It’s About Time—Considerations and Requirements for DSS and Line Current Differential Applications

Ed W. Chen
Consolidated Edison

Brian Smyth, Marcel van Rensburg, and Manodev Rajasekaran
Schweitzer Engineering Laboratories, Inc.

Presented at the
8th Annual Canada Protection Symposium
Toronto, Canada
December 5–7, 2023

Originally presented at the
76th Annual Georgia Tech Protective Relaying Conference, May 2023

It's About Time—Considerations and Requirements for DSS and Line Current Differential Applications

Ed W. Chen, *Consolidated Edison*
Brian Smyth, Marcel van Rensburg, and Manodev Rajasekaran,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—Protection engineers are increasingly using time synchronization for protection applications as modern technologies evolve. Protection applications that rely on time synchronization require a thorough analysis of how any changes in time-synchronization accuracy and reliability can impact these applications. Additionally, the knowledge of different time-synchronization protocols, mediums, and distribution methodologies is critical for proper operation and reliability. Designs that were sufficient less than a decade ago for automation or control applications could be insufficient for modern technologies where protection schemes rely on more stringent time synchronization.**

This paper discusses considerations that a protection engineer must evaluate for a line current differential protection scheme when applying GNSS (Global Navigation Satellite Systems) for data alignment. Additionally, the authors present the differences between local and global time-source synchronization and how it can affect the performance of digital secondary system (DSS) applications. The authors explain lessons learned from several DSS installation support activities, focusing on protection schemes and schemes that combine conventional and DSS-based relays. Time-synchronization protocols, such as IRIG-B, IEEE C37.118, IEEE 1588 Precision Time Protocol (PTP), and the distribution of the time signal must be applied using the best practices, as discussed in this paper, to ensure a robust and secure design. Commissioning tips are also provided to help guide successful implementation of time into the various protection schemes.

Finally, the paper presents four cases highlighting line current differential and DSS-based applications where an improper time-source configuration led to undesired behavior of the protection scheme. These cases focus on the time-source installations and how the time-source configuration led to the undesired behavior.

I. INTRODUCTION

Coordinated Universal Time (UTC) has been used since the early 1960s to bring a common time reference to multiple locations and applications all over the world. UTC does not include compensation for different time zones, instead end devices can add a UTC offset to adjust the hours to derive their local time. UTC is based on the time at Greenwich, England, and effectively replaces Greenwich Mean Time The time must be occasionally updated to account for differences in the Earth's rotations, and this is accomplished using leap seconds. The International Earth Rotation and Reference Systems Service is responsible for monitoring the Earth's rotation and publishes a bulletin notifying of a pending addition of a leap second. It is important to note that, in the future, leap seconds may be removed.

With a common global time reference available, the next challenge is distributing the time all over the world with precision. In 1973, the U.S. Department of Defense helped develop a satellite-based radionavigation system called the Global Positioning System (GPS). This system is operated by the U.S. Air Force and owned by the U.S. Government (see Fig. 1). With 30 operational satellites, a receiver can pinpoint its location to within a few meters and calculate how long it took to receive a signal within ten nanoseconds [1].

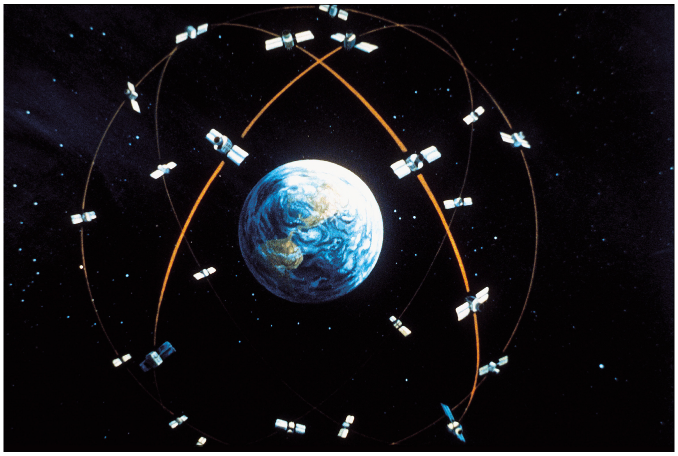


Fig. 1 The GPS is a constellation of over 30 Earth-orbiting satellites.

Several equivalent versions of GPS exist, such as Galileo, which is what the European Union uses , and additionally, Russia's system called GLONASS, and China's BeiDou system. These GNSS systems are generally referred to as high-accuracy positioning, navigation, and timing (PNT).

As technology evolves and the reliability of these PNT systems improve, humanity is finding new ways to apply them in a variety of new applications. Power system protection is one application that is evolving and requires new ideas and improvements, which includes utilizing time.

II. TIME SOURCES AND APPLICATIONS

This paper refers to satellite-based radionavigation systems such as GPS as GNSS or global reference signals, since there are different versions all over the world.

Some devices use a global reference directly while others are meant to redistribute it to even more end devices. Clocks play the important role of synchronizing to a global reference and providing a means to distribute time to other end devices. If an end device, such as a protective relay, uses an external clock to update its own internal clock, then it must know how accurate the external clock providing that time is compared to the true

UTC time. International standards were developed to define the behavior of time accuracy for various applications. These standards include but are not limited to IEEE C37.118, IEEE 1588, IEEE C37.238, and IEC 61850-9-3.

Information typically embedded within the time message indicates the accuracy of the clock that is providing the signal and is referred to as time quality. This information provides the end device with the accuracy of the clock so the device can determine if it is accurate enough to synchronize its internal clock to. Some protection and monitoring applications specify a 1 μs accuracy to UTC time and if the external clock is not within that specification, the end device can choose to ignore the input signal and switch to its own internal clock to continue to keep time.

In timekeeping systems, the term *stratum* is used to define the level from an authoritative time source. Each stratum level is assigned a number, starting with zero for the reference clock at the top of the hierarchy. A Stratum 0 device is connected directly to a high-precision time source to provide a reference clock. An example Stratum 0 device would be an atomic clock or a GNSS. A Stratum 1 device obtains time by synchronizing to a Stratum 0 reference, and an example would be a GPS clock that obtains time from a GNSS that is synchronized to an atomic Stratum 0 reference.

One important understanding in applying clocks and time in protection and automation applications is the concept of holdover. When a clock loses its Stratum 0 reference, such as time provided by GNSS, and is relying on its own internal components to keep time, it is said to be the holdover state. Clocks provide a constant time update to end devices, but what happens if the clock loses its Stratum 0 reference? Since the clock is providing such important information, and applications such as protection are relying on it, methods must be applied to ensure dependability. Clocks use an internal oscillator crystal to keep time in absence of the global reference signal. These components are oscillating at an approximate frequency, and this is used to count in time. However, no oscillator is truly perfect and based on its frequency variation, temperature, quality control during manufacturing, and its implementation, it will have some amount of drift. End devices typically use lesser quality oscillators and rely on external clocks to provide the correct reference to update it. One example of this is a clock in a microwave oven. Since its clock is not updated by a global reference signal, after it is set it will drift away from the UTC time. If this time is never adjusted, over a year for example, it will be a few minutes off from another clock that is tied to a global reference, such as a cellphone. The advantage of using a global reference signal is that the clock can constantly update and correct this drift and maintain a very accurate representation of the UTC time. Since protective relays use standards to drive their behavior, the notion of 1μs will be used for this discussion. An end device internal oscillator can keep a 1μs accuracy to UTC time for typically less than one minute. Without a correction from a global reference or an external clock, the internal time in that device will drift more than 1 μs from the UTC time and any function relying on time may be affected.

Better oscillators have been developed to allow for longer holdover states while maintaining the required accuracy. By controlling the development process, these oscillators can obtain lower drift rates and allow a clock to maintain the 1 μs accuracy requirement for much longer. Two types of oscillators will be discussed: temperature-compensated crystal oscillator (TCXO), and oven-controlled crystal oscillator (OCXO). The oscillator frequency can be affected by temperature and causes variation in the output, which directly affects the total drift rate of the oscillator. By compensating the output frequency of the oscillator for various temperatures, the oscillator can maintain a better output [2]. A TCXO oscillator uses a thermistor network to measure the temperature and appropriately compensate the output frequency of the oscillator. An OCXO oscillator uses a small heater on the chip to control the temperature. This makes the OCXO oscillator larger in size and can draw appropriate amounts of power. This is why TCXO oscillators are ideal for smaller portable electronic devices such as cell phones. Since the OCXO oscillator can control the temperature directly, it allows for better accuracy over a wider temperature range. A typical drift rate of an OCXO oscillator is approximately 5μs/ day while a TCXO is 36 μs/day at constant temperature but can be more than 300 μs/day for temperatures ± 1 degree C of the specified temperature. The drift rate directly corresponds to the holdover accuracy of the clock while not receiving an update from a global reference signal. For example, if a clock has an OCXO oscillator with a specified drift rate of 5 μs/day, it would be able to be in holdover, i.e., lose the global reference signal, and still provide a 1 μs accuracy output for almost an additional 4.5 hours. This can play a very important role when using this type of clock for protective relay applications. Comparatively, a TCXO oscillator would maintain a 1 μs accuracy for up to an additional 40 minutes after the loss of the GNSS reference signal.

