Symmetricom®

WHITE PAPER

Power Utilities

Mitigating GPS Vulnerabilities and Protecting Power Utility Network Timing

Introduction

The Global Positioning System (GPS) is ubiquitous as a source of precise timing for utility data networks and power grid operations. GPS and other existing and planned Global Navigation Satellite Systems (GNSS) deliver atomic clock accuracy to virtually any location with access to the satellite signals.

Electric power utilities use precise GPS-based timing at their power transmission and distribution facilities to time stamp data and measurements. The time stamped data from widely dispersed locations allows root cause analysis following grid disruptions which have ever greater impact as economies develop and become ever more dependent on electric power. As the grids evolve to smart operations, very precise time stamps will allow centralized control centers to manage the grid for higher efficiency and to avoid wide area outages. Without accurate time stamps, the collected data cannot be correlated and becomes useless.

In addition to substations and grid management, timing is also essential in data center and operating center local area networks, and throughout the utility telecom and wide area networks. By looking at the overall network picture, a utility can form strategies and practices to protect their timing and synchronization infrastructure.

This paper will review the nature of GNSS signals and the timing requirements of modern power utilities; then look into the vulnerabilities of the system; and finally present solutions to mitigate threats and protect timing throughout power utility networks.

GNSS Systems

There are four GNSS systems in operation or planning stages as of 2013. The United States GPS is most widely used around the world, while Russia's GLONASS is preferred in some areas. China has deployed the Beidou regional system and is expanding it to become a global system known as Compass. The European Union is in planning and testing stages preparing the Galileo system.

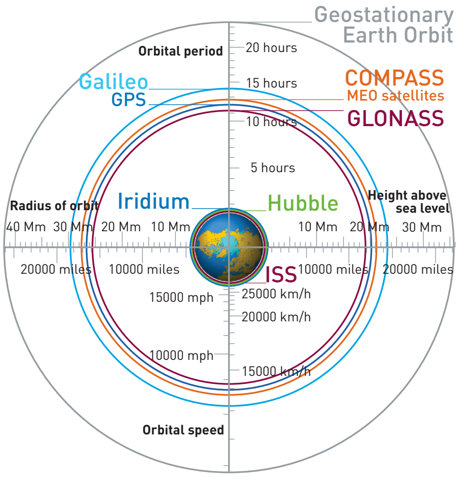


Figure 1: GNSS systems in general: an array of 24-30 satellites, in mid-earth orbits over 19,000 kilometers away, circling the earth every 12 hours

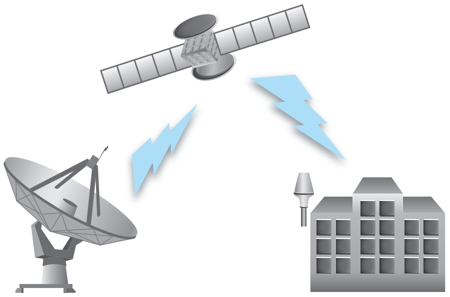


Figure 2: GNSS systems have three basic components:

1. Control Stations send position and time synchronization information to the satellites
2. Satellites send their position and time information to Earth
3. Receiver calculates its position and time

This paper will primarily reference the U.S. GPS, though all GNSS operate in a similar manner. Most importantly, they are all subject to similar vulnerabilities, and timing systems benefit from the same mitigation solutions. The systems are complex and full descriptions would be unnecessarily technical for our purpose; therefore we will look at how they operate only to a level to understand vulnerabilities. The GPS system is a constellation of operational and backup satellites that orbit the earth every 12 hours. GPS satellites carry multiple atomic clocks, typically cesium, which is the frequency reference used in the international definition of a second. A GPS receiver with visibility of at least 4 satellites can use the information transmitted in the signals to solve for position and precise time.

