Secure, Wide-Area Time Synchronization

Ken Fodero, Chris Huntley, and Dave Whitehead
Schweitzer Engineering Laboratories, Inc.

Published in
Line Current Differential Protection: A Collection of Technical Papers Representing Modern Solutions, 2014

Previously presented at the
1st Annual Protection, Automation and Control World Conference, June 2010,
and 12th Annual Western Power Delivery Automation Conference, April 2010,
under the current title

Originally presented at the
36th Annual Western Protective Relay Conference, October 2009,
under the title "Wide-Area Time Synchronization for Protection"

Secure, Wide-Area Time Synchronization

Ken Fodero, Chris Huntley, and Dave Whitehead, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Modern electric power protection, monitoring, and control systems rely on the availability of high-accuracy time. Precise time enables technologies like synchrophasors, IEC 61850 Process Bus, and highly accurate, wide-area power system event reporting. Today, high-accuracy time is generally provided by Global Positioning System (GPS) clocks. However, if GPS is the only source of accurate time, it becomes the single point of failure in systems that rely on precise time. GPS may become unreliable due to solar activity, intentional or unintentional jamming, or the U.S. Department of Defense (DoD) modifying GPS accuracy or turning off the satellite system.**

I. Introduction

The availability of economical precise time from Global Positioning System (GPS) or satellite clocks has made precise time widely available in substations, control houses, and even remote devices such as recloser controls. The widespread deployment of this technology has further enabled applications previously too costly or just not possible without it.

IEC 61850 Process Bus and the use of synchrophasors for system control are examples of applications that would not be possible without wide-area precise time.

The role of precise time has shifted from just providing time reference for a Sequential Events Recorder (SER) to a critical input in the protection scheme. In this new role, precise time is performing a function similar to teleprotection in pilot relaying schemes. The measures used to evaluate a teleprotection channel are security and dependability. To increase security and dependability, equipment and component redundancy are often used.

There are several interference sources for a GPS receiver. As in all communications-based protection schemes, the dependability of the data during these interferences is key. This paper discusses some of these noise conditions, mitigation techniques, and schemes.

The security of the GPS signal may also be of concern. A new GPS clock protection scheme is introduced that addresses these concerns and provides high-accuracy timing across a wide area even with the loss of GPS availability.

II. Atomic Time Scales

There are several atomic time scales. Temps Atomique International (TAI) is an extremely accurate time scale based on a weighted time average of nearly 200 cesium atomic clocks in over 50 national laboratories worldwide. TAI is "science" time, useful for making measurements in relativity experiments. The Bureau International des Poids et Mesures (BIPM) near Paris, France, started with a TAI equivalent to earth-based time (UT1) on January 1, 1958. Coordinated Universal Time (UTC) is an atomic time derived from TAI time, with one-second adjustments to keep it close to UT1. UTC time is the international standard for civil and legal time.

III. GPS and UTC Time

GPS time is an atomic time that began on January 6, 1980, and is generated at the U.S. Naval Observatory. GPS time is not adjusted (always 19 seconds behind TAI) and is therefore also offset from UTC by an integer number of seconds. GPS satellites broadcast the UTC time offset in the navigation (NAV) message. GPS clocks receiving GPS time and the NAV message apply the UTC time offset correction automatically as a part of the lock sequence. In mid-2009, GPS time was ahead of UTC by 15 seconds, as shown in Fig. 1.

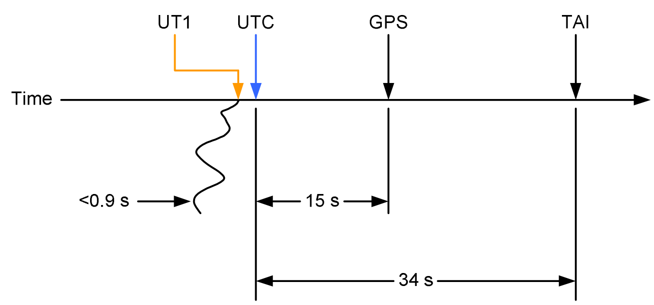

Fig. 1. Atomic time scales (for 2009)

UTC is kept within 0.9 seconds of UT1 by occasionally adding 1-second steps called leap seconds. This adjustment maintains agreement between the atomic and astronomical time scales. The decision to introduce a leap second in UTC is the responsibility of the International Earth Rotation Service (IERS). Without the addition of leap seconds, the sun would be seen overhead at midnight (rather than at noon) after approximately 50,000 years.

UTC provides a worldwide time reference and is preferred for wide-area monitoring and control applications. The use of local time for these applications proves cumbersome because there are 24 different (one hour) time zones across the earth plus 6 additional fractional (half hour) time zones, as shown in Fig. 2. Daylight-Saving Time (DST) adds a seasonal offset that needs to be accounted for as well. While it is unlikely that events will need to be coordinated between continents, many continents cross many time zones [1].