Historically, time synchronization has not been used directly in power protection schemes. Most applications involving time synchronization were related to communications and event reporting. Supervisory control and data acquisition (SCADA) systems were among the first types of applications using time references for data alignment. In these applications, the client device polls for information from remote server devices every five seconds. However, today more applications are applying time because of the improvements made to clock accuracy and resiliency to loss of its global reference signal. Synchrophasors is an application that uses synchronized voltage and currents measurements taken at the same instant in time. This technology has been used for a variety of applications including, but not limited to:

- Determining power system modes of oscillation.
- Voltage stability studies.
- Detection of islanding conditions.
- Detection of power swing and out-of-step conditions.
- Event analysis.

For synchrophasor applications, the IEEE C37.118 standard defines a 1us accuracy to properly time stamp the voltage and current measurements and produce a synchronized measurement with less the one percent total vector error.

Line current differential is a protection scheme that relies on communications and, in addition, needs to account for communication delay. If accurate time is available at both ends of a line, then time can be used to align data and compensate for the communication delay. There are many advantages to this approach, but it can also create challenges. Section IV explains how time can be utilized in these applications. Additionally, digital secondary systems (DSSs) require time for data sample alignment, and Section V explains the challenges and considerations for these applications.

III. TIME-SOURCE DISTRIBUTION METHODS

Clocks can distribute time to multiple end devices through various protocols and different media types. Some methods rely on a direct or distributed cable connection from the time source, while newer technologies are evolving to distribute time over local-area networks (LANs) and wide-area networks (WANs).

A. *Cable-Connected Time Distribution*

IRIG Standard 200-04 is one method for the redistribution of time [3]. There are multiple formats within this specification, and they are denoted by a suffix letter. For electric utility applications, the suffix B is used, and is referred to as IRIG-B. IRIG-B is typically distributed to the end device via coaxial cable with a BNC connection. Additionally, IRIG-B can be distributed over a serial cable connection, which is very useful in protective relays since most relays have a serial cable connected to them for general communications. This serial communication cable can carry the IRIG-B signal on a single pin of that cable saving installation costs of running a separate cable. Communications processors can be used for this application, receiving an IRIG-B signal from an external clock, and then redistributing that signal to multiple end devices. Fig. 2 represents a typical IRIG-B signal distribution system, demonstrating a clock providing time to an end device, such as an intelligent electronic device (IED), directly or through a communications processor that is used to distribute to multiple IEDs.

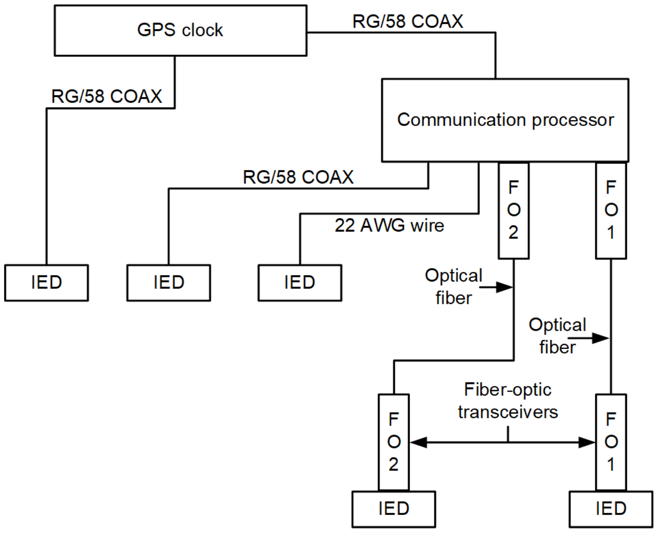


Fig. 2 Typical IRIG-B signal distribution.

B. *LAN and WAN Time Distribution*

Newer technologies include distributing time over an Ethernet network. IEEE 1588 is a standard that defines how this can be achieved over a complex network that has a significant amount of variability. Precision Time Protocol (PTP) was developed to account for the packet delay variation, pass through delays, and communications media latencies within an Ethernet network and can compensate for the delay in the signal, so when the end device receives the signal it can still be within the required accuracy. PTP is applied using a grandmaster (GM) clock which is then distributed through transparent clocks to an end device. Since multiple clocks can be added to a network, a GM needs to be defined. An end device, such as a relay, must be able to receive a PTP message and any intervening switch that is in the network path to the end device must be PTP aware. Switches that are PTP aware add information to the Ethernet message indicating the added delay so that it can be appropriately compensated for at the end device. Additionally, PTP can be applied to a Parallel Redundancy Protocol (PRP) network. In this type of application, information is duplicated on two separate LANs. Fig. 3 demonstrates this type of configuration.

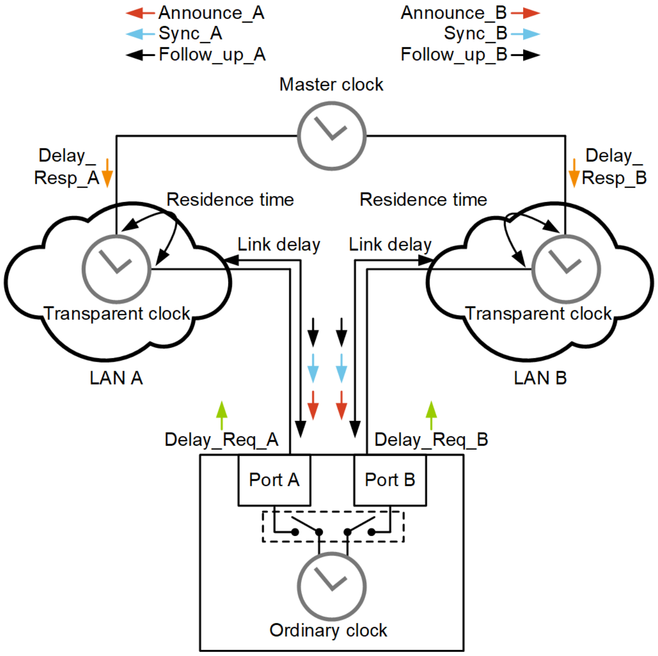


Fig. 3 PTP time synchronization of a PRP network.

This type of network allows an end device to synchronize to a single clock that is providing time over two independent LANs. A Best Master Clock Algorithm (BMCA) will select the master clock with the best accuracy and the lowest path delay. For example, if information from LAN A is received on Port A of the end device and information is received from LAN B on Port B, the BMCA can determine the best network between LAN A and LAN B, since they are connected to the same GM. This configuration provides some resiliency in the case that one of the LANs fail, such as a switch failing, since the alternate LAN can still provide time. The figure also shows transparent clocks (Ethernet switches), which are clocks that receive the time from the GM clock, update their time reference, *and* transparently pass the information on to the end device.

A separate GM clock can be used for each LAN, but this is not recommended for IEC 61850-9-2 Sampled Values DSS applications. This is because the end devices may employ different BMCA algorithms and may choose the clock accuracy based on network location and delay from each GM, and ultimately lock to different clocks.

C. Hybrid Time Distribution Network

Finally, hybrid solutions exist such as time distribution gateway (TDG). This type of application helps mitigate vulnerabilities that exist with a single source time reference. A TDG solution uses multiple local time inputs as well as highly accurate time from GNSS and distributes time across various WANs. Fig. 4 provides an example of a TDG network. For more information on TDG hybrid solutions refer to [4].

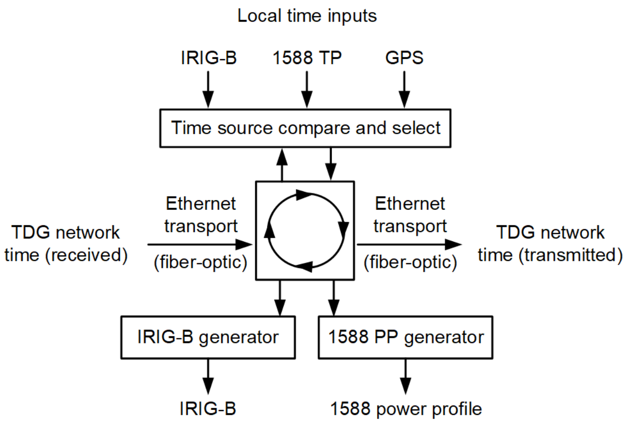


Fig. 4 TDG network.

IV. LINE CURRENT DIFFERENTIAL APPLICATIONS USING TIME

With the advancements in time resiliency and distribution methods, protective relays are applying more applications using GNSS time. One application is data alignment in line current differential protection schemes. This scheme is denoted by the ANSI number 87L.

Line current differential schemes are configured with a protective relay at each terminal creating a zone of protection. Fig. 5 shows a conventional two-terminal differential scheme with an alternate hot-standby channel. A hot-standby channel can be applied for seamless failover to an alternate channel in the case that the primary channel fails or degrades in synchronization quality.