Power Utilities

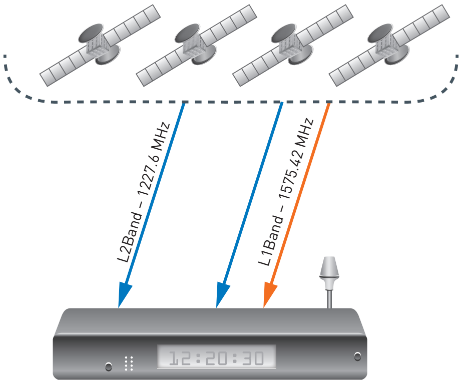


Figure 3: GPS signals are very low power: 25 to 100 Watts, from a distance over 20,000 kilometers away

GPS signals are transmitted in two frequency bands called L1 and L2. The Coarse Acquisition (C/A) code which includes the position and time information used in civilian and commercial applications is carried in the L1 band. Unfortunately the C/A code is more vulnerable than the P(Y) code used by the government and military. The P(Y) code is transmitted on both the L1 and L2 frequencies and is encrypted. Even more importantly, GNSS signals are very weak, as low as -160 dBW at the surface of the earth—1/10th of 1 quadrillionth of a Watt—making them easily susceptible to jamming and other interference. GPS signal strength has been compared to an ordinary light bulb located in space over 20,000 kilometers away.

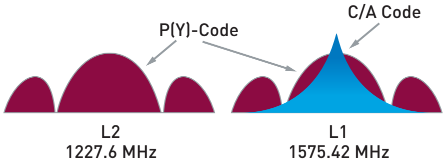


Figure 4: L1 and L2 GPS signals. L1 Corse Acquisition Code is the signal available for commercial use.

Timing is Essential to the Grid

Timing has always played an important a role in power grid operations, but never more than now. The Smart Grid fundamentally changes the role of time information from something used to relate historical data points in post-fault investigations to now enabling real time analysis for prompt remedial action and eventually automated operations.

Modernized substations collect data points much more frequently (for example phasor measurements taken 30 to 120 times a second versus once a second in a traditional SCADA solution) and require higher time stamp accuracy. To handle the increase in data, networks employ high bandwidth, low cost Ethernet. The Network Time Protocol (NTP) has served the industry well, and it will continue to play an important role in utility networks where applications require only millisecond accuracy. However, the IEC 61850 standard for power utility automation establishes 1 microsecond (±1 μsec) as the accuracy requirement for critical smart substation operations such as synchronized phasor measurements (known as synchrophasor: phasor measurements with an accurate time stamp) and digitized sampled values.

To achieve that accuracy, the IEEE 1588 Precision Time Protocol (PTP) is expected to be in the next edition of the standard.

The Precision Time Protocol, implemented in accordance with the Power Profile (IEEE C37.238-2011), will deliver the accuracy required for critical substation applications. Real time data from many substations, located kilometers apart, will flow in Wide Area Measurement Systems to central control centers where the time stamps enable the control applications to correlate the data and turn it into actionable information. The grid will be able to safely operate closer to peak efficiency and react quickly to prevent outages over wide areas.

Though not all substations are "smart" and synchrophasors may be only a future consideration, accurate data time stamps with a common reference are important to the operation of the power grid. Whether from the latest Intelligent Electronic Devices (IEDs) or collected by a legacy SCADA system, without accurate timestamps the data is useless. The Global Positioning System provides a very accurate time reference, however when GPS is not available the system cannot operate as intended for long, and therefore vulnerabilities of the GPS have become a major concern.