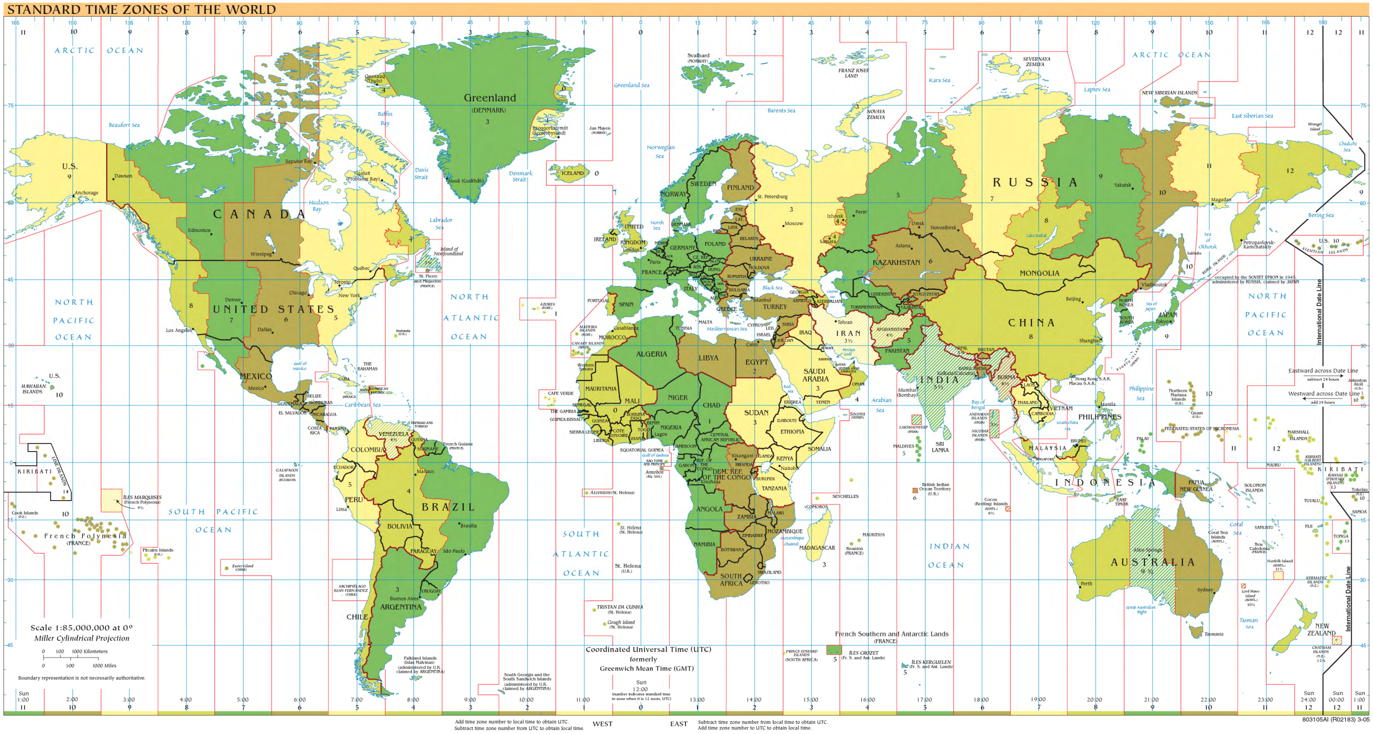

Fig. 2. Time zone map of the world

IV. IRIG-B

Using a common time reference is really just the start. Next, we need a means to distribute the time reference to downstream devices or intelligent electronic devices (IEDs). The format most commonly used today to distribute the synchronized time information is defined in the IRIG Standard 200-04.

IRIG-B, as fully described in IRIG Standard 200-04, is a very popular format for distributing time signals to IEDs. Time is provided once per second in seconds through day of the year in a binary coded decimal (BCD) format and an optional binary seconds-of-the-day count. The format standard allows a number of configurations that are designated as *Bxyz*, where *x* indicates the modulation technique, *y* indicates the counts included in the message, and *z* indicates the interval.

The most common formats used in our industry are IRIG-B002 (modulated) and IRIG-B000 (unmodulated). The time-code format IRIG-B002 is a BCD time code (HH,MM,SS,DDD). This format represents traditional or legacy IRIG-B. The time-code format IRIG-B000 consists of a BCD time code (HH,MM,SS,DDD) plus straight binary seconds (SBS) of the day (0 to 86,400 seconds) and contains “control” bits for function extensions; e.g., the year, leap second, DST, UTC time offset, time quality, and parity fields described in Annex F of both IEEE 1344 and IEEE C37.118.

The IEEE control bit assignments can be seen in Table I. IEDs that require high-accuracy time (<1 microsecond) are programmed to check the control function bit field and use this additional information to determine the quality of the received time.

TABLE I
IRIG-B CONTROL FUNCTION BIT ASSIGNMENTS

IRIG-B Position ID	Control Bit Number	Designation	Explanation
P 50	1	Year, BCD 1	Last two digits of year in BCD
P 51	2	Year, BCD 2	
P 52	3	Year, BCD 4	
P 53	4	Year, BCD 8	
P 54	5	Not used	Unassigned
P 55	6	Year, BCD 10	Last two digits of year in BCD
P 56	7	Year, BCD 20	
P 57	8	Year, BCD 40	
P 58	9	Year, BCD 80	
P 59	–	P6	Position identifier #6
P 60	10	Leap second pending (LSP)	Becomes 1 up to 59 s before leap second insert
P 61	11	Leap second (LS)	0 = add leap second, 1 = delete leap second
P 62	12	Daylight saving pending (DSP)	Becomes 1 up to 59 s before DST change
P 63	13	DST	Becomes 1 during DST
P 64	14	Time offset sign	Time offset sign: 0 = +, 1 = –
P 65	15	Time offset: Binary 1	Offset from coded IRIG-B time to UTC time. IRIG-coded time plus time offset (including sign) equals UTC time at all times (offset will change during DST).
P 66	16	Time offset: Binary 2	
P 67	17	Time offset: Binary 4	
P 68	18	Time offset: Binary 8	
P 69	–	P7	Position identifier #7
P 70	19	Time offset: 0.5 hr	0 = none, 1 = additional 0.5 hr time offset 4-bit code representing approximate clock time error 0000 = clock locked, maximum accuracy 1111 = clock failed, data unreliable
P 71	20	Time quality	
P 72	21	Time quality	
P 73	22	Time quality	
P 74	23	Time quality	
P 75	24	Parity	Parity on all preceding data bits
P 76	25	Not used	Unassigned
P 77	26	Not used	Unassigned
P 78	27	Not used	Unassigned
P 79	–	P8	Position identifier #8