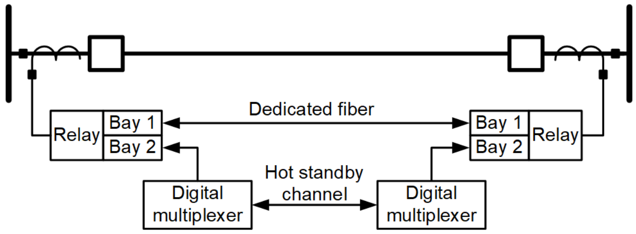


Fig. 5 Conventional two-terminal differential scheme.

87L protection uses a communications channel to exchange the measured currents at each terminal and applies Kirchhoff's current law to create a very simple and secure protection scheme. The main challenge for 87L schemes is that they require data to be realigned to account for delays through the communications channel, since the relays can be separated by large distances. 87L schemes are not limited to just two terminals but, rather, can be applied in three or more terminals, as well. Multiterminal line current differential applications are becoming more common as distributed generation and tapped loads are added to the bulk electric system.

The channel delay needs to be estimated so that the relays can align the local and remote current data properly. Data alignment can be accomplished in two ways. The first and most secure method is called channel-based synchronization, which is achieved using a ping-pong algorithm to estimate the clock offset between the two relays. This method utilizes a two-way travel time by exchanging some information over an approximately symmetrical channel (i.e., the latency in both the transmit and receive directions are equal). With the channel being symmetrical, the algorithm can calculate the one-way delay by dividing the roundtrip delay derived from the ping-pong message exchange by two. This method is very secure since it does not rely on any additional equipment to calculate the channel delay. An example of the channel-based, ping-pong exchange is shown in Fig. 6.

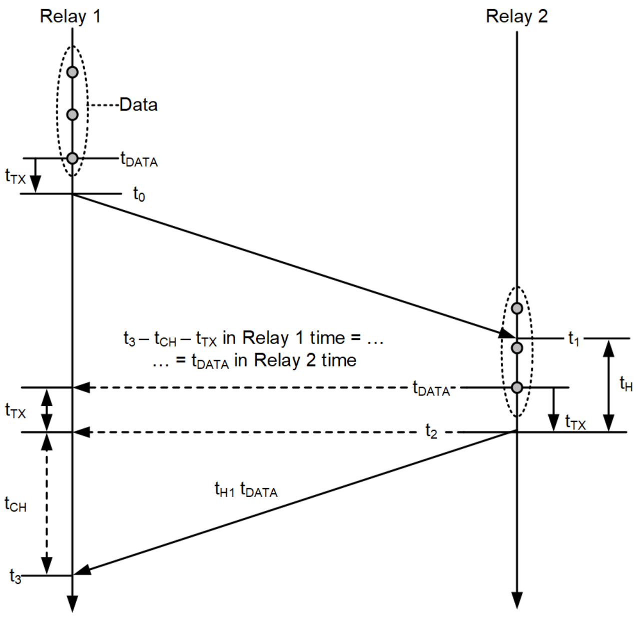


Fig. 6 Channel-based, ping-pong synchronization method.

Since the ping-pong algorithm depends on the channel being symmetrical, it does create challenges for communications networks which do not meet that requirement. If the channel is asymmetrical, it will cause data to be misaligned and create a false differential operate current. Line current differential algorithms, such as the generalized alpha plane, can provide some resiliency to these phenomena. The alpha plane, as shown in Fig. 7, uses a ratio of the equivalent local to equivalent remote currents and plots them in a real and imaginary plane [5].

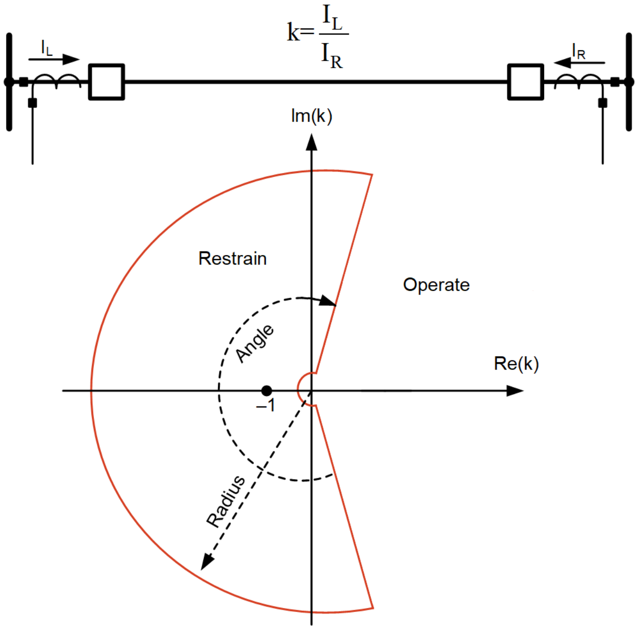


Fig. 7 Traditional alpha plane characteristic.

The alpha plane ratio, k, has an ideal blocking point at –1. This plots in the restraint region when current that is flowing into the differential zone equals the current that flows out of the differential zone. Since the local and remote currents would be 180 degrees out of phase of each other ideally, when the ratio is taken, it plots at –1. Likewise for an ideal internal fault, the local and remote currents would be in phase and would plot on the right side of the alpha plane in the operating region.

Now consider misalignment of the local and remote currents caused by incorrect channel delay measurement caused by asymmetry in the communication channel. For every 1 ms that data are misaligned on a 60 Hz power system, a shift in the current will equal 21.6 degrees. This misalignment creates a false differential current as well as moves the k value in the alpha plane away from the ideal blocking point. Therefore, the alpha plane can provide some resiliency to misalignment but, at some point, channel asymmetry can exceed the security of the algorithm and another method needs to be applied.

For 87L applications with signification channel asymmetry and GNSS time is available, time-based synchronization can be used to align the data between multiple relays. This method uses external time sources to align the data samples, so they are taken at the same point in time (relative to the top of second), and provides time stamps to the data. Since the data are time stamped, the channel requirements to be approximately symmetrical are no longer required. Fig. 8 shows a simple configuration of time-based synchronization for an 87L protection scheme with a nonsymmetrical communications channel. Note, in Fig. 8, the clock source may be from two independent clocks, one at each terminal, and will be the most common application. A single time source distributed over an Ethernet network, such as PTP, could be represented as a single clock, as in the figure.

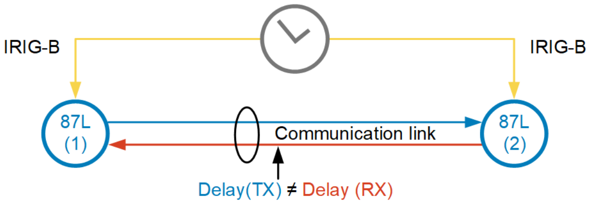


Fig. 8 Time-based 87L application with nonsymmetrical communications channel.

Another type of communications media gaining popularity for 87L protection is Ethernet. In this type of communications network, the channel transmit and receive delays are nondeterministic; therefore, time-based synchronization is required for data alignment. Ethernet communication is attractive because the differential relay needs only one connection to a network, which can then communicate to multiple remote relays in the differential zone. In a serial application, a dedicated point-to-point link is required, which limits the number of remote terminals a relay can communicate with due to hardware limitations.

Time-based synchronization adds the ability to apply line current differential protection in very challenging communication networks. However, it also exposes the protection to other modes of failure. For example, if the external clock providing the time reference fails, the line current differential protection could be affected, causing it to become unavailable or even cause an unintended operation. Some relays offer fallback modes that allow the differential protection to switch to the channel-based mode, or a hot-standby channel, if certain requirements are met. This provides a means to retain protection even in the absence of external time. However, in some applications, such as Ethernet communication or very asymmetric serial channels, this is not possible. In such cases protection would be impacted, so a stable and reliable global reference time signal combined with a clock with excellent holdover behavior becomes imperative. Section VI explains the challenges using time and some of the considerations a protection systems engineer should apply if time-based synchronization is applied in a protection scheme. Section VIII provides best practices as well as some commissioning tips for time-related applications.

V. DSS TIME REQUIREMENTS

DSSs define an application where measurement devices are placed near the primary equipment in the substation yard with the purpose of providing digitized samples and signals to protection relays in the control house. Fig. 9 shows an example DSS network.