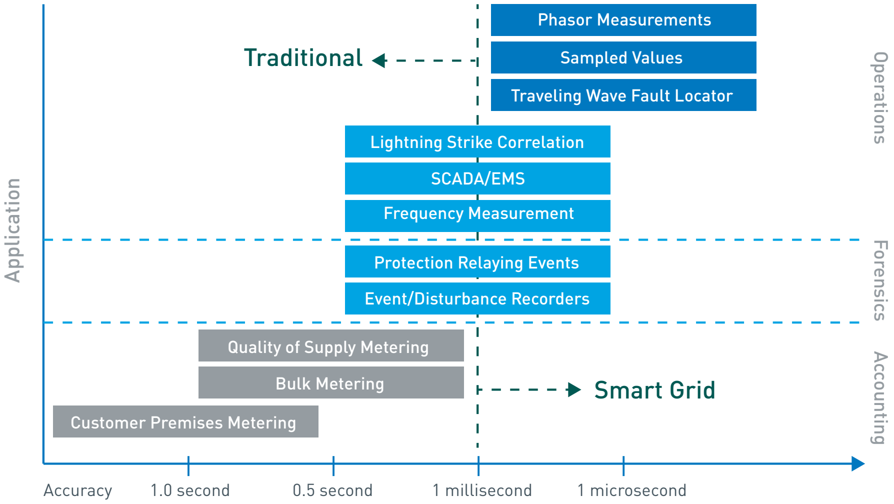


Figure 5: Timing requirements for substation applications

Power Utilities

GPS Vulnerabilities

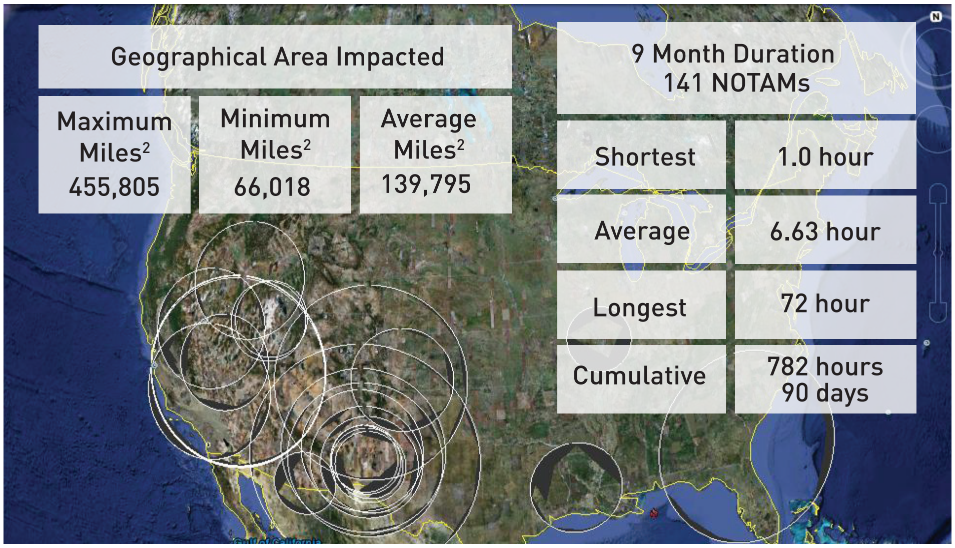
GPS vulnerabilities take many forms: environmental and manmade, accidental and malicious, and errors inherent in the space-based system itself. Results from a nine month study conducted by the U.S. Department of Defense indicated an outage somewhere in the study area approximately 12% of the time, affecting on average approximately 4.5% of the continental United States. Concern is so high the Department of Homeland Security launched the "U.S. GPS Interference, Detection and Mitigation Program" with the energy sector identified as a "critical infrastructure key resource."

Jamming and Spoofing

Jamming is probably the most commonly cited threat to GPS today. Inexpensive civilian devices are easily found on the Internet, and with the advent of position tracking in commercial vehicles, drivers are using them to avoid being monitored. In their simplest form, jammers transmit a relatively powerful noise signal that crosses the GNSS frequencies causing nearby receivers to lose their lock on the satellite signal.

Spoofing is more sophisticated. Instead of simply drowning out the GPS signal with noise, spoofers substitute a counterfeit signal with altered data. In a spoofing technique known as meaconing, GNSS signals are recorded and then rebroadcast on the same frequency, but the timing information is no longer accurate. The spoof signal has greater power which captures the receiver lock. The receiver continues to operate, but now bases its position and time calculations on the incorrect input. In work conducted by the University of Texas at Austin, it was determined that a spoofing attack can cause PMUs to violate the IEEE C37.118 standard [1].

Figure 7: Jammer device and spoofing equipment



Geographical Area Impacted		
Maximum Miles^2	Minimum Miles^2	Average Miles^2
455,805	66,018	139,795

9 Month Duration 141 NOTAMs	
Shortest	1.0 hour
Average	6.63 hour
Longest	72 hour
Cumulative	782 hours 90 days

Source: FAA, 2010

Figure 6: GPS testing conducted by the U.S. Department of Defense

Equipment Failures and Interference

Not as exotic, but probably having greater operational impact, failures of GPS timing are often traced to problems with the GPS equipment and installation or other nearby equipment. Antennas and cables are exposed and subject to breakage. Nearby electronic equipment can malfunction or degrade and radiate energy that interferes with the GPS signal. GPS "antenna farms", not uncommon in power substations, can be a problem if a connector loosens or degrades causing an impedance mismatch and noise radiation.