The time quality indicator code, as defined in detail in Table II, consists of a four-bit code, is used by several clock manufacturers, and is in several existing standards. It is an indicator of time accuracy or synchronization relative to UTC and is based on the clock's internal parameters. The code presented here is by order of magnitude relative to 1 nanosecond. The 1-nanosecond basic reference is fine enough to accommodate all present industry uses now and into the foreseeable future. As an example, with GPS technology at better than 100-nanosecond accuracy level, a 0000 code (indicating the source is locked) goes to a 0011 or a 0100 code when it loses lock. Note that the usage of 0000 precludes the accuracy information, so some vendors always transmit the actual accuracy field.

TABLE II
IRIG-B CONTROL FUNCTION TIME QUALITY INDICATOR CODE

Binary	Hex	Value (Worst-Case Accuracy)
1111	F	Fault—clock failure, time not reliable
1011	B	10 s
1010	A	1 s
1001	9	100 ms (time within 0.1 s)
1000	8	10 ms (time within 0.01 s)
0111	7	1 ms (time within 0.001 s)
0110	6	100 µs (time within 10^{-4} s)
0101	5	10 µs (time within 10^{-5} s)
0100	4	1 µs (time within 10^{-6} s)
0011	3	100 ns (time within 10^{-7} s)
0010	2	10 ns (time within 10^{-8} s)
0001	1	1 ns (time within 10^{-9} s)
0000	0	Normal operation, clock locked

V. IEEE 1588 STANDARD

The IEEE 1588 standard defines a method to share precise time with multiple network elements. This standard also defines a Precise Time Protocol (PTP) that is used to calibrate out the delays introduced by the network communications paths and the network element pass through delays.

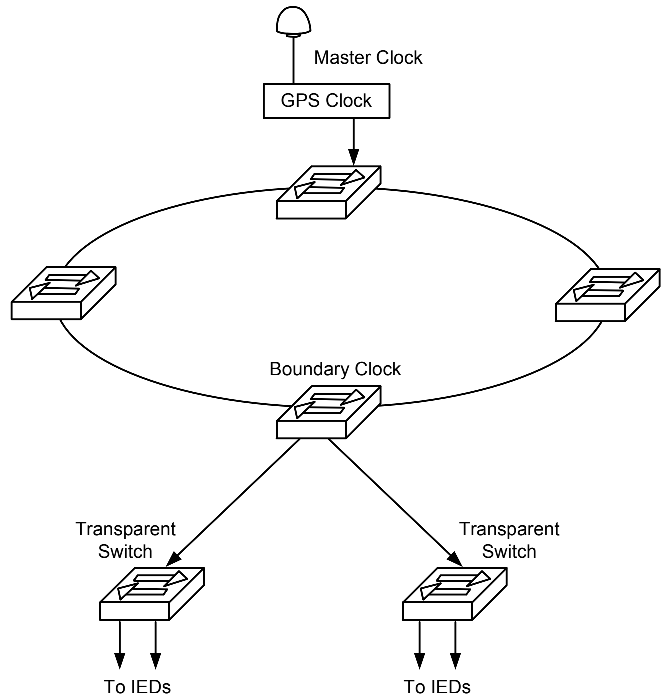

Fig. 3. Time-distribution hierarchy using the IEEE 1588 standard

The primary advantages of the IEEE 1588 precise-time distribution method compared to IRIG-B are:

- The need for separate time-distribution cables is eliminated.
- When more than one master clock is used, source redundancy is achieved.

One disadvantage is that it is an Ethernet-based protocol and therefore does not support legacy IRIG-B devices or products that are not Ethernet capable. The IEEE is currently developing a standard profile for use by the power industry. This profile will be draft standard IEEE C37.238.

VI. SYNCHROPHASOR APPLICATIONS

Synchronized phasor measurements or synchrophasors provide a means for comparing a phasor to an absolute time reference. The availability of high-accuracy satellite-synchronized clocks makes synchronized phasor measurement possible. Through the use of the clock, the phasor measurement unit (PMU) produces a reference sinusoidal wave. This reference wave is a nominal frequency sinusoidal wave for which maximum occurs at the exact start of each second. The measured local voltage or current is then compared to this reference wave, as shown in Fig. 4.

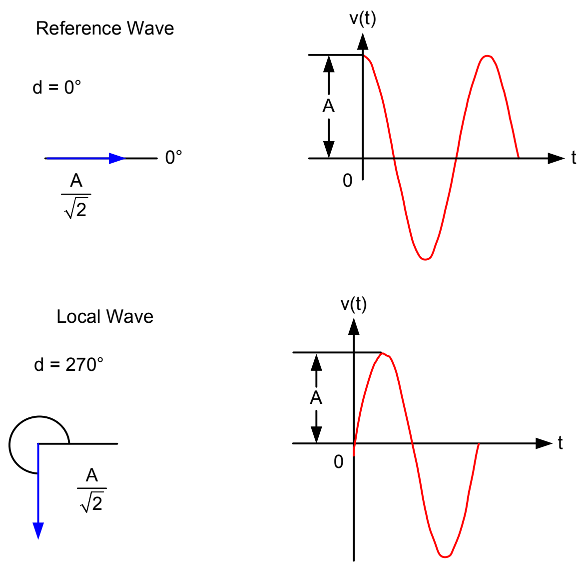

Fig. 4. Reference wave and local wave with angular comparison

Because the reference wave is dependent on a GPS-generated time signal, this wave will be the same at all different PMU locations. Therefore, a local phasor can be compared with a phasor at any other location, and the angular difference between the two phasors represents the absolute difference between the two locations. In this application, any time offset between the sampling intervals at two locations results in an angular mismatch or error in the synchrophasor data. Time alignment is just one error source.

