesium can easily be kept in a gaseous state, which ultimately makes observing the energy level transitions easier [22] [23]. Additionally, cesium has only one stable isotope, which also makes its energy levels easier to observe because no extraneous energy levels from additional stable isotopes confuse the observation [22]. Combined, these ideal characteristics ultimately make cesium oscillators some of the most accurate oscillators: they are accurate enough to maintain nanosecond-level holdover performance for several months [22].

5. ONGOING RESEARCH AT THE CENTER FOR ALTERNATIVE SYNCHRONIZATION AND TIMING

CAST's primary goal is to enable a resilient power grid by building a bridge between the rich ecosystem of timing and synchronization solutions and utility operators. The CAST team performs research and development, benchmarking and assessment, and development of best practices for the implementation and operation of commercial off-the-shelf solutions to facilitate streamlined integration by power utilities. CAST maintains an operational timing laboratory at ORNL, with connections to grid testbeds as well as commercial utility and industry partners around the country.

Although a robust timing and synchronization offerings are available from commercial vendors, significant challenges remain to achieve low-cost scaling of grid-specific precision synchronization solutions to the large geographic operating areas of power utilities. Important areas of research include improving the performance of network-based time synchronization over large areas and using space-based solutions independent from GPS. The following additional areas of research investment are being explored by the US Department of Energy and CAST:

- Characterizing the reliability and resilience of TWSTFT for GPS-independent GMC synchronization.
- Evaluating the performance of space-based internet providers (low Earth orbit satellites) to augment terrestrial networks for PTP-based synchronization.
- Evaluating cloud-based timing-as-a-service providers to meet grid synchronization precision requirements.
- Evaluating commercial satellite PNT providers for applicability to grid-specific use cases.
- Documenting best practices for integration and operations of timing equipment in typical utility environments (e.g., operations centers, substations).
- Assessing commercial NTP and PTP performance-monitoring software and developing turnkey open-source solutions to augment the commercial marketplace.
- Assessing the cybersecurity and communications security risks and vulnerabilities of synchronization protocols, architectures, and equipment.
- Validating and benchmarking the performance of jamming and spoofing detection algorithms in commercial timing/clock solutions.
- Assessing the holdover performance of various clock architectures for GPS-independent operations.
- Investigating novel over-the-air WAS methods to augment TWSTFT.

6. SUMMARY

CAST's goal is to alleviate the GPS receiver from being the sole source of time within the power grid architecture. This document identifies the necessary systems and practices to implement a terrestrial complementary timing system to augment GPS/GNSS and provide resilience to disruptions in that time source. CAST will assist federal partners with the evaluation, installation, and operational expertise to implement these components within their local network environments.

The use of standard PTP ensures a properly designed and implemented network path that can deliver the timing precision needed by the various time-sensitive power grid applications, such as protective relaying, synchrophasor/phasor measurement unit networks, supervisory control and data acquisition networks, substation automation, energy market, and many others. One crucial item to consider is the ability to mix and match timing delivery techniques from the PTP root time source to the RSUs (BCs), as best served by the available timing transport technologies. Those approaches identified as NIST-serviced technologies can be obtained directly from the NIST Boulder Time and Frequency Division.

Additional information about the CAST project at ORNL can be found at https://cast.ornl.gov/about-cast/. Technical and implementation questions can be posed to the CAST team at ORNL at https://cast.ornl.gov/contact/.

7. REFERENCES

[1] Department of Energy, Office of Electricity, "Department of Energy (DOE), Office of Electricity (OE), Response to NIST Request for Information (RFI) about Profile of Responsible Use of Positioning, Navigation, and Timing Services," 10 Jul. 2020. [Online]. Available: https://www.nist.gov/system/files/documents/2020/07/14/pnt-0038.pdf.

[2] North American Electric Reliability Corporation, "Disturbance Monitoring and Reporting Requirements," 25 Sep. 2015. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-002-2.pdf.

[3] National Cybersecurity & Communications Integration Center, "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure," 6 Jan. 2017. [Online]. Available: https://www.cisa.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf.

[4] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008),* pp. 1-499, 2020.

[5] S. Bize, "The unit of time: Present and future directions," *Comptes Rendus Physique,* vol. 20, no. 1-2, pp. 153-168, 2019.

