Understanding the Impacts of Time Synchronization and Network Issues on Protection in Digital Secondary Systems

Arun Shrestha, Mauricio Silveira, Jaya Yellajosula, and Sathish Kumar Mutha
Schweitzer Engineering Laboratories, Inc.

Presented at the
PAC World Global Conference 2021
Virtual Format
August 31–September 1, 2021

Understanding the Impacts of Time Synchronization and Network Issues on Protection in Digital Secondary Systems

Arun Shrestha, Mauricio Silveira, Jaya Yellajosula, and Sathish Kumar Mutha,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—A digital secondary system (DSS) replaces copper cables used for substation secondary systems with fiber-optic cables used to exchange information between primary equipment and protection and control devices. This results in improved personnel safety, reduced electromagnetic interference, and lower substation construction cost. In an IEC 61850-based DSS, an Ethernet network is used to exchange time synchronization and Sampled Values (SV) data between devices. For protection functions to remain available, both the time sources and protection network should be in robust condition.**

This paper analyzes the impacts of time synchronization and network issues on protection functions for an IEC 61850-based DSS. Test cases that demonstrate disabling of protection functions due to loss of a time source and a delay in protection function operation during network congestion are presented. A quick overview of a simple point-to-point-based (P2P-based) DSS, in which protection is independent of external time source and Ethernet network, is also provided.

I. Introduction

A conventional substation employs large amounts of copper cables to exchange analog and binary signals between primary equipment and protection and control devices. The conventional secondary system is costly and can expose workers in control houses to dangerous high-energy cables. On the other hand, a digital secondary system (DSS) uses fiber-optic cables to communicate between the relays in the control house and the merging units (MUs) in the switchyard. This eliminates copper cables between the primary equipment and the protective relays, leading to improved personnel safety and lower substation construction cost. Two types of DSS solutions are currently available [1][2]. The first DSS solution currently available, one that is based on IEC 61850 standard, uses switched network architecture to communicate between MUs and relays. Since this DSS is based on IEC 61850 standards, it promises interoperability between devices from multiple vendors. The second DSS uses point-to-point (P2P) architecture, in which an MU is directly connected to a relay via a fiber-optic cable. Both solutions have their own merits and unique challenges.

An IEC 61850-based DSS requires both network switches and dedicated time source for operation [3]. All protective relays and MUs are time-synchronized either by directly connecting to an Ethernet network-based time distribution protocol, such as Precision Time Protocol (PTP), or using a dedicated connection like IRIG-B, or both. The time source allows relays to correctly time-align data received from multiple MUs, accounting for sampling time variation and network delays, before passing the data to protection functions. In a P2P-based DSS, data received from multiple MUs are time-aligned using an internal clock of the relay, thereby eliminating the need for an external time source. This simplifies the overall DSS design. In select applications, relay may further be synchronized to an external time source or another relay allowing it to support synchrophasors and line differential applications.

For protection to remain enabled in an IEC 61850-based DSS, both the time source and the protection network should be online and in robust condition. However, there are many real-world issues that can challenge these two critical components and impact overall protection system availability and performance. Regarding time synchronization, the issues can include unavailability of the GPS signal, questionable reliability and redundancy of satellite clocks, and inconsistent synchronization behavior of protective relays and MUs from multiple manufacturers. Similarly, Ethernet networks not being engineered correctly can lead to loss of packets or result in high network delay. These network issues can momentarily disable protection functions or reduce the overall protection speed.

This paper is written with protection engineers as the target audience. It focuses on the impact of time synchronization and network issues on protection functions in an IEC 61850-based DSS. Section II describes time synchronization methods and various time synchronization events (e.g., loss of time source or GPS signal spoofing) that impact protection. Network engineering is covered in Section III; the section details the adverse effect of a poorly designed network on protection. Section IV describes protection system design for a DSS. In Section V, test results are provided to help the reader better understand the impact of time synchronization, and network issues on protection functions are presented. Section VI provides a brief overview of a P2P-based DSS and compares it against an IEC 61850-based DSS. Finally, concluding remarks are presented in Section VII.

II. Synchronization Methods for DSS Solutions

In the modern era of digitized power system grids, time synchronization plays a pivotal role in the design of reliable protection and control systems. There are numerous power system applications that rely on time synchronization either via

a local clock or a global clock through single or multiple Global Navigation Satellite Systems (GNSSs). In a DSS, time synchronization allows a relay to time-align Sampled Values streams received from multiple MUs before passing the signals to protection functions. Hence, an accurate time source and time synchronization technique are critical for correct operation of DSS devices.