To date, synchronized phasor measurements have been used mainly for power system model validation, post-event analysis, real-time display, and other similar activities. However, synchrophasors have a greater potential than monitoring and visualization. Synchrophasors increasingly contribute to the reliable and economical operation of power systems as real-time control and protection schemes become broadly used. The availability of precise time over a wide area, as provided by the GPS system, becomes more critical as we shift from a monitoring to a control mode [2].

VII. IEC 61850 Process Bus

IEC 61850-9-2, Communication Networks and Systems in Substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled Values Over ISO/IEC 8802-3 specifies that the current transformer (CT) and voltage transformer (VT) outputs that are presently hard-wired to various devices (relays, meters, IEDs, and supervisory control and data acquisition [SCADA]) be digitized at the source and then communicated to those devices using an Ethernet-based local-area network (LAN).

Sampled Values (SV) data must be synchronized to a common time reference in order to be useful for protection and control applications. Currently, the IEC 61850 series of standards recommends the Network Time Protocol (NTP) as the primary synchronization method and recognizes the fact that the NTP time accuracy (0.1 to 1 millisecond) is insufficient for SV applications which require <1 microsecond accuracy. The standard therefore allows time to be distributed by independent means as well; Fig. 5 shows the use of an external time source. To achieve microsecond-level time synchronization to date, IRIG-encoded time signals from GPS clocks are used. In the future, IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems will be used to distribute the 1-microsecond accuracy timing required. IEEE 1588 uses the existing LAN cables to distribute high-accuracy time, eliminating the need for the additional IRIG cabling.

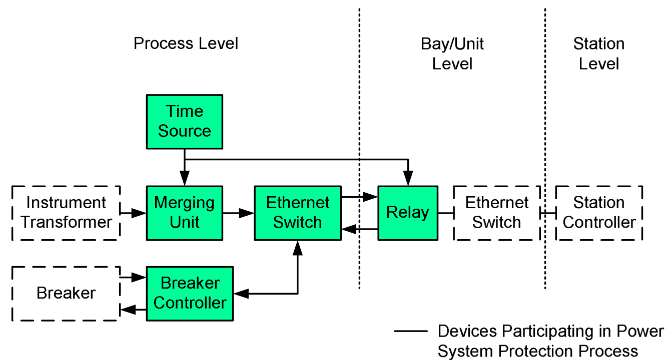

Fig. 5. IEC 61850 sample measured values system

The availability of precise time over a wide area, as provided by the GPS system, becomes critical as we shift from analog distribution of CT and VT data to process bus distribution as defined in IEC 61850-9-2. Without reliable, high-accuracy time, SV data become mostly useless [3].

VIII. GPS Vulnerabilities

The following section is an examination of possible causes and/or sources of GPS signal interference. It should be noted that the GPS system and GPS satellite clocks used in substations to date have provided highly accurate and reliable time. To further improve the reliability of any system, it is important to understand all possible interference sources. Many of the following, although interesting, are fortunately very rare.

A. Solar Flares

It has been known for some time that the GPS system can be disrupted by electromagnetic storms created by solar flares.

One major electromagnetic storm that occurred on October 28 and 29, 2003, reportedly had some GPS units down for as long as 19 hours.

These storms are caused by electrically charged particles and electromagnetic fields, which are spewed by the sun during the flare. These particles and fields travel relatively slowly toward earth. To the GPS receiver, these fields appear as high levels of background noise or as high energy in band signals, depending on the event. Space weather forecasters can usually give GPS users several hours to several days of warning that a disruption may be coming.

On December 5 and 6, 2006, two powerful solar flares occurred. The solar flare that occurred on December 6 produced fields ten times higher than previously recorded. In fact, at its peak, the flare produced 20,000 times more emissions than the rest of the sun. This energy was enough to disrupt GPS receivers on the entire sunlit side of the earth for approximately 10 minutes.

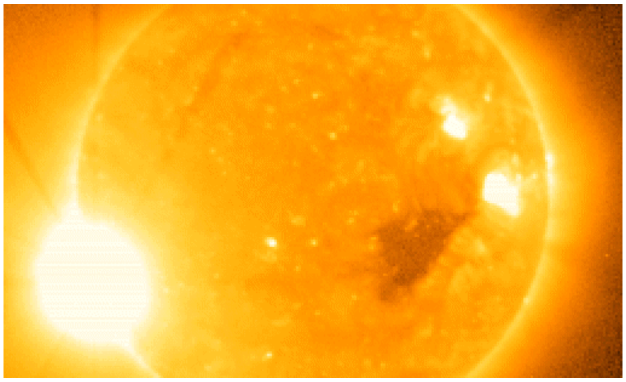

Fig. 6. Solar flare recorded December 5, 2006, by the X-ray Imager onboard the National Oceanic and Atmospheric Administration (NOAA) GOES 13 satellite.

Uncharacteristically, the emissions from the December 6 flare traveled at the speed of light and passed quickly through the atmosphere that usually blocks incoming radiation. As a result, GPS receivers were jammed with little to no warning. Another interesting fact about this flare is that it occurred during the solar minimum. The solar cycle is around 11 years. The solar minimum is the part of the cycle when the least amount of solar activity is expected.