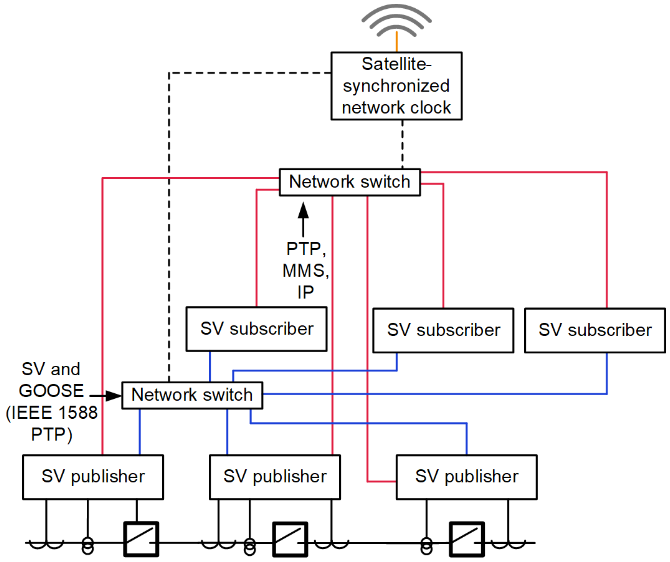


Fig. 9 Example DSS network.

To ensure coordination of the digital information that is distributed to multiple IEDs, a common time reference is needed. This time reference is provided by globally synchronized clocks with one of the several media available to the user. When considering IEC 61850-based applications, the preferred medium is fiber Ethernet cables using PTP, since the IEC 61850 solution already uses Ethernet as the means of communication between devices. Ethernet is not deterministic by nature, so this presents a challenge to the user designing an Ethernet network that is suitable for the application. Some protection functions use signals from both local and remote substation equipment, like line-protection relays discussed in this paper. This requires careful consideration in Ethernet network design for time distribution as well as selective disabling of the protection functions if the global time source is lost.

In a PTP network, every device in the network modifies PTP event messages to add the residence time, thus ensuring accurate compensation for network delays. A globally synchronized clock provides time that is traceable to International Atomic Time (TAI) and UTC time through a global time reference or a comparable global reference system. Data from devices synchronized to a global clock can be used in both local- and wide-area applications such as 87L schemes. A clock in a holdover state does not have the traceability to a GNSS source but can keep all devices in the local network synchronized to each other. Subscriber devices receiving data from merging units (MUs), each connected to a different local clock which is in a holdover state, cannot be used in wide-area applications.

Stratum 1 clocks that are referenced to a Stratum 0-time reference, such as a GNSS clock, can be affected by several factors that may cause it to lose high-accuracy synchronization momentarily or for periods of time. For this reason, these clocks can keep time very accurately and provide high-accuracy time to the IEDs subscribed to it. This is acceptable for some protection applications since any drift in time is applicable to all the local IEDs in the substation and does not affect the overall operation of the substation. This presents a scenario where devices allow for the use of certain functions and features while locally synchronized from a common clock with high-accuracy holdover timekeeping and selectively disabling some protection functions when the global high-accuracy time source is not present. This is defined as local and global time synchronization. Fig. 10 demonstrates how a clock can be used to provide local time synchronization when the PTP GM clock loses connection to the satellites. In this case, the clock goes into holdover and provides time to the local devices as a local source.

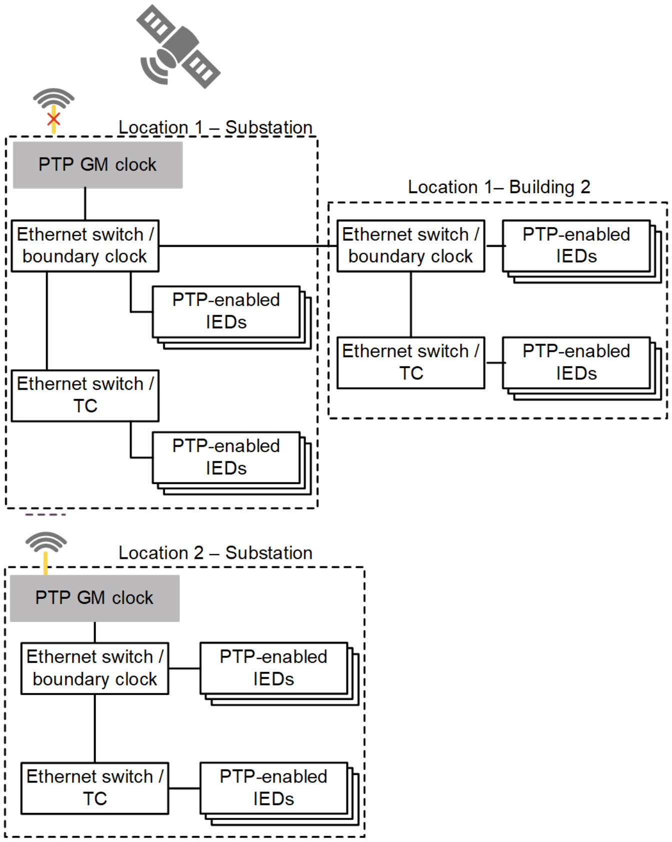


Fig. 10 PTP GM clocks provide local and global time to devices.

The use of local timekeeping and selective protection disabling introduces challenges that conventional systems did not have to consider; therefore, the user needs to give consideration to all protection elements and where the digitized data originates. IEDs, Ethernet switches, and global clocks form an essential part of the protection system design and need to be monitored for any momentary or persistent disturbances. The IEC 61850-7-4 standard provides an array of logical node classes that are useful for monitoring these devices, and since it is standardized, it allows the user to design the system based on their requirements.

Another feature required by the IEC 61850-based DSS is mode/behavior control. This is required because of the need for routine maintenance testing of IEDs. Since the signals are digitized in DSS solutions, the requirement is to put selected devices in a specific mode of operation that allows for isolated testing or combined testing. Mode control is explained in detail in [6]. These modes allow for greater flexibility but do not remove the requirement for time synchronization. The user must take this into consideration when designing these systems since temporary use of test devices may publish information with test flags, and the time references they are connected to, which may be discarded by the subscribing relays if not aligned.

Redundancy is applied to help prevent a single mode of failure in protection systems. The same techniques can be applied in DSS with multiple global clocks connected to the network and the relays and MUs determine which clock is the best source, as explained by the BMCA. Additionally, the user can also use PRP to duplicate the critical networks and have a full redundant system available for failover if there is a network failure.

Since time is a critical component in a network-based DSS, redundant paths are required to transmit PTP messages between devices. A PRP network can provide multiple redundant paths (LANs) to transmit PTP messages, ensuring that the time synchronization is not affected by a single point of failure. This provides a highly reliable and accurate time-synchronization solution for DSS applications. In addition to having multiple paths, it is critical to design the network with multiple clock sources to avoid the failure of a single clock. When two or more master clocks are present in the network, the master clocks and follower devices use the BMCA based on the master clock's attributes and the network attributes as published in the PTP announce message to choose the best available master clock. The newly elected master clock becomes the GM while the rest of the master clocks become passive. This allows all devices in the network to have a consistent and accurate time reference. When the GM clock fails, the rest of the master clocks in the network elect a new GM using the BMCA. Follower clocks further use the BMCA to elect a single GM from two independent LANs for synchronization.

Since a PRP network allows for multiple redundant paths for data to be exchanged, a failure on one of the LANs may go unnoticed, thus reducing the overall reliability of the system. Advanced diagnostics and monitoring of each of the LANs is critical, to ensure prompt action is taken to replace a failed component in the network, thus restoring the reliability of the system.

VI. CHALLENGES USING TIME

Many challenges exist with applying time in protection critical applications. These include but are not limited to:

- Loss of GNSS reference
- Firmware design in both protective relays and clocks
- Hardware
- Installation and distribution of time
- Protocols supported in all devices

Fortunately, most of these challenges can be addressed and dependability can be maintained for protection functions by applying good practices, as explained in Section VIII.

Protection functions that are relying on time must have appropriately designed firmware to endure the challenges outlined in this paper. Decisions must be made based on the protection scheme and the relay's ability to ride through a loss of global time reference. For example, the relay itself has its own internal oscillator that is used to keep internal local time. This oscillator is trained to the input global time reference when the signal is present. However, when the signal is absent, the oscillator can continue to keep time but drifts away from the true UTC reference. The relay designers are familiar with the hardware used and know the approximate worst case drift error related to this oscillator crystal. Using the estimated drift rate, a protection algorithm can maintain enough accuracy to continue protecting the line for some specified amount of time, although very limited. After the estimated drift of the internal oscillator, the algorithm has to block the protection scheme relying on this time reference. If the global time reference returns within this additional window, the relay internal oscillator will start to train itself to synchronize with the input time signal and protection can remain in service. If the global reference does not return within that drift rate window, protection would have to be blocked from operation if there are no other fallback methods available. These types of firmware modifications can change over the years; hence it is a good practice to review new firmware revisions periodically and test this behavior during commissioning.

In addition to the protective relay, consideration must be given to the installation, including the selection of the clock hardware along with how the time signal will be distributed. The most critical decision is the quality of the oscillators in the clock and balancing the cost for the application. If the application is relying on time for a protection scheme, the absolute best oscillator available should be chosen for the clock. As mentioned previously, selecting an OCXO oscillator provides substantial improvement in the overall holdover state. In this case, if the global reference to the clock is lost, the clock uses its internal oscillator and still provides a 1 µs accuracy signal to the protective relay for approximately four and a half hours, in most cases.