A. Time Synchronization Method

Devices used in DSS solutions may require time source accuracy down to microseconds. Two widely used methods to distribute accurate time are discussed briefly.

1) IRIG-B

The IRIG-B standard is widely used for transmitting accurate time information across short distances, and is described in detail in IRIG Standard 200-04. To represent time information, IRIG-B uses a pulse width modulated 100 Hz signal. It reflects the accuracy of the time information and offers information about the time quality. IRIG-B signal rising edges are precise time stamps that can be designed to be within 100 nanoseconds of Coordinated Universal Time (UTC) when distributing time from a Stratum 1 clock. Signals from IRIG-B are typically delivered through coaxial or fiber-optic cable for longer distances. Dedicated time distribution cables can fail independently, leading to undesirable cases where only some of the end devices are synchronized to each other.

2) PTP

In an IEC 61850-based DSS, both communications and time synchronization services are recommended to be provided over the same channel. This feature ensures that all communicating devices share the same sense of time, and that failure and recovery procedures are well-defined. The primary goal is to ensure that all devices that can communicate with each other are also synchronized to each other. This goal can be achieved in a local-area-network-based (LAN-based) setting using IEEE 1588 PTP, which can provide precision exceeding 100 nanoseconds [4]. Dedicated hardware circuits for precision time-stamping of Ethernet frame arrival and departure times, as well as methods for exact measurement of communications link delays, are used to accomplish this accuracy [5].

Individual devices can use time-stamping hardware to precisely measure the moment when the first bit of a PTP message reaches the device input (reception) or is created by the device output (transmission). The physical network interface connector (the end of the fiber or the Cat 5 RJ-45 end connector) is the exact time-stamping point, but it is mostly implemented at the physical layer (PHY) output. In this instance, the PHY delay must be constant and known, or it must be less than the manufacturer's stated accuracy level.

IRIG-B systems can readily coexist with PTP because both systems can achieve one-microsecond accuracy or better. As a result, most network-based substation equipment is projected to continue to support all two-synchronization alternatives, providing power system operators with the high level of flexibility needed to ensure system updates and retrofits. Table I shows an abstract comparison between two different time-distribution methods [6].

TABLE I
COMPARISON BETWEEN IRIG-B AND PTP

Time-Distribution Method	**IRIG-B**	**PTP (IEEE C37.238 Profile)**
Physical layer	Coaxial cable	Ethernet
Operating model	Master-slave	Master-slave
Synchronization accuracy	~500 ns to 1 µs	~100 ns to 1 µs
Compensation for latency	Yes, using cable length as inputs	Yes, compensated by all devices in the network
Update interval	Once per second, pulse per second	Configurable typically once per second
Relative cost	Low	Medium to high (early adoption)

B. IEEE and IEC Standards for Time Synchronization

1) IEEE 1588 and IEEE C37.238

IEEE 1588-2019 [4] was published to establish guidelines for industry-specific PTP to achieve accurate time synchronization over Ethernet. This standard defines how to transfer time over networks using profiles and it provides various default profiles for different applications.

IEEE C37.238 [7] is derived from IEEE 1588, which is dedicated to power system applications and extends support for dynamic time inaccuracy for better monitoring of time quality.

2) IEC 61850-9-3-2016

IEC 61850-9-3-2016 [8] has made it possible to integrate PTP into the IEC 61850 standard. The standard describes a PTP profile for power utility automation for high accuracy time synchronization (defined in IEC 61850-5). The standard proposed using Layer 2 communication, a P2P delay mechanism with default best master clock algorithm, and multicast communication.

Table II provides a comparison between power utility profiles for PTP.