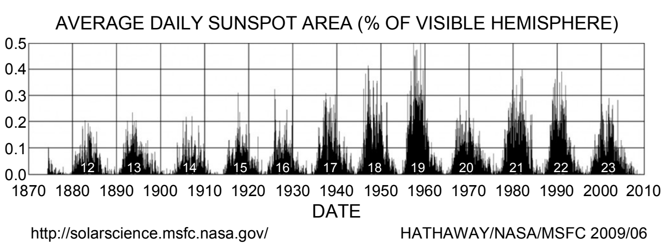

Fig. 7. Chart depicting the recorded solar cycles

We entered Solar Cycle 24 in 2008 and to date have experienced some of the lowest activity in the past 100 years. For example, in 2008 there were no sunspots observed on 266 of the year's 366 days (73 percent). The closest year with more blank suns was in 1913, which had 311 spotless days. The activity for 2009 so far appears to have dropped even lower. As of March 31, there were no sunspots on 78 of the year's 90 days (87 percent). This will all be ending shortly as the sun is moving into a period of solar maximum, which is expected to peak in 2012. Sunspots are planet-sized islands of magnetism on the surface of the sun. They are also sources of solar flares, coronal mass ejections, and intense ultraviolet (UV) radiation.

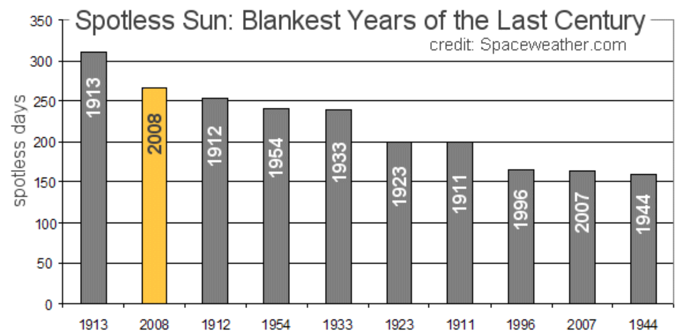

Fig. 8. Graph of the ten most spotless years of the sun in the last century

B. *Intentional GPS Jamming*

> The GPS signal strength measured at the surface of the earth is about –160 dBw ($1 \cdot 10^{-16}$ watts), which is roughly equivalent to viewing a 25-watt light bulb from a distance of 10,000 miles. This weak signal can easily be blocked by destroying or shielding the GPS receiver's antenna [4].

Because the received GPS signal is so weak, it can easily be jammed by transmitting a signal in the proper frequency range. This blocking signal will "blind" the GPS receiver from the intended satellite signals.

GPS jammers are more readily available than you might expect. Rental car agencies, taxi companies, and almost all delivery vehicles use a combination of GPS and cell phone technology to keep track of where their vehicles are located. Even the popular OnStar® service offered by General Motors uses this technology. Many people feel this is an invasion of their privacy and seek ways to defeat these systems. The manufacture and use of these personal countermeasures have developed into a niche market for the paranoid and those with illegal intentions. Most of these devices have very short effective ranges, in the order of 5 to 10 meters. There are many plans to build these devices available on the Internet as well; these homemade devices are capable of much stronger signal strengths and have a larger range.

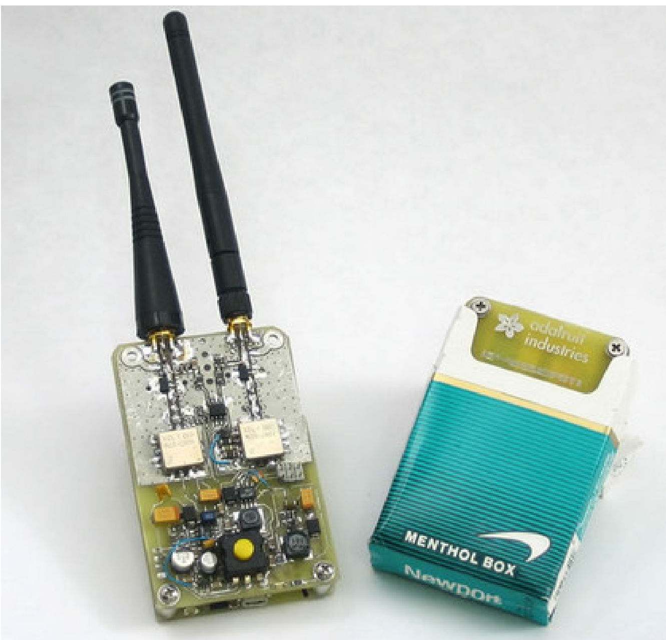

Fig. 9. Commercially available GPS and Global System for Mobile communications (GSM) jammers

GPS and GSM blockers, when used in vehicles to prevent Big Brother from watching the daily travels of a paranoid rental car customer or "detoured" delivery vehicle, can also prove to be a nuisance if located too closely to a substation GPS antenna. It should be noted that there are no known incidents of this occurring.

Another source of GPS interference can be the federal government. The following is an excerpt from an "Overview of the U.S. Federal Government's Policy on Activities Which May Cause Interference to GPS":

> On occasion, the US Federal Government is required to conduct GPS interference tests, exercises and training activities that involve jamming of GPS receivers. These events go through a lengthy coordination process involving the Federal Aviation Administration (FAA), the US Coast Guard (USCG), the Department of Defense (DoD) and other government agencies.
>
> Due to the fact that these training and testing activities can involve a number of aircraft, ships and/or other military equipment and up to hundreds of personnel, cancellation or postponement of a coordinated test should only occur under compelling circumstances. In general, only safety-of-life/safety-of-flight conflicts warrant cancellation or postponement of a coordinated interference test. [5]

GPS jamming (if an issue at all) would most likely affect individual GPS receivers and not a wide area.

C. *Intentional GPS Skew*

1) *Selective Availability*

The initial implementation of the GPS system had a random error factor of up to 100 meters. Selective Availability (SA) was turned off in 2000.