Figure 8: GPS "antenna farm"

Environmental

Clouds, rain and snow alone have no meaningful effect on GPS signals, however, natural weather conditions certainly can have an impact. Lightning strikes or high winds can take out antennas. Sleet and ice can freeze over the antennas and impair their ability to receive a signal.

Solar flares are bursts of energy from the sun resulting in an increase in radiation that can temporarily impact the GPS signals and cause errors in timing calculations by the GPS receivers.

Figure 9: Environmental factors such as antenna icing and solar flares can impact GPS signals

Errors Inherent in Space Based Systems

Unimpaired GPS signals travel at the speed of light, and typical civilian GPS receivers base their calculations on that constant. Unfortunately there are several sources of error inherent in spaced-based systems that can impact the accuracy of the calculations. Timing systems with multiple references are better able to adjust for these errors.

[1] Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks, Daniel P. Shepard and Todd E. Humphreys *The University of Texas at Austin*, Aaron A. Fansler *Northrop Grumman Information Systems*

Power Utilities

Here is a brief summary of the source for these errors:

Satellite Orbit Error: Inaccurate reporting of a satellite's location impacts the GPS receiver's calculations of position and time.

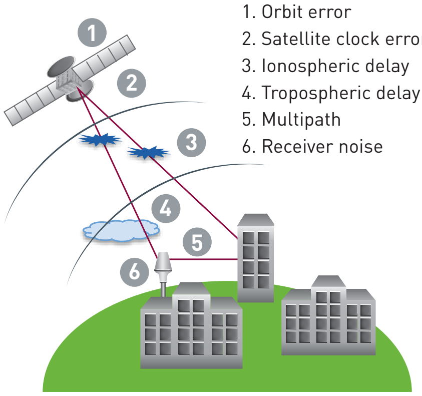
Satellite Clock: Even atomic clocks are subject to drift and noise. Much of this is corrected as part of the signal message, but some error remains.

Ionosphere and Troposphere Delay: Far away signals are delayed by a varying quantity of free electrons, depending on how close the satellite is to the horizon. Closer to earth, signals are delayed by varying temperature and humidity. Receivers will partially compensate for the delay but cannot adjust for all the variation error.

Multipath: GPS signals may bounce off of buildings or other obstructions causing delay in the signal.

Receiver Noise Error: Receiver noise can introduce jitter into the signal, introducing timing errors.

Outages Happen



1. Orbit error
2. Satellite clock error
3. Ionospheric delay
4. Tropospheric delay
5. Multipath
6. Receiver noise

Figure 10: Sources of GPS timing errors

All of the above mentioned vulnerabilities are real—not just possibilities. The U.S. Department of Homeland Security maintains a database of events as part of its mission to protect Critical Infrastructure and Key Resources (CIKR).

Location	Date	Cause & Impact
GPS system	March, 1993	Upload to the satellites of bad navigational data
St Charles, MO	11-21 October, 1994 May 1995	GPS/L1 interference from test equipment at nearby aerospace facility
GPS system	18 March, 1997	Anomaly that caused satellite's time to jump forward approx 2hrs and 20 minutes
New York, New Jersy	December, 1997 - January 1998	Transmitter inadvertently left on, interfering with airline flights within a 300-kilometer radius
Chesterfield, SC	15-23 April 1999	Army communications system radiating in GPS/ L1 band
GPS system	March, 2000	Upload to the satellites of bad navigational data
Moss Landing, CA	15 April – 22 May, June & Fall, 2001	TV antenna pre-amp radiating in GPS/L1 band, GPS denied throughout harbor region
GPS system	July, 2001	Clock drift out of spec on individual satellites
Mesa, AZ	13-18 December, 2001	"Unintentional jamming signal generator radiating at 1575.002 MHz, GPS denied for 180nm radius
Douglas, Isle of Man	2002	Poor CCTV camera installation blocked GPS signals
GPS system	June, 2002	Upload to the satellites of bad navigational data
GPS system	January, 2004	Upgrade to ground segment software caused problems with timing receivers
San Diego, CA	22 Jan, 2007	US Air Force, emission due to personnel error, wide-scale denial of GPS
GPS system	April, 2007	32nd satellite added causing problems with receivers not designed to handle only 31
New York, NY	2008	GPS outage and effected systems similar in character to '07 San Diego event
GPS system	January, 2010	Upgrade to ground segment software caused problems with timing receivers
GPS system	January, 2010	Clock drift out of spec on individual satellites
Leesburg, VA	July 2011 - January 2012	100mW jammers caused minor disturbance to FAA Control Center, ZDC
Newark Airport, NJ	2009 - 2011	FAA equipment going off line intermittently. Traced to a truck with a jammer driving by on frequent trips
Korea	March, 2011	U.S. military reconnaissance aircraft forced to land due to GPS jamming
Korea	March, 2011	N. Korea military jammers believed to have knocked out 146 cell sites
Iran	December, 2011	GPS meaconing used to capture U.S. drone
Las Vegas	March, 2012	DoD event, unintentional; exercised Cease Buzzer; Las Vegas airport ground stop for approximately 1 hour
Korea	May, 2012	"North Korea pumps up the GPS jamming in week-long attack"