TABLE II
PTP PROFILES

PTP Profile Standard	IEEE C37.238-2011	IEC/IEEE 61850-9-3	IEEE C37.238-2017
Domain number	0–127	0–127	0–127, 254
IEEE C37.238 TLV	Mandatory	None	Mandatory
Alternate time offset indicator TLV	Required	None	Needs a control to allow user to select
Grandmaster (GM) ID	8-bit GM ID (incompatible with IEEE C37.238-2017)	None	16-bit GM ID (incompatible with IEEE C37.238-2011)
Jump seconds	Next discontinuity might indicate leap second adjustment today	No TLV to provide actuals, local time offset not provided	Shall be 0 when local time does not use daylight-saving time, else shall be Nx900, with N an integer <>0
Time inaccuracy	Through TLV version 1	Through IEEE 1588 GM clock quality	Through TLV version 2
Virtual LAN (VLAN)	Mandatory	Optional	Optional

3) Time Synchronization Requirements for DSS

Time synchronization is essential for the successful operation of a DSS. Loss of time synchronization in a DSS produces an artificial phase shift, which can lead to false tripping. There is a wide range of time synchronization techniques; 1 PPS, IRIG, and PTP are used in DSS. To meet the high accuracy requirements for an IEC 61850-based DSS, PTP is considered the best method for time synchronization. The time synchronization accuracy requirements for an IEC 61850 substation are listed in Table III [9]. For SV and synchrophasor applications, time accuracy of 1 µs or better is recommended (T5 time synchronization class).

TABLE III
TIME SYNCHRONIZATION CLASSES

Time Synchronization Class	Accuracy (µs)
TL	>10,000
T0	10,000
T1	1,000
T2	100
T3	25
T4	4
T5	1

Fig. 1 shows a simple DSS network architecture with a PTP-based time distribution system. To implement PTP time synchronization on the process bus, communication networks should be robust enough to handle Sampled Values (SV), GOOSE, and PTP traffic; failure of one of them will affect the others, because they share the same network communication layer. Extensive testing is required on each DSS to assess its vulnerabilities and immunities associated with PTP time synchronization [10].

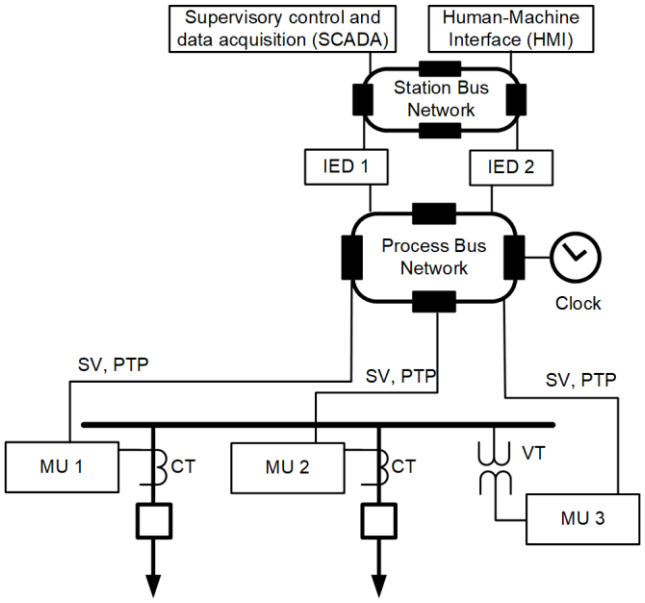

Fig. 1. PTP-based time distribution system for DSS.

These vulnerabilities can include antenna failure, poor satellite reception, GNSS jamming and spoofing, multiple GNSS constellations, network-related contingencies, and spoofing or manipulating SmpSynch (IEC 61850-9-2:2011 defines a field called SmpSynch, which indicates the synchronization source of the IED publishing Sampled Value packets to the network) [11]. In order to design a robust time distribution system for DSS solutions, engineers should consider implementing multiple grandmaster clocks, with each clock using more than one antenna to avoid jamming and spoofing. Additionally, time synchronization clock hardware resiliency can be achieved by using a high stability OCXO (oscillator) and network resiliency can be achieved by implementing network architecture like PRP, HSR, and software-defined networking (SDN) [12] [13].

III. Network Engineering for DSS

In a DSS, a communication network is used to exchange information between primary equipment and protection and control devices. A robust and engineered network is critical for reliable DSS operation. To maintain power system reliability, it is necessary to understand the effects of latency, jitter, packet loss and bandwidth usage, and network design on the protection system.

A. Latency

Network latency is a measurement of delay in a system. Latency accounts for processing delays, network queuing delays, and propagation delays [14]. Fig. 2 shows a DSS system with an MU connected to a network through its communications processor interface (CP) and a protection relay connected to the same network. This remote data acquisition scheme introduces delays and it directly impacts the performance of the protection relay. The SV Network Delay (SVND) is the sum of the MU processing delay and the process bus network delay.