To further improve resiliency and protect against a single loss of the GNSS reference affecting the protection scheme, other methods can be applied in parallel. PTP with multiple networks and TDGs or other network time distribution approaches, such as PTP over PRP, are some of the available options. Using PTP with multiple LANs provides redundancy and protects the overall system from a single point of failure. As shown in Fig. 11, a second master shown as "Optional Redundant Clock" provides redundancy if the GM clock fails or is taken out of service, all while not having to reconfigure the IEDs.

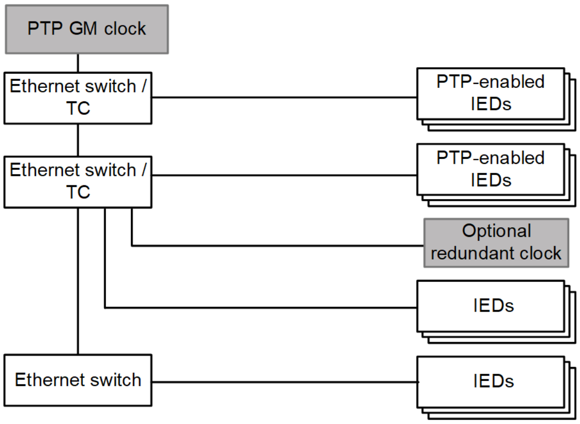


Fig. 11 PTP GM clock with redundant clock configuration.

The design of the PTP network plays a critical role in the resilience of global time reference. While multiple switches that are PTP aware can be used, it is recommended to have less than 15 hops in a PTP solution. Applying virtual LANs (VLANs) to segregate PTP traffic helps ensure the traffic is only sent to where it needs to be, as explained in [7].

The installation and distribution of time in a substation has many considerations. Designing a cost efficient yet reliable source of time can be challenging but is achievable. Modern relays are designed to accept time from multiple types of sources. Distribution of time is also a major consideration. Special attention needs to be given to the devices in between the clock and the end devices. Communications processors often provide the ability to redistribute time over a serial connection, as shown in Fig. 12.

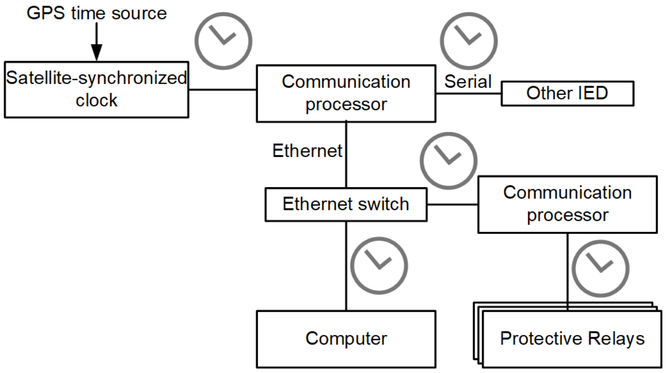


Fig. 12 Time distribution over serial and Ethernet interfaces from communications processor.

In this type of system, the communications processor and/or Ethernet switch may not have the proper components to continue to provide time or indicate the accuracy of the main clock to other devices. Field Case 2 in Section VII demonstrates a field event where the lack of time-quality information was not passed through a communications processor and led to undesired behavior of the end device.

Finally, the protocols supported in both the clock and the end device must be appropriate for the application. Consideration of the protocols used and which standard each device complies to must be evaluated. It is common to find a clock that is on the latest standard of a protocol, while the end device is not. Careful analysis of the differences between the protocols must be done to ensure that there will not be complications. For example, if a clock supplying PTP complies to IEEE C37.238: 2017, it is not compatible with an end device that supports IEEE C37.238:2011. But if the end device is compliant to IEC 61850-9-3:2016, they would be compatible. Comparison for the differences in PTP protocols can be found in [8].

In addition to protocols, the interpretation of the standard may be different between vendors. Behavior of the clock and these protocols are governed by standards; however, most standards are open to interpretation. Field Case 3 discusses one example where the standard was misinterpreted by a clock manufacturer and led to a misoperation of an 87L differential scheme.

VII. FIELD CASES

A. Field Case 1

A 4.4-mile 345 kV transmission underground cable runs between Station E and Station W, and it is protected by two sets of identical line current differential relays. Each set of line current differential relays uses two separate routes of digital T1 channels. System 1's line current differential scheme is based on this utility's corporate-owned digital T1 as its primary channel and a leased digital T1 as its hot-standby channel. For channel diversity, System 2's line current differential scheme is based on the leased digital T1 as its primary channel and the corporate-owned digital T1 as its hot-standby channel. Both sets of line current differential relays at each station use time-based data alignment via PTP. Both sets of line current differential relays at each station have phase and ground distance elements as backup.

On February 13, 2019, there was a Phase-C-to-ground fault right outside of Station W. The relays at both Station E and Station W operated and cleared the fault. However only Station E System 1 relay's line current differential elements operated. System 2 and its remote Station W's System 1 and System 2 relays all operated on their respective ground distance elements. None of the channels were in alarm condition, so why did only one differential relay operate during an internal fault?

Based on Fig. 13, Station W's System 1 and System 2 and Station E's System 2 Relays had the word bit 87USAFE asserted during this internal fault. The 87USAFE logic momentarily blocks the line current differential protection when the communications channel is not synchronized. The communications channel loses synchronization when the data cannot be time-aligned or there are a high number of lost packets in the communications network. A communication report from the primary relay at Station W indicated that it had lost over 200,000 data packets in the previous 24 hours. However, none of the other relays observed any packet loss in their communications reports.

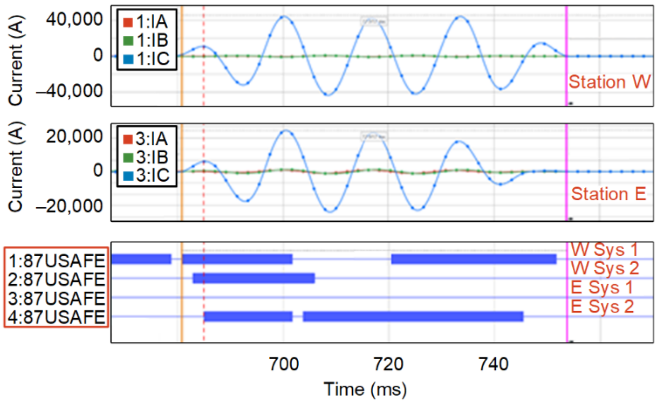


Fig. 13 Relays with line current differential protection in Blocked state.

The settings retrieved from the System 1 relay at Station E revealed Channel 1- and 2-time source settings: 87TIMC1 = I and 87TIMC2 = I (I = internal), respectively. Relays connected to C37.94-compliant multiplexers require this setting to be set to E (E = external) to ensure proper synchronization of the relay with the multiplexer. Incorrectly applying the transmit data settings can cause lost packets in the Station W System 1 relay. The utility modified the transmit data settings on the System 1 relay at Station E, which resolved the lost packets that were reported at the Station W System 1 relay. After the setting modification, the 87USAFE logic continued to assert and de-assert in all four relays, suggesting that another reason may exist for loss of channel synchronization.

This line current differential relay provides a channel recorder that can be configured to capture the data exchanged between the relays during loss of synchronization. The utility used the channel recording feature to collect data from the System 1 relay at Station W. The channel recorder data indicated that GNSS time at Station E was not reliable. The relays were configured in time-based synchronization mode (setting 87CHnSN = T), which uses GNSS time to align the line current differential data. If the GNSS signal is not reliable, the relay cannot properly align the remote communication data and the 87USAFE logic blocks the line current differential protection.

After consulting with the relay manufacturer, the utility modified the relay setting to use channel-based synchronization mode (setting 87CHnSN = C), which does not rely on a global reference time. The relays protecting this feeder were monitored for approximately 72 hours, measuring a maximum channel asymmetry of 0.55 ms (where the relay manufacturer suggested to use time-based synchronization only when channel asymmetry between the line current differential relays exceeds 2.5 ms), ensuring the relays could be set to channel-based synchronization mode. This setting change resolved the synchronization errors, and 87USAFE is no longer blocking the line current differential protection.

The time-source signals for the relays at Station E were obtained from PTP via the Ethernet switch, as shown in Fig. 14. They travel through the PTP Translator and the transistor-transistor logic (TTL)/Coaxial Adapter, then finally go into the relays' IRIG-B ports. This PTP Translator converts IEEE 1588 (PTP) signals into legacy time codes (included IRIG-B), with a TTL copper output. The root cause of the time distribution discrepancy was never determined but is assumed to be related to this configuration.