2) *GPS Spoofing*

GPS spoofing is performed similar to GPS jamming except that instead of using a strong interference signal, a counterfeit GPS signal is sent. The victim GPS receiver locks on to the stronger signal and accepts the incorrect data. There are many GPS test systems available that produce multiple simulated satellite signals at a very low level. Combined with the proper amplifier, these test systems can be converted into counterfeit sources.

D. *Other Possible Issues*

The DoD and U.S. Department of Transportation (DoT) have committed to make GPS available to civilian users at all times, except in a national emergency. The departments also commit the United States to provide the signal worldwide without a fee for a minimum of 10 years.

IX. Wide-Area Time Distribution

With the commercial availability of GPS, high-accuracy synchronized time is widely available. More recently, GPS time sources have become less expensive while providing even higher accuracy. These GPS clocks are in wide use today, operating with protection, monitoring, and control devices. Through the use of GPS, time synchronization of better than 1 microsecond worldwide is now realized. The availability of these time sources on the power system has already greatly improved the process of event analysis and is enabling applications such as synchrophasor measurement and process bus.

Application reliance on high-accuracy time has changed the role of the GPS receiver from an accessory to a required piece of hardware. As with substation protection devices, one method of achieving high reliability is through redundancy. Critical protection systems often have primary and backup components.

Compliance to industry environmental specifications, such as the IEEE and IEC standards, is another method used to ensure hardware robustness in the harsh substation environment.

Using redundant GPS receivers, as shown in Fig. 10, is one method to avoid a single point of failure for the time signal. This requires additional hardware to select the source device and provide the distribution of the time signals. This method provides redundant clocks but still introduces a single point of failure at the source selector and distribution device. One solution that could provide more reliability is the ability of the GPS clocks to accept high-accuracy signals from each other. Each clock uses its own internal received signal and selects the signal from the other clock upon local receiver trouble, as shown in Fig. 11.

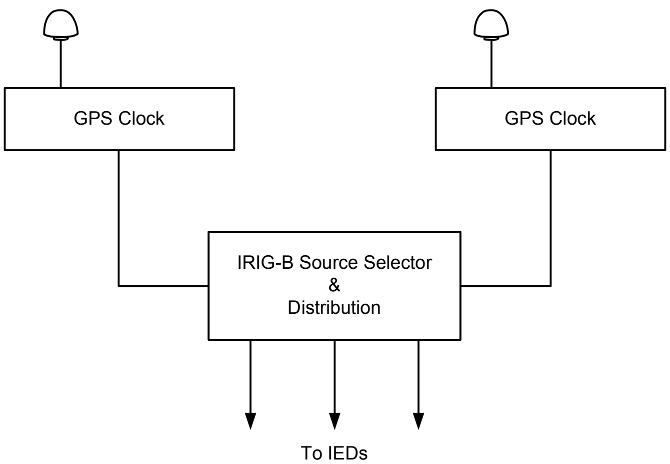

Fig. 10. Redundant clock sources with failover

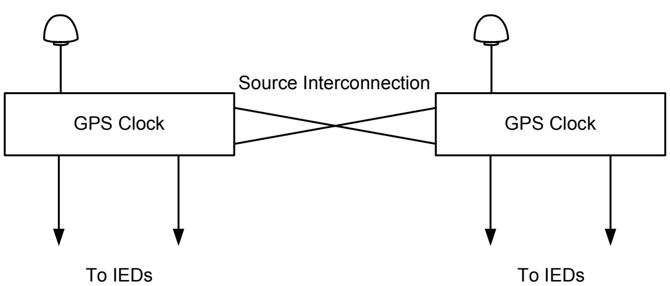

Fig. 11. Redundant clocks providing backup for each other

The methods demonstrated in Fig. 10 and Fig. 11 provide hardware redundancy all the way to the antenna and feed lines. In the case of a catastrophic failure, such as a power supply failure, the IEDs receiving timing information from that clock will lose their time source.

Clocks that support the IEEE 1588 standard will have more options for alternate time sources. The IEEE 1588 standard defines a method of providing high-accuracy time over an Ethernet network. With this type of transportability, the redundant time signal can now be provided by the clock in an adjacent substation, as shown in Fig. 12.

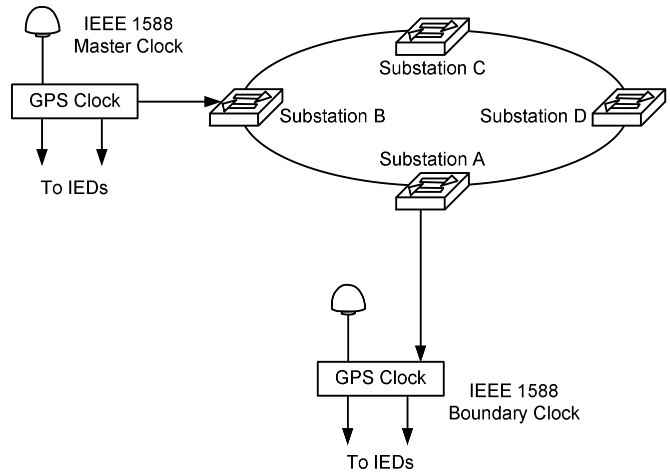

Fig. 12. IEEE 1588 time distribution uses multiple noncolocated clocks

X. SONET Communications and Timing

Communications systems that utilize time-division multiplexing (TDM) techniques are frequency-synchronized (syntonized) by design. Early multiplexer systems, such as T1 and T3, used a plesiochronous synchronization method. These systems, known as PDH systems, operated at the same nominal digital rate but were synchronized with different clocks. This meant that occasional data slips would occur to keep the system synchronized.