Figure 11: Examples of GPS outage events compiled from published reports and open literature.

Power Utilities

Other governments have programs of their own. The list shown here is just a sampling compiled from public sources and news stories to demonstrate the wide array of things that go wrong.

Mitigation Solutions

Rubidium Atomic Clocks

The first line of defense against loss or impairment of GPS signals is to deploy clocks with robust holdover capability. Holdover is the period of continuing operation when the primary timing reference source is lost. That is, when the GPS signal is lost, timing is held by the clock oscillator in the equipment. The period of effective holdover is a function of the application (which determines the accuracy requirement that must be met) and the type and performance of the holdover oscillator in the equipment design. There are a wide variety of oscillator types in use today; each provides a different performance / cost value.

Temperature Controlled Crystal Oscillators (TCXO) are often used because they are inexpensive, but they provide essentially no meaningful holdover capability. When holdover is important, Oven Controlled Crystal Oscillators (OCXO) and rubidium (Rb) atomic clock oscillators are most commonly used. Rubidium provides longer holdover and can support more stringent accuracy requirements, but typically cost more than OCXO alternatives.

In traditional substations, OCXO solutions that can hold millisecond accuracy for approximately 24 hours may be adequate. In smart substations, where the timing requirement is more stringent and the impact of incorrect time stamps on the data is great, rubidium atomic clock oscillators are considered best practice. Actual oscillator performance is affected by environmental factors such as temperature changes; both the degree of change and the rate of change. In general terms, rubidium clocks can hold ±1 microsecond accuracy for 8 or more hours, while OCXO will hold for less than half of that time under the same temperature circumstances.

Figure 12: Rubidium miniature atomic clock, embedded component in timing equipment.

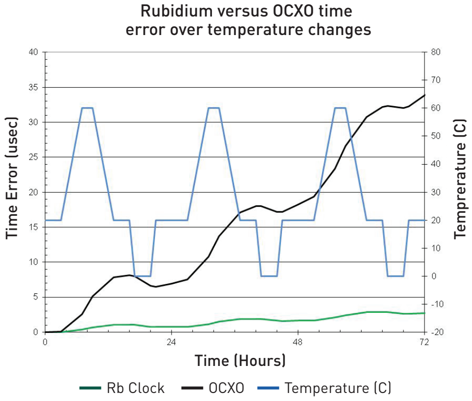


Figure 13: Comparison of OCXO and rubidium holdover

Cesium

Another way to protect against GPS vulnerabilities is to use a cesium based primary reference in your network in addition to GPS. Cesium "periods of radiation" are used in the international definition of a second, and as mentioned earlier, cesium clocks are actually on board the GPS satellites. Deploying a cesium clock as the primary reference essentially eliminates the risk of GPS vulnerabilities. Cesium clocks are costly compared to holdover oscillators, so deploying one at every location is not feasible. However, deployment at centralized locations, combined with network distribution of time, allows its cost to be leveraged across several locations and networks.

Figure 14: Examples of cesium clocks

Network Distributed Time

In very simple terms, network distributed time consists of a GPS primary reference incorporated into a time server or grandmaster clock, and then the time is distributed to clients or slaves embedded in the equipment. Multiple masters in dispersed locations provide protection when the GPS in one area suffers an outage. Network distributed time can also provide backup against other sources of timing disruption such as simple equipment failure or human error.