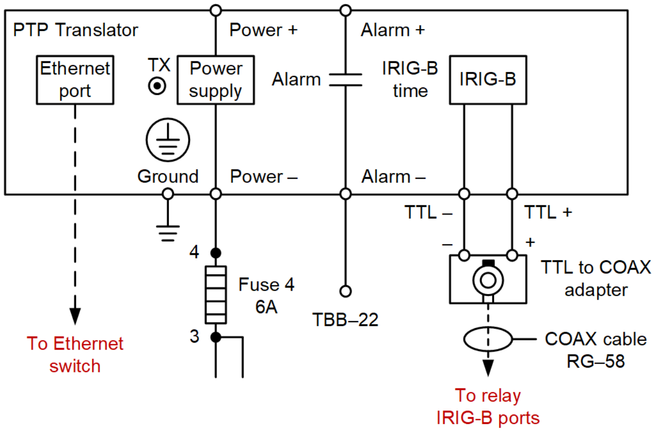


Fig. 14 Station E's relays' connection to time source.

B. *Field Case 2*

A 230 kV transmission line was protected by a pair of differential relays that operate in a dual channel hot-standby communications installation. In this configuration, if the primary communications channel is deemed to be of lesser quality than the hot-standby channel (HSB), the relay switches to the HSB channel for the data transfer. In this case, the primary channel is Channel 2, which is a 1,550 nm direct-fiber connection configured in channel-based synchronization. The HSB channel is an 850 nm C37.94 interface that is connected to a multiplexer and set to use time-based synchronization. Fig. 15 shows the channel configuration for this installation.

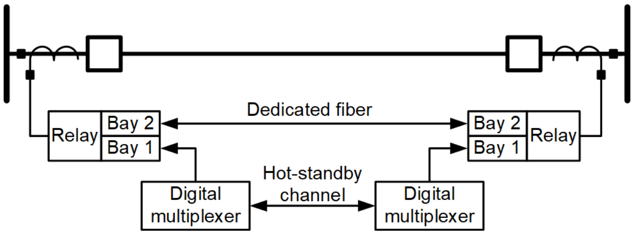


Fig. 15 Differential relay communications for Field Case 2.

The relay's primary channel was out of service, so it switched to the HSB channel once time was indicated as available. Upon enabling the differential protection, the relay's 87L data were misaligned and the relays issued a trip command to the breakers. Fig. 16 shows the misalignment upon enabling based on the HSB channel.

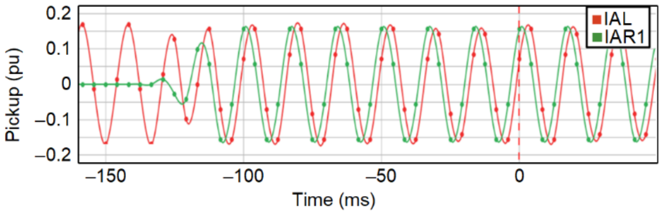


Fig. 16 Misalignment of 87L data.

The differential relay used in this application has a feature that captures the 87L differential data as it enters and leaves the relay. This 87L channel recorder was used to troubleshoot the issue, and it indicated that there was a shift in the external time in one of the relays. This pinpointed the substation that had the issue and allowed for additional troubleshooting.

It is important to remember that time-based synchronization relies on time-quality bits from the clock being shared through the IRIG-B message to the end device. In this installation, the clock signal is distributed through a communications processor, since the device already connects to all the relays and can provide the time signal over the same serial connection. This communications processor has its own internal clock and oscillator to continue to provide time if the reference input is lost from the external clock. Unfortunately, the communications processor does not pass the time-quality bits from the original clock signal; instead, it always indicates perfect accuracy. In the C37.118 standard, the time-quality bits of all 0s would indicate a perfect lock to the UTC time. Implementing it this way made it backwards compatible to the original IRIG-B signal that did not pass time-quality bits. If a clock is not C37.118-compliant, it will always pass these time-quality bits as 0s, indicating a perfect lock within 1 µs accuracy. In this case, the clock was not synchronized to the true UTC reference, since it had lost the global reference signal from its antenna, but the communications processor did not pass the time-quality bits to the end device. Therefore, the relay was using this time that had drifted by approximately 6.6 ms at the time of the operation which misaligned the data by over 140 degrees.

To confirm the behavior in the substation, which at the time of investigation was showing the signals in perfect alignment, the antenna was removed from the clock to allow it to drift and verify that the misalignment would occur again in the relay. After approximately four hours with the clock not connected to the GNSS reference, the relay indicated it was supposedly synchronized, and the time-quality bits indicated a perfect lock to the UTC reference. However, the data were misaligned by over 40 degrees in the communications report. This test confirmed that the relay was not getting the time-quality bits from the original clock after the IRIG-B signal was passed through the communications processor. A terminal emulator program was connected to the clock and the device correctly indicated that it was not within the required accuracy, yet the relay was still indicating that the clock signal was locked. The utility decided to connect this particular relay directly to the clock through a coaxial cable with a BNC connection. Testing the loss of GNSS signal scenario again proved that this approach would properly follow the clock and block when the time-quality bits indicate that the clock is not within the required accuracy to UTC. The utility also determined the GNSS antenna used in the application was an old design and installed without the proper clearance from the control building. These installation issues contributed to the original cause of GNSS signal loss. A new antenna was ordered and installed correctly to improve the reception reliability of the GNSS signal.

C. *Field Case 3*

A 115 kV transmission line was protected by a pair of differential relays using time-based synchronization which incorrectly operated the breakers when no fault was present. A pair of backup relays performing only distance protection did not operate.

The event report data indicated that time was lost a few hours prior to the event and returned just shortly before the relays operated. These relays were operating in a time-fallback mode that would block the 87L function whenever external time was not available. Shortly after the time was received at the relay, it enabled protection and the relay issued a trip command to the breakers. Fig. 17 shows the local and remote currents for the event.

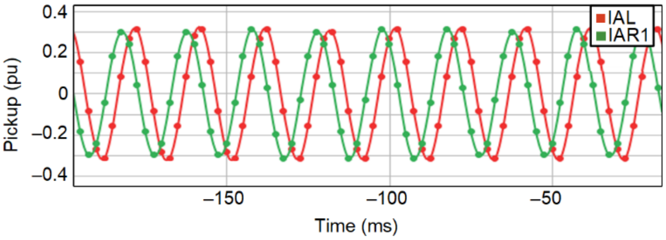
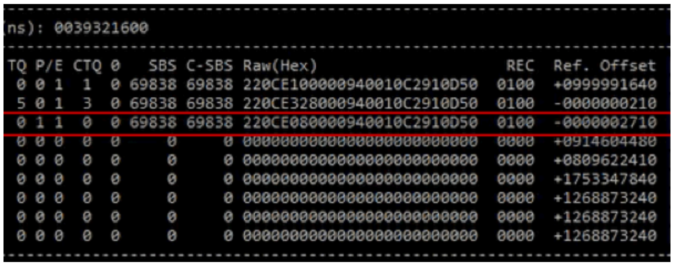


Fig. 17 Misalignment of 87L data after global reference acquisition.

Investigation of the clock output indicated an issue with how the clock updates the time-quality bits after acquiring the GNSS signal. The clock would indicate a perfect lock with the time-quality bits once the clock had locked onto the global reference; however, it was still outputting a time that was not locked to the reference. Fig. 18 shows a capture of the IRIG output of the clock and that the time was 2,710 µs off from the reference offset. At the same instance, the time quality was indicating a 1 µs accuracy to the end devices.



```
---------------------------------------------------------------------------
ns): 0039321600
---------------------------------------------------------------------------
TQ P/E CTQ 0    SBS C-SBS Raw(Hex)                    REC   Ref. Offset
 0 0 1   1   0 69838 69838 220CE100000940010C2910D50  0100  +0999991640
 5 0 1   3   0 69838 69838 220CE328000940010C2910D50  0100  -0000000210
 0 1 1   0   0 69838 69838 220CE080000940010C2910D50  0100  -0000002710
 0 0 0   0   0     0     0 0000000000000000000000000  0000  +0914604480
 0 0 0   0   0     0     0 0000000000000000000000000  0000  +0809622410
 0 0 0   0   0     0     0 0000000000000000000000000  0000  +1753347840
 0 0 0   0   0     0     0 0000000000000000000000000  0000  +1268873240
 0 0 0   0   0     0     0 0000000000000000000000000  0000  +1268873240
 0 0 0   0   0     0     0 0000000000000000000000000  0000  +1268873240
---------------------------------------------------------------------------
```

Fig. 18 Screen capture of IRIG test.

As seen in the figure, the time was not locked to the reference, but the clock was indicating perfect time lock with TQ = 0; therefore, the differential relay used this time to align data when it was not supposed to.

Discussing the findings with the clock manufacturer proved that they had a misunderstanding of the IEEE standard. They indicated the clocks assert the time-quality bits when the clock locked onto the GNSS reference, not necessarily when the clock outputs the correct time. The manufacturer then agreed to update the firmware in the clock to have the correct behavior. This new firmware was tested and confirmed to have proper behavior for a clock that is compliant to IEEE C37.118. This utility has continued to use this new clock firmware and has not had any issues since 2015, when this case originally occurred.