Synchronous optical network (SONET) technology solved this problem through tight control over the synchronization and use of a centralized system clock. GPS clocks are typically used to provide the frequency synchronization source for SONET networks. A typical SONET network will always have one Stratum 1 (±10ppt) clock and most likely a second Stratum 1 clock for redundancy or backup, as shown in Fig. 13.

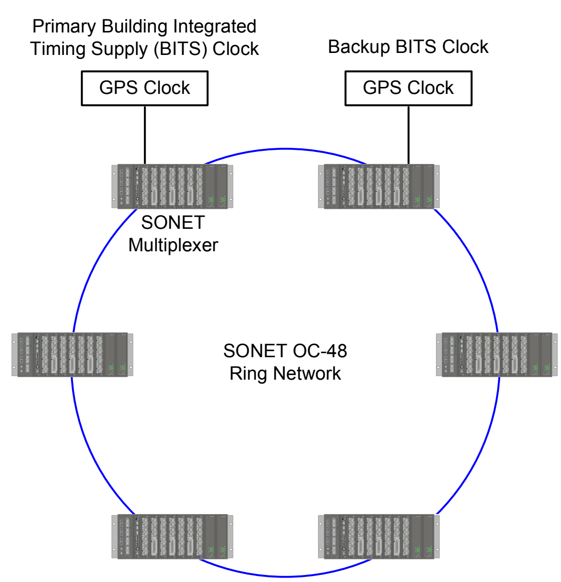

Fig. 13 SONET system with a primary and backup Stratum 1 timing source

Today many substations are equipped with GPS clocks, and all of these clocks are linked through satellite communications. These clocks are also capable of autonomous operation when the satellite link is lost, with some performance degradation over time. Therefore, if anything were to cause interference in the area of one substation, only the clock at that substation and associated IEDs would be affected.

Wide-area synchronization currently exists through the use of local GPS receivers. The goal is to make the system more robust. One solution is to interconnect all of the clocks.

SONET and Ethernet systems use ring topologies to provide traffic survivability during communications link failures. The proposed system provides a ring topology for the GPS clocks. With all of the clocks in the system networked in a ring topology, the loss of single or multiple satellite downlinks will not disrupt the distribution of high-accuracy timing information. In addition, this clock topology solves issues caused by jamming signals, a broken element in the antenna system, or any other localized disturbances.

When the GPS clocks are interconnected through the communications network, an exponentially more robust time system will result.

When we integrate the clock into the communications system and use the information from all (legitimate) time sources in the network, average all of the individual times at each terminal, a timing flywheel is created.

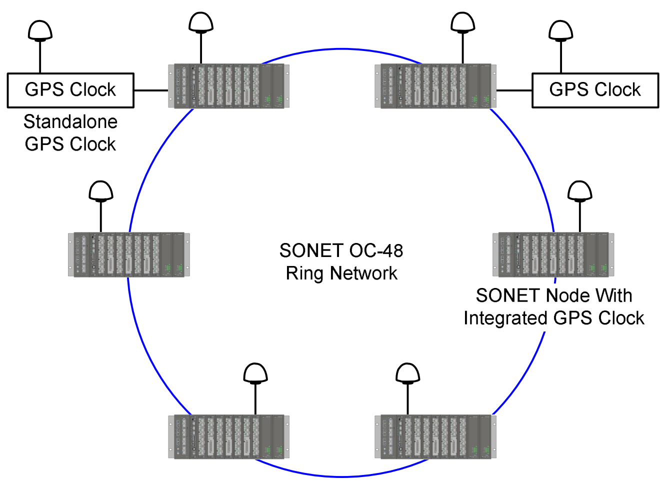

Fig. 14. SONET system with integrated GPS receivers for high-accuracy time distribution

This system has many high-accuracy sources (<1 microsecond) available and uses these to perform frequency source averaging to create the time flywheel. Due to the number of potential time sources in the system, clocks that are greater than a set tolerance off from the system average can be identified. These rogue clock signals are ignored by the system until their output comes into compliance. This methodology prevents spoofed GPS clocks from causing errors in the system. Even the local node is able to identify that the local time signal is in error and cannot be trusted, based on a comparison to the system time.

For added stability, the system can also accept high-accuracy timing signals from external clocks. However, if the external clocks are of similar design, they will be susceptible to the same local interferences. The recommended alternative would be a GPS trained cesium atomic clock. Although the GPS portion of the clock is susceptible to common GPS clock issues, the holdover accuracy of a cesium-based clock is capable of providing high-accuracy time for a much greater time period than a standard crystal oscillator-based clock. The addition of a cesium clock to the system offsets the effect a large solar flare could have on the system, where all of the receivers in any one network would most likely be affected. With the addition of an atomic clock, the system provides ride through for any temporary major GPS outage.

XI. System Performance

Should there be a solar flare or a total GPS failure and no atomic clock source in the proposed network., the time flywheel maintains a high-accuracy (<1 microsecond) relative time. This means that all of the clock signals provided by the system will be within 1 microsecond relative to each other. The system time will drift off from UTC time over time.

Maintaining relative time is important. Sample measured values rely on accurate time available between substations; we can continue to trust the measurements. Wide-area control systems using synchrophasor data can continue during a temporary loss of GPS timing.

Can the system initialize without availability? The proposed timing system will converge relatively quickly on a time. This time will be the average of all the unsynchronized clocks. The time will not be very close to UTC time, but all nodes in the system will be within 1 microsecond of each other. Fig. 15 demonstrates the convergence process of an eight-node system consisting of two four-node rings interconnected. As demonstrated in the graph, when the nodes are as far as 10,000 units apart, the system still synchronizes within 20 time samples. Each bar in the chart represents the local-time offset at each of the eight nodes.