[6] W. Lewandowski and C. Thomas, "GPS time transfer," *Proceedings of the IEEE,* vol. 79, no. 7, pp. 991-1000, 1991.

[7] Network Time Foundation, "History of Network Time Protocol," 27 Jun 2022. [Online]. Available: http://www.ntp.org/ntpfaq/NTP-s-def-hist/. [Accessed 5 Jan. 2023].

[8] National Institute of Standards and Technology, "Two-Way Satellite Time and Frequency Transfer (TWSTFT)," 10 May 2016. [Online]. Available: https://www.nist.gov/pml/time-and-frequency-division/time-distribution/two-way-satellite-time-and-frequency-transfer. [Accessed 20 Mar. 2025].

[9] International Telecommunication Union, "G.709 : Interfaces for the optical transport network," 12 Oct. 2020. [Online]. Available: https://www.itu.int/rec/T-REC-G.709. [Accessed 20 Mar. 2025].

[10] M. K. Iqbal, M. U. Iqbal, M. B. Iqbal and M. H. Iqbal, "Optical fiber switches," in *2012 International Conference on Open Source Systems and Technologies*, 2012.

[11] Federal Communications Commission, "Point-to-Point Microwave," 20 Mar. 2025. [Online]. Available: https://www.fcc.gov/wireless/bureau-divisions/broadband-division/point-point-microwave. [Accessed 20 Mar. 2025].

[12] Advanced Television Systems Committee, Inc., "ATSC 3.0 Technical Documents," [Online]. Available: https://www.atsc.org/documents/atsc-3-0-standards/. [Accessed 20 Mar. 2025].

[13] M. A. Lombardi, "Multi-Source Common-View Disciplined Clock: A Fail-Safe Clock for Critical Infrastructure Systems," *Journal of Research of the National Institute of Standards and Technology,* vol. 126, 2022.

[14] D. Reilly, H. Stenn and D. Sibold, "Network Time Protocol Best Current Practices," Jul. 2019. [Online]. Available: https://www.rfc-editor.org/info/rfc8633. [Accessed Apr. 2025].

[15] Department of Homeland Security, Office of Science and Technology, "Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture," 9 Jun. 2022. [Online]. Available: https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture.

[16] Adtran, Inc., "ePRC+ Optical Cesium – Behond the limits," 12 Mar. 2021. [Online]. Available: https://wsts.atis.org/wp-content/uploads/2021/03/ePRTC-and-Optical-Cesium-Beyond-the-Limits.BESSE_.pdf.

[17] Adtran, Inc., "OSA 3350 Optical pumping cesium clock with outstanding frequency stability," 16 Sep. 2024. [Online]. Available: https://www.oscilloquartz.com/en/resources/downloads/data-sheets/osa-3350.

[18] M. Bartock, J. Brule, Y.-S. Li-Baboud, S. Lightman, J. McCarthy, K. Meldorf, K. Reczek, D. Northrip, A. Scholz and T. Suloway, "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services," National Institute of Standards and Technology, Gaithersburg, MD, 2023.

[19] D. Hagarty, S. Ajmeri and A. Tanwar, Synchronizing 5G Mobile Networks, Indianapolis: Cisco Press, 2021.

[20] Adtran, Inc., "OSA 5422 Compact PTP grandmaster, NTP Server, SB/MB-GNSS receiver, multi-interfaces," 20 Nov. 2024. [Online]. Available: https://www.oscilloquartz.com/-/media/oscilloquartz/resources/data-sheets/pdfs/osa-5422.pdf?rev=-1&hash=45C1B7A4ECA991D8664EF0ED12135B84.

[21] Brandywine Communications, "GPS Disciplined Oscillator Module (GPSDO)," 14 Oct. 2022. [Online]. Available: https://www.brandywinecomm.com/wp-content/uploads/2022/10/GPS-Disciplined-Oscillator-Module.pdf.

[22] P. Banerjee and D. Matsakis, An Introduction to Modern Timekeeping and Time Transfer, Cham: Springer Nature Switzerland AG, 2023.

[23] A. Christianson, Bellarmine University Chem 104, LibreTexts, 2025.