D. *Field Case 4*

A utility company implemented their first IEC 61850 Sampled Values (SV)-based DSS protection system using several manufacturers' devices. The lead engineer was working with a large team from their organization since they had to familiarize everyone with the different technologies. During lab testing, a selection of devices was tested, and settings were made for each protective relay, MU, Ethernet switch, and the clock source. Following the successful lab tests, they ordered all the devices and proceeded to a factory acceptance test. With all the devices installed, they noticed that a line-protection SV-subscriber relay from one manufacturer was only processing SV data from one MU and not the other MU, as previously configured.

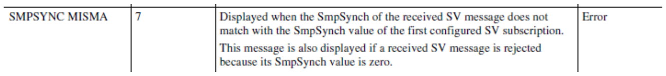
The affected MU and the SV-subscriber relay were from different manufacturers, but this proved to be a good test for interoperability and the user reached out to both manufacturers for assistance.

Diagnostic information captured from the SV-subscriber relay showed that it is was not processing SV data from the second SV MU because of the failure code: SMPSYNC MISMA, as shown in Fig. 19.

```
SV SubsID 1
--------------------------------------------------------------------------

 Ctrl Ref: XXXXX_MUMU01/LLN0$MS$MSVCB01
 AppID  : 4129
 Last Update : 05/13/2020 10:50:11

 Accumulated downtime duration (since last reset)  :
0000:00:24.961
 Maximum downtime duration                         : 00.000



SV SubsID 2
--------------------------------------------------------------------------

Ctrl Ref: XXXXX_MU1/LLN0$MS$MSVCB01
 AppID  : 4030
 Last Update : 05/13/2020 10:50:11

 Accumulated downtime duration (since last reset)  :
0000:00:24.960
 Maximum downtime duration                         : 00.000

 #  Date        Time      Failure
 1  05/06/2020  16:05:50  SMPSYNC MISMA
 2  05/06/2020  16:05:49  SMPSYNC MISMA
 3  05/06/2020  16:05:49  SMPSYNC MISMA
 4  05/06/2020  16:05:48  SMPSYNC MISMA
 5  05/06/2020  16:05:48  SMPSYNC MISMA
 6  05/06/2020  16:05:47  SMPSYNC MISMA
 7  05/06/2020  16:05:47  SMPSYNC MISMA
 8  05/06/2020  16:05:46  SMPSYNC MISMA
```

Fig. 19 Diagnostic information from the SV-subscriber relay.

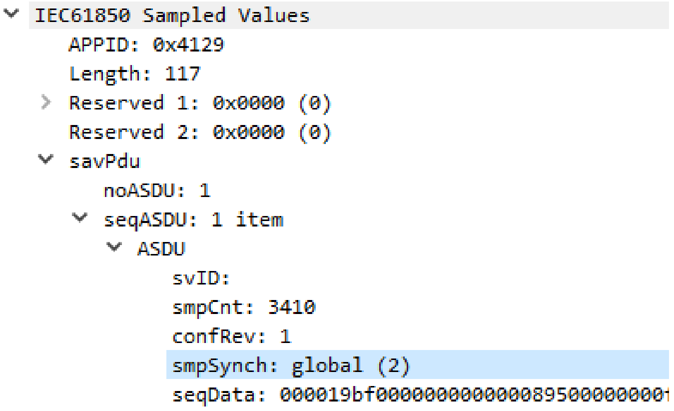
The previous SV-subscriber error code is explained in the manufacturer documentation, as seen in Fig. 20.



SMPSYNC MISMA	7	Displayed when the SmpSynch of the received SV message does not match with the SmpSynch value of the first configured SV subscription. This message is also displayed if a received SV message is rejected because its SmpSynch value is zero.	Error

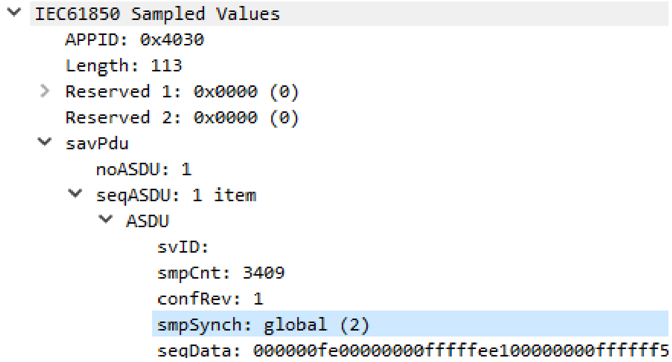
Fig. 20 SV-subscriber relay warning codes showing SMPSYNC MISMA.

Based on the information gathered, the second SV subscription is either not matching the SmpSync of the first SV subscription or the SmpSync value is zero. The lead engineer provided Wireshark Ethernet network captures, Fig. 21 and Fig. 22, of the process bus Ethernet traffic to the manufacturer since that is where the SV data are published by the MUs and subscribed to by the SV-subscriber relay. The Ethernet capture shows that both the first SV subscription MU and the second SV subscription MU have SmpSync as global, indicating both MUs are synchronized to a GNSS clock.



```
IEC61850 Sampled Values
    APPID: 0x4129
    Length: 117
  > Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  savPdu
      noASDU: 1
      seqASDU: 1 item
        ASDU
            svID:
            smpCnt: 3410
            confRev: 1
            smpSynch: global (2)
            seqData: 000019bf000000000000089500000000
```

Fig. 21 smpSynch from MU used in SV-subscription 1.



```
IEC61850 Sampled Values
    APPID: 0x4030
    Length: 113
  > Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  savPdu
      noASDU: 1
      seqASDU: 1 item
        ASDU
            svID:
            smpCnt: 3409
            confRev: 1
            smpSynch: global (2)
            seqData: 000000fe00000000fffffee100000000ffffff5
```

Fig. 22 smpSynch from MU used in SV-subscription 2.

Further investigation revealed that the SV-subscriber relay was not synchronized to the GNSS source. The manufacturer explained that if the SV-subscriber relay is not synchronized to a GNSS source, it will fall back to local timekeeping mode and only process the first SV stream, which has App ID: 4129, in this case. Investigation of the SV-subscriber relay not synchronizing to the GNSS source while the MUs did, led to the discovery that the firmware of the clock used was upgraded after the lab tests. This firmware upgrade changed the version of PTP to be compliant to C37.238:2017, which the SV-subscriber relay does not support but the MUs do. Another engineer in the team was responsible for the clock firmware, and that led to the oversight of the changed profile. This proved a valuable learning experience for the user with regards to what data needs to be gathered for such an issue and how important it is to understand the exact impact a firmware change in any device has on the whole IEC 61850-SV system.

VIII. BEST PRACTICES AND COMMISSIONING TIPS

As the field cases in this paper demonstrate, there are many considerations when applying time to protection-based applications. These field cases could all have been prevented if proper steps, best practices, and testing were applied during the commissioning process, had the users known the specific concerns when using time.

A. Best Practices

Applying time to protection-based applications requires a fundamental understanding of how global time is received and distributed through multiple devices. There are multiple resources, including this paper, that provide a good overview of the various standards and enough detail to apply time appropriately in these applications.

Time-quality bits, standards, device hardware, and device firmware all need to be thoroughly reviewed during the system design process. For each application, it is important to determine the requirements for the functions that are using time and choose the equipment that meets those needs. Obviously, time simply being used for coordinating a sequence of events has much different requirements than applications that are aligning data in an 87L protection scheme or synchronizing an IEC 61850-9-2 SV configuration.

A clock with an appropriate oscillator provides resilience to loss of global reference and allows protection to have better availability. As with all protection applications, there is a cost versus benefit to these choices. However, if protection is reliant on time, investing in the best hardware is imperative. If any additional equipment is used to help distribute the time through a substation, such as a communications processor, consideration must be given to ensure that it will pass the time-quality bits from the original clock. For PTP applications, selection of switches that are PTP aware and the standards they support should be considered. Selecting multiple GM clocks is also an option for a single LAN or two LANs in PRP, which can provide more resiliency but needs to be fully tested.

Choosing the right equipment also includes selecting the correct firmware. Devices must comply with appropriate standards and be compatible with all other devices in the system. As shown in the PTP discussion, there are cases where an end device may not accept the version of the protocol that the clock or other device is supplying. This includes different iterations of the protocol indicated by the year it was released, so the entire standard needs to be reviewed to understand the difference and identify any compatibility issues.

A review of the product's firmware history can be very valuable. As pointed out in Field Case 3, firmware could be updated over the years to improve the behavior of the clock, distribution equipment, or the end device itself. Paying close attention to standards that are supported in each firmware revision can help engineers choose the correct version for their application. It is recommended to document the firmware versions of all devices during the commissioning process and note specific standards each device supports. This will assist in future firmware upgrade evaluations and help determine or identify compatibility issues.