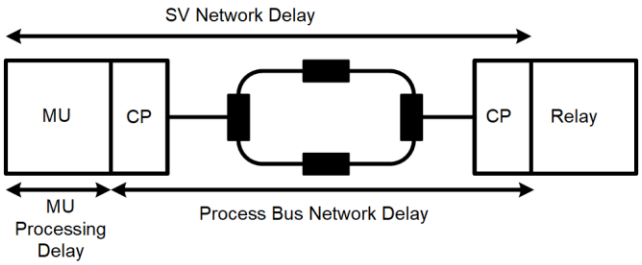

Fig. 2. Sampled Values Network Delay (SVND) for an MU.

IEC 61850-5 standard defines the time requirements for latency in protection systems as the transfer time [9]. Table IV lists the transfer time requirements for protection and control applications.

TABLE IV
TRANSFER TIME REQUIREMENTS

Transfer Time Class	Transfer Time (ms)	Application
TT0	>1,000	File transfers
TT1	1,000	Alarms
TT2	500	SCADA commands
TT3	100	Slow automation functions
TT4	20	Fast automation functions
TT5	10	Status changes
TT6	3	Trip, blocking, sampled analog exchanges

In a DSS, TT6 transfer time is desirable but only accounts for the process bus network delay. To better define the overall latency, the MU processing delay needs to be determined. Equation (1) defines the overall latency for a DSS relay.

$$DSS_{Latency} = MAX(SVND) + (N+1) \bullet Ts \quad (1)$$

where:

MAX(SVND) is the maximum SV network delay for all subscribed streams.

N is the number of lost packets that the DSS relay is able to ride through by interpolating missing packets.

Ts is the sampled period.

Fig. 3 shows two measured SVND over time from two different MU manufacturers, MU-A and MU-B.

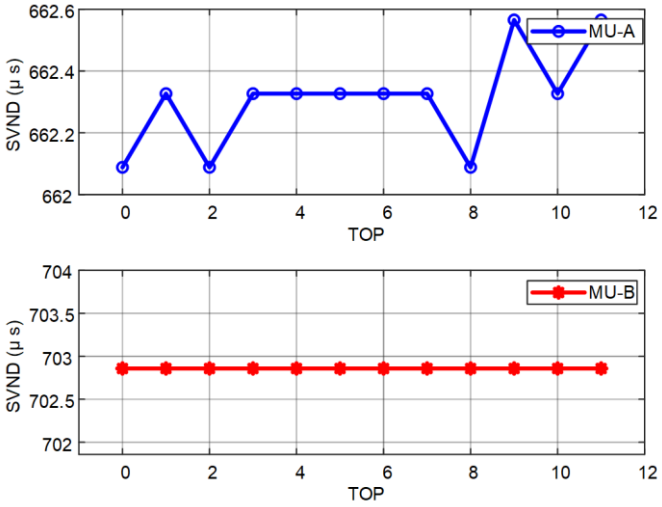

Fig. 3. Network delay for two MUs.

The maximum network delay recorded was 662.5 µs from MU-A and 702.75 µs from MU-B. If the measurement is taken from the reception device, the MAX(SVND) can be considered as the overall process bus network delay (processing delay plus propagation delay).

The N is a safety factor introduced by the subscriber interpolation capabilities, and it is used to ride through missing sample situations and packet losses. It is essential to balance N with the protection system time performance; for example, N = 3 causes an additional 4-sample delay (N + 1). Ts is defined by the MU profile characteristic; for IEC 61850-9-2 LE at 60 Hz, the sampling rate is 4.8 kHz. Therefore, Ts is 208.3 µs. Table V summarizes the overall DSS relay latency for using MU-A and MU-B. Latency doubles in case of IEC 61869-9:2016 compliant 4.8 kHz stream which packs two data points into one SV frame, for a publishing rate of 2.4 kHz.

TABLE V
DSS LATENCY FOR MU-A AND MU-B

MU	MAX(SVND) (µs)	N (samples)	Ts (µs)	DSS Latency (ms)
MU-A	662.5	3	208.3	1.459
MU-B	702.75	3	208.3	1.536

The DSS latency can be used as a setting that defines the maximum latency acceptable by the DSS relay. Therefore, in a system that uses MU-A and MU-B, the protection relay latency setting should be set to a value greater than 1.536 ms to accommodate the overall network delay and ride through three consecutive packet losses.