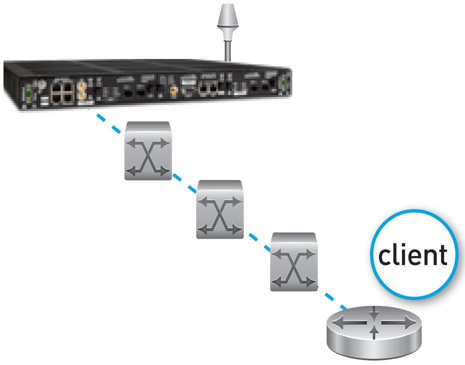


Figure 15: Network Distributed Time

Power Utilities

Network Timing Protocol (NTP) is the most commonly used protocol for distributing time over packet networks. It is relatively inexpensive to deploy and supported by virtually all networked equipment. Though not designed for precision, NTP accuracy remains adequate for a wide range of power utility applications.

More accurate timing can be distributed over a wide area communications network such as the utility's telecom network using the IEEE 1588 Precision Time Protocol (PTP). GPS signal impairments in one location will likely not affect a different location many kilometers away. In the case of smart substation applications which need microsecond timing, wide area network distributed time stamps alone will likely not meet the requirement. However, PTP Grandmaster clocks at the substation can use the time information from a centralized grandmaster as an aid to extend the holdover period when GPS is lost. Best practice in substations is to deploy redundant master clocks, each with its own GPS receiver. Time is distributed throughout the substation using traditional and PTP technologies. GPS "antenna farms" are eliminated; easing management and maintenance, and reducing possible sources of GPS error. Depending on design, the same PTP Grandmaster may also support other timing technologies such as IRIG-B, PPS, NTP and E1/T1; allowing the PTP signal over the telecom network to provide extend timing backup to the entire substation.

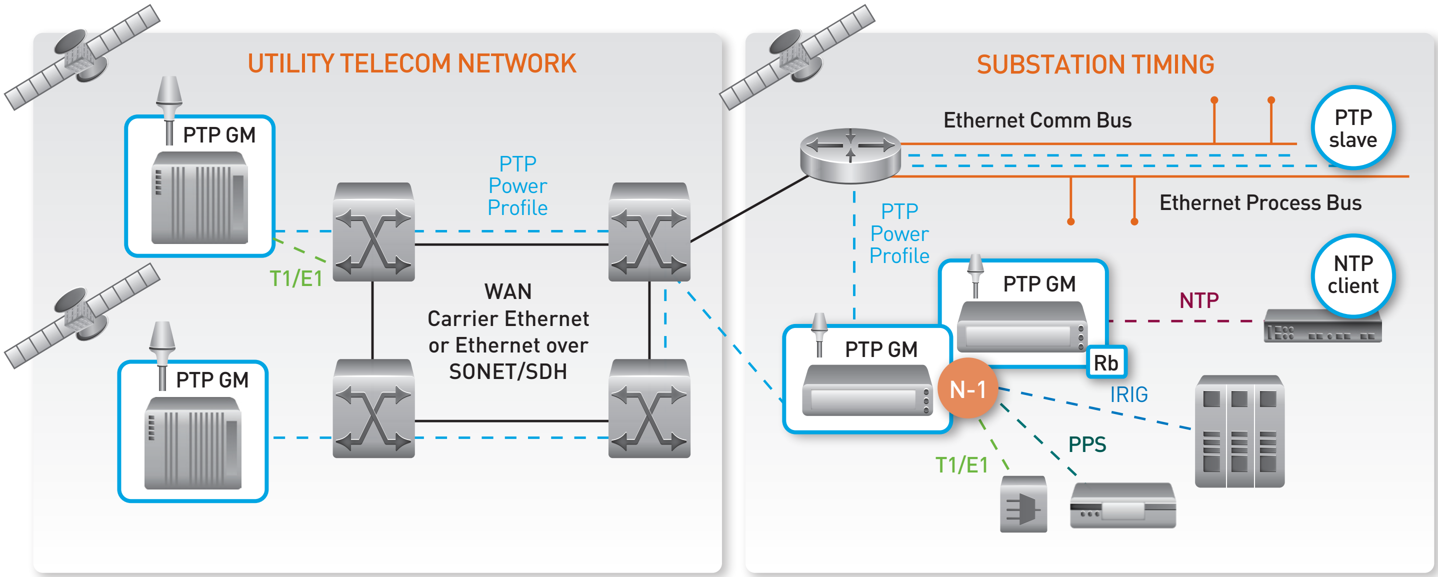


Figure 16: Time distribution in power utility telecom and substation networks

Data centers and operations centers should also protect the timing in their local area networks. This can be achieved by a several means, often operating in conjunction with one another. Grandmasters and time servers in one location can back up time servers in a different location using the wide area network connections between the computing centers. Connection to a national time service provides another source for timing backup. And, as mentioned earlier, the primary sources can be protected using a cesium clock and/or rubidium oscillators for holdover.