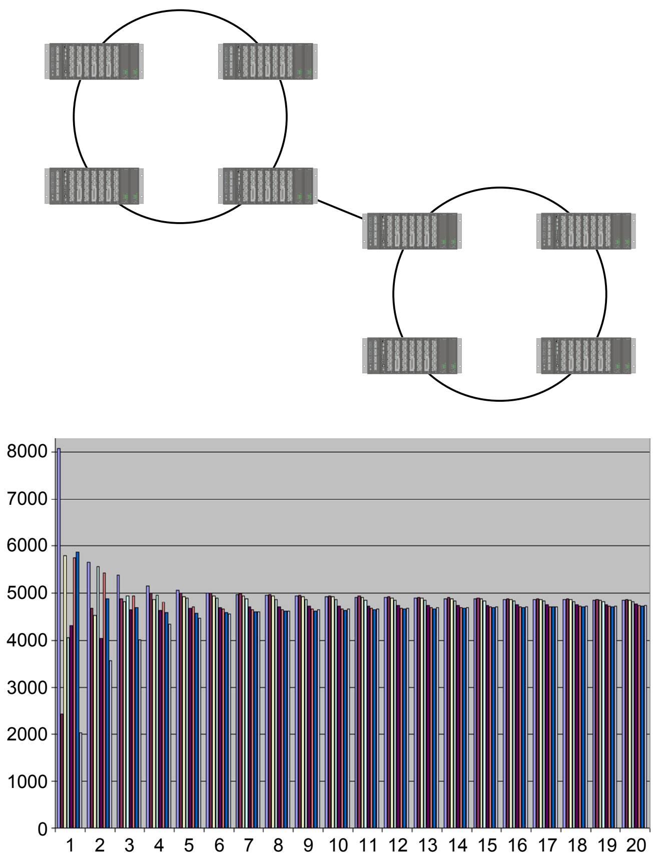

Fig. 15. Convergence of time across a dual-ring eight-node system

XII. Conclusions

The GPS satellite network has been providing reliable high-accuracy time for many years now.

The GPS system can be interfered with both intentionally and cosmically.

With the wide-scale implementation of technologies such as sample measured values and control systems using synchrophasor data, extremely reliable high-accuracy time has now become a requirement.

There are many ways to provide reliable time. This paper has discussed the advantages and disadvantages of a few.

A system that is capable of providing highly reliable relative time allows islanded sample measured value and synchrophasor systems to continue to operate even with a total loss of the GPS system.

XIII. References

[1] K. Behrendt and K. Fodero, "The Perfect Time: An Examination of Time-Synchronization Techniques," proceedings of the 60th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, May 2006.

[2] R. Moxley, "Synchrophasors in the Real World," proceedings of the 7th Annual Western Power Delivery Automation Conference, Spokane, WA, May 2005.

[3] V. Skendzic, I. Ender, and G. Zweigle, "IEC 61850-9-2 Process Bus and Its Impact on Power System Protection and Control Reliability," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[4] J. S. Warner and R. G. Johnson, "GPS Spoofing Countermeasures," Los Alamos National Laboratory, December 2003.

[5] U.S. Coast Guard Navigation Center (U.S. Department of Homeland Security), "Overview of the U.S. Federal Government's Policy on Activities Which May Cause Interference to GPS." Available: http://www.navcen.uscg.gov/gps/gpsnotices/default.htm.

XIV. Further Reading

E. O. Schweitzer, III and D. E. Whitehead, "Real-Time Power System Control Using Synchrophasors," proceedings of the 62nd Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, May 2008.

IEC 61850-9-2, *Communication Networks and Systems in Substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled Values Over ISO/IEC 8802-3*, First Edition, 2004.

IEC 61850-9-2 LE (Lite Edition), *Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2*, UCA® International Users Group, 2004.

XV. Biographies

Ken Fodero is currently a research and development manager for the time and communications product lines at Schweitzer Engineering Laboratories, Inc. (SEL) in Pullman, Washington. Before coming to SEL, he was a product manager at Pulsar Technology for four years in Coral Springs, Florida. Prior to Pulsar Technology, Ken worked at RFL Electronics for 15 years, and his last position there was director of product planning.

Chris Huntley, P.E. received his M.A.Sc. in engineering physics from the University of British Columbia in 1960. After a two-year Athlone Fellowship in the United Kingdom and a diploma in electrical engineering from Imperial College, Chris joined the research and development group of GTE Lenkurt Electric in Burnaby, B.C. Here he designed both analog and digital (FDM and SONET) multiplexer products, including teleprotection interfaces (DTT, HCB, C37.94) under a variety of owners from GTE and B.C. Tel through Nortel and GE. In 2007, he started a communications development group for Schweitzer Engineering Laboratories, Inc. in Burnaby, B.C. He is a senior member of IEEE and is active in many IEC, Cigre, and AES professional groups. He also holds 10 patents on communications circuit technologies.

David Whitehead, P.E. is the vice president of research and development at Schweitzer Engineering Laboratories, Inc. (SEL). Prior to joining SEL, he worked for General Dynamics, Electric Boat Division as a combat systems engineer. He received his BSEE from Washington State University in 1989, his MSEE from Rensselaer Polytechnic Institute in 1994, and is pursuing his Ph.D. at the University of Idaho. He is a registered professional engineer in Washington and Maryland and a senior member of the IEEE. Dave holds seven patents with several others pending. He has worked at SEL since 1994 as a hardware engineer, research engineer, and chief engineer/assistant director, and has been responsible for the design of advanced hardware, embedded firmware, and PC software.

20100114 • TP6395-01