B. Jitter

Jitter is the variation in the time delay between the transmitted and received signal. In a DSS system, the interval jitter includes the MU publication period and the propagation delay jitter. The jitter is a statistic value, and it is an essential criterion for evaluating the process bus design [15]. The jitter needs to be consistent with the defined sampled period profile. For example, IEC 61850-9-2 LE at 60 Hz has a sampled period of approximately 0.208 ms. Fig. 4 shows the packet interval over time (jitter) between MU-A and MU-B. Table VI summarizes the measured jitter between the two MU manufacturers.

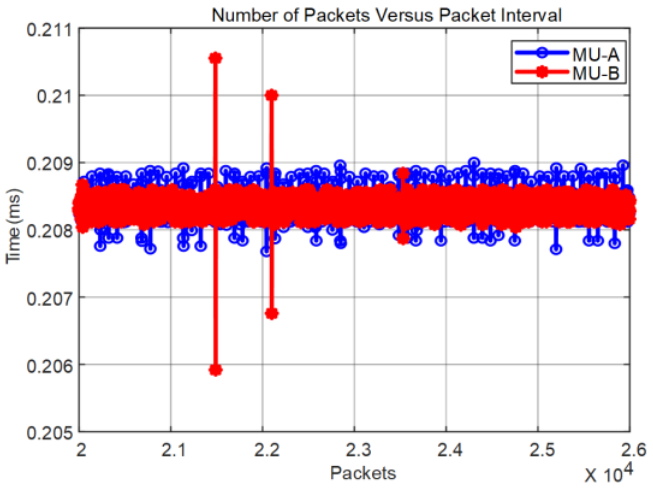

Fig. 4. Measured jitter for two MUs.

TABLE VI
MEASURED JITTER FOR MU-A AND MU-B

Jitter	MU-A (µs)	MU-B (µs)
Maximum	212.64	225.12
Minimum	203.8	192.12
Mean	208.33	208.34

C. Available Bandwidth and Throughput

Available bandwidth is defined by the amount of traffic that can be pushed to a system or network without affecting the network communication. Throughput is the real measure of how much meaningful data are successfully transferred from the source to the destination without overhead [16]. In a DSS communication channel, the bandwidth and throughput utilization depend on the topology and protocols used. For example, Fig. 5 shows an IEC 61850-based DSS that uses SV, GOOSE, and PTP protocols to exchange analog, binary, and time synchronization data to accomplish the protection of the primary substation equipment. Eventually, IP traffic is used for engineering access and file event retrieval.

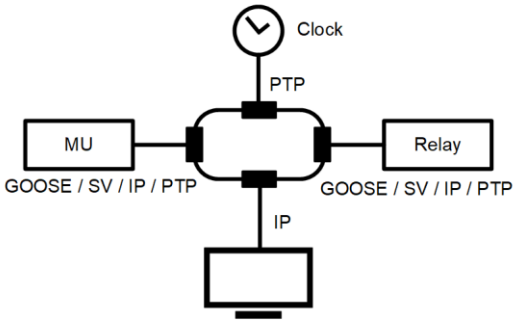

Fig. 5. IEC 61850-based DSS network using multiple protocols.

Table VII summarizes the total bandwidth usage by the DSS system:

- 1 MU with 4 SV messages at 60 Hz, using IEC 61850-9-2 LE profile, and 4 GOOSE messages.
- 1 protection relay publishing 4 GOOSE messages.
- GOOSE messages calculated during a burst condition [17].
- 1 clock publishing PTP messages using the PTP power profile.
- 1 computer with IP traffic for event collection and engineering access.

For this scenario, the total usage is approximately 30 Mbps. Therefore, a 100 Mbps link should be sufficient to accommodate the application.

TABLE VII
BANDWIDTH USAGE IN AN IEC 61850-BASED DSS NETWORK

Data	SV	GOOSE	PTP	IP
Bytes per message	140	300	102	600
Number of messages	4	8	4	3
Messages per second	4,800	40	1	10
Bandwidth (Mbps)	21.50	0.768	0.00326	0.144
Total bandwidth (Mbps)	22.4			

Another way to implement a DSS is through dedicated P2P links. An MU is connected to a protection relay through a dedicated fiber-optic cable. The dedicated DSS protocol carries the analog, digital, and local time alignment time correction to protect the primary substation equipment. Table VIII summarizes the overall bandwidth usage for 4.8 kHz and 10 kHz.