Conclusion

Timing, always important, is more critical than ever as power utilities modernize their operations. Accuracy requirements have become more stringent, and timing protection has become essential as operations move toward more proactive and real-time applications.

Vulnerabilities of the current and planned Global Navigation Satellite Systems (GPS, GLONASS, Compass, Galileo) have caused governments and network operators to investigate and deploy solutions that mitigate the impact of GNSS impairments and outages.

Several techniques are available to power utility network operators: rubidium holdover, cesium primary sources and network distributed time. Each solution has advantages and disadvantages relating to technical feasibility and cost.

The solutions are not mutually exclusive, and power utilities can choose among them deploy the best timing architecture for their networks.

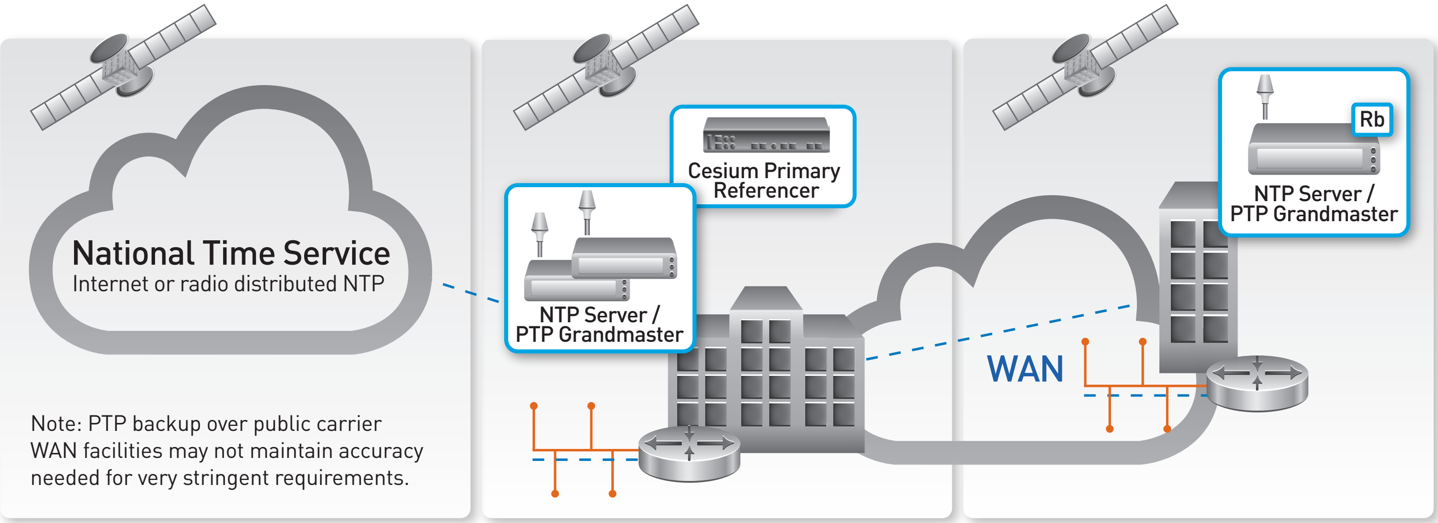

National Time Service
Internet or radio distributed NTP
Note: PTP backup over public carrier WAN facilities may not maintain accuracy needed for very stringent requirements.
Cesium Primary Referencer
NTP Server / PTP Grandmaster
WAN
Rb
NTP Server / PTP Grandmaster

Figure 17: Protected time distribution for data centers and operations centers

Symmetricom
2300 Orchard Parkway
San Jose, California 95131-1017
tel: 408.433.0910 fax: 408.428.6960
www.symmetricom.com