End devices typically have a lot of valuable monitoring capabilities that should be used. For example, reviewing the instruction manual and obtaining useful information, such as available digital relay bits that can be programmed into the Sequential Events Recorder (SER) or added to an event record itself, should be completed. Some relays also have additional functions, as pointed out in Field Case 2, where an 87L channel recorder was used to identify the issue with time that caused the misalignment of the differential data. Taking advantage of these features can provide useful information for future analysis and assist in troubleshooting during the commissioning process.

For line current differential applications, it is recommended to use channel-based synchronization whenever possible. Time-based synchronization can still be used but added complexity and extra points of failure accompany this type of application, requiring additional testing before putting the devices in service.

Finally, simplicity is key. Limiting the number of devices in between the GNSS source and the end device enhances the overall security and reliability of the time distribution network. Fewer devices equate to fewer points of failures and fewer compatibility issues that could lead to potential unforeseen errors.

B. Commissioning Tips

During commissioning, the following tests should be conducted to fully understand the behavior of a clock and the end device.

To fully test the clock's behavior, various conditions need to be explored. One of the most critical tests includes disconnecting the antenna, which is providing the GNSS signal. This test should include investigating the proper amount of holdover available based on the oscillator hardware selected. This will require the antenna to be disconnected for multiple hours to investigate the total time for holdover. Many times, this can be achieved with the relay that has available digital relay bits that parse the IRIG message and indicate the clock's accuracy. The test could include monitoring the time at which the antenna is disconnected and using the SER to monitor when the accuracy is determined to be greater than 1 µs. Some clocks offer commands that can be issued through a terminal session to force the quality bits to a certain state as well. This is very useful to determine how all the equipment in the system, including the end device, behaves during this scenario.

The next step is to attach the antenna to the clock after being disconnected for some time and verify how long it takes the clock to lock to the Stratum 0 reference. Confirm that it outputs the correct time within 1 µs when it asserts its corresponding time-quality bit. In the end device, verify that the time-quality bits are changing as expected. In applications using a differential relay, verify that no misalignment occurs by having the relay trigger an event report on the assertion of its time-quality bits or any other trigger that allows you to see how the relay behaves during this condition. If the line current differential relay has a time-fallback mode to a channel-based synchronization, observe the behavior during this fallback as well as the device transitioning back to time-based. If different clock vendors are used at each end of the differential zone, each clock should be tested independently to ensure proper holdover, fallback, and reacquisition of a global reference. The relay should be observed during the transition to the holdover state in the clock, as well as when it transitions back to time lock with the time-quality bits indicating the required accuracy.

If any additional equipment is part of the time distribution system, such as a communications process or an IRIG distribution module, similar tests should be conducted with this intermediary device.

In the case of PTP installations, multiple GM clocks can be part of the system. Each of these clocks should be tested in a similar fashion to standard clocks, and the overall system should be evaluated for performance when the time is changed from one GM clock to another. Each clock should have the global antenna removed independently and reconnected to test failover and transitions to and from the secondary clock. Additionally, some clocks support forcing bad quality and can be used to test competing clocks for superior accuracy and becoming the main provider of time. Testing failures of PTP switches should also be considered, and in the case of PTP over PRP networks, each individual LAN should be exercised by testing all points of failure in the network and verifying the end device performance.

It is recommended to test the reception of the GNSS signal to verify the full installation and distribution of time to the end devices. The clock and relay data logs should be reviewed after a few days to ensure that the clock is continuously receiving the GNSS signal and no anomalies are observed. This can pinpoint issues such as antenna installation or failing cable connections before the devices go into service. It is also recommended that the data logs be reviewed after a month or so to verify that the entire time system is stable.

Finally, the clock is an electronic device. As such, it has its own diagnostics and can perform a restart to remove corruptions that may occur in its internal components. During the commissioning process, the clock should be power cycled to simulate this type of behavior. Both the behavior of the clock and the end device should be observed to make sure both have expected behavior during this type of failure. Power cycling a device can have drastically different behavior than simply losing a global reference. An additional step should be to perform these tests on the relay to ensure it powers up, locks to the correct time, and updates everything internally before enabling protection.

In DSS applications, testing both local and global time modes along with selective protection element disabling should all be exercised. Use of the test mode at one end for differential schemes, or any scheme that involves remote protection, such as pilot schemes, should be exercised and a proper procedure for future testing should be documented in case troubleshooting is needed in the future. It is best to determine the issues during the commissioning process and develop a good test plan for future troubleshooting exercises.

IX. CONCLUSIONS

Time can be applied in protection-based applications with resiliency and security if proper steps are taken to fully evaluate the behavior of the clock, the end device, and everything in between.

Understanding how clocks and time distribution work is imperative to applying time in protection-based applications. Investigation of the standards and knowledge of a device’s compliance with those standards ultimately leads to success or failure in applying time. PTP is a newer protocol and is still evolving; therefore, newer iterations are being developed all the time. While these standards are a bit more complicated, they do offer many benefits and provide better resiliency to loss of time synchronization. Using a combination of multiple standards, such as IRIG, PTP, or TDG, helps engineers develop multiple redundancies for critical applications.

Once a design is chosen, proper commissioning can ensure that everything was implemented properly, and the selected equipment can achieve the desired performance. Including testing of the time source/sources can prevent future misoperations. Reviewing all devices firmware revision history can help avoid unsupported protocols or issues that have been addressed from prior versions. This short review can save hours of troubleshooting in the field and during commissioning.

DSSs introduce challenges for time distribution and require very high-accuracy GNSS time sources to work as intended, but these systems also provide the user with the ability to easily expand a substation by adding more feeders/bays by simply mapping digitized signals to existing equipment, as opposed to running cables, which results in shorter outages and reduced production downtime.

X. REFERENCES

[1] NASA, “What is GPS,” June 2019.

[2] Suntsu Electronics, Inc., “Temperature-Compensated Crystal Oscillators – TCSO’s.”

[3] National Institute of Standards and Technology, “Time and Frequency Division.”

[4] D. Williams, M. Elshafi, K. Fodero, C. Huntley, and P. Robertson, “Using Wide-Area Precise Time Distribution to Increase Dependability and Security of Substation Time Synchronization,” presented at the 75th Annual Conference for Protective Relay Engineers, College Station, TX, March 2022.

[5] J. Miller, J. Burger, N. Fischer, and B. Kasztenny, “Modern Line Current Differential Protection Solutions,” presented at the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

[6] E. Hernandez, T. Whitesell, and K. Leggett Wyszczelski, “A Practical Guide to Substation Testing Using IEC 61850 Mode and Behavior,” presented at the Power and Energy Automation Conference, Seattle, WA, March 2020.

[7] L. Thoma, “Best Practices for Implementing PTP in the Power Industry,” 2018. Available: selinc.com.

[8] IEEE PSCC Task Force, “Revision of IEEE Std C37.238, Power Profile for IEEE-1588: Why the Big Changes?”

XI. BIOGRAPHIES

Ed W. Chen graduated from City University of New York with a Bachelor of Science in Electrical Engineering Science and from Worcester Polytechnic Institute with a Master of Science in Electrical and Computer Engineering. Ed joined National Grid New York in 2010. In 2012, he became a relay protection engineer in their protection analysis and relay project engineering groups. In 2016, Ed joined Consolidated Edison Company of New York, Inc. and continues to work there as a relay protection engineer. In 2022, Ed was promoted to the section manager of protection support & analysis in Consolidated Edison Company of New York, Inc. Ed is a registered Professional Engineer in the state of New York.

Brian Smyth received a BSEE and MSEE from Montana Tech at the University of Montana in 2006 and 2008, respectively. He joined Montana Tech as a visiting professor in 2008 and taught classes in electrical circuits, electric machinery, instrumentation and controls, and power system analysis. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2009 as an associate power engineer in the research and development division. Brian is currently a senior engineer in the transmission department and holds two patents. In addition to working for SEL, Brian joined Montana Tech of the University of Montana in 2014 as an affiliate professor, where he teaches courses in power system protection. He received the Distinguished Alumni award from Montana Tech in 2016 and the IEEE Southwest Montana Chapter, Engineer of The Year award in 2017. He is an active IEEE member and Chair for Region 6 Western Montana Section and is a registered professional engineer in the state of Washington.

Marcel van Rensburg is a product engineer in protection systems research and development at Schweitzer Engineering Laboratories, Inc. (SEL). Marcel received his National Diploma in Electrical Engineering from Central University of Technology, Bloemfontein, South Africa, in 2012, during which time he joined SEL as an associate application engineer. Marcel received his Baccalaureus Technologiae from the Tshwane University of Technology, Pretoria, South Africa, in 2016, and served customers with training and technical support as an application engineer with an emphasis on automation for seven years in Sub-Saharan Africa. Marcel is a member of IEEE and a U.S. representative to IEC 61850 TC 57 WG 10.

Manodev Rajasekaran is a senior engineering manager in research and development at Schweitzer Engineering Laboratories, Inc. (SEL) focused on developing digital secondary system (DSS) products. He joined SEL in 2008 as a hardware engineer and has been designing protective relays. He received his master’s in Electrical Engineering from the University of Idaho in 2000.

20230419 • TP7108