TABLE VIII
BANDWIDTH USAGE IN A DEDICATED P2P DSS

Data	Dedicated DSS protocol at 4.8 kHz	Dedicated DSS protocol at 10 kHz
Bytes per message	200	200
Number of messages	1	1
Messages per second	4,800	10,000
Bandwidth (Mbps)	7.6	16

Therefore, using a dedicated P2P link allows the application to support high sampling rate while using less bandwidth.

D. Impacts of the Network Design

A network consists of an environment used to share information and resources between two or more linked devices. In a network-based DSS, the network design and engineering play a significant role in maintaining the system reliability [18]. There are several types of DSS schemes available in the literature and they range from single P2P links through full redundancy network designs [1] [10] [19].

Network technology allows for several architecture types and associated features, such as data sharing, redundancy, availability, and cybersecurity. However, in a DSS, the network is part of the protection system, and simplicity is a constraint used to maintain system reliability. Simplicity in a protection system is defined as the minimum protective equipment and associated circuitry to achieve the protection system objective [20]. The network design should inherit the same principle to maintain protection system reliability and performance.

One direct impact of the simplicity affects data serialization in the DSS protection relay. Fig. 6 shows the data serialization process using the DSS network design and the DSS P2P design.

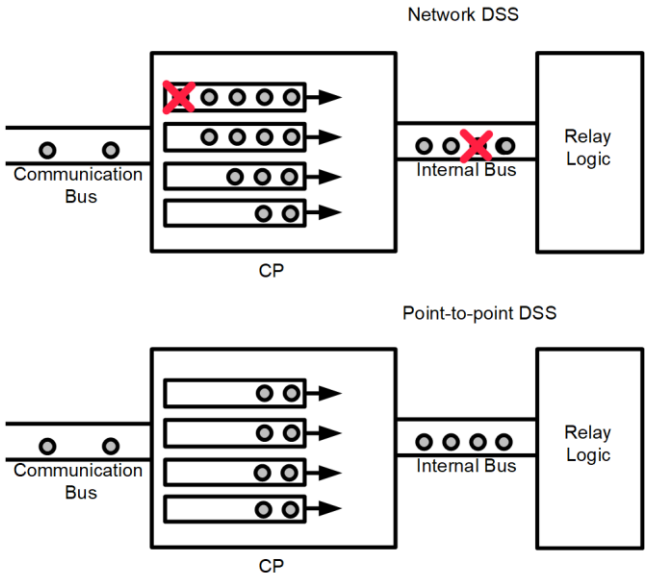

Fig. 6. Network and P2P DSS serialization.

In an Ethernet-network-based DSS, the packet delivery is not deterministic. Therefore, it is susceptible to network overload situations, such as cyberattacks, bad network designs, and downtimes due to network reconfiguration [21]. During this situation, the data serialization process of packets can be compromised, causing packet loss at the communication network level, which can lead to misoperation. Best network design principles, such as VLANs and SDN technology, can be used to avoid DSS protection system outages due to network overload and attacks on cybersecurity [22]. Network redundancy principles, such as ladder architecture, can be used to avoid network downtime, preventing power system protection from being unavailable during network outages [12] [23]. However, including all of those mitigation strategies adds complexity to the protection system design.

In a P2P DSS, the link is dedicated to only DSS traffic, avoiding possible network engineering mistakes and enhancing the cybersecurity of the system. In addition, multiple P2P links can be used to achieve data-sharing capabilities.

IV. Protection Relay Design for DSS

In an IEC 61850-based DSS, a protection relay receives current and voltage signals published by MUs in a digital format via an Ethernet network. The received signals (SV streams) from multiple MUs are time-aligned in the relay before the data are sent to the protection functions. Hence, a DSS protection relay needs to handle the following situations:

- Loss of one or more SV packets
- Variable SV network delay
- Loss of SV streams
- Time synchronization state (SmpSynch) of each SV stream

A. DSS Latency

As discussed in Section III, SV network delay includes MU processing delay and the process bus network delay. When MUs from multiple manufacturers are used and the MU SV stream passes through different nodes in a network, the network delay for each MU can be different. A user-configurable DSS latency setting is usually provided in a DSS relay to handle this situation. It is essential to provide ride through capability for loss of one or more SV messages. The buffer time for the number of SV messages that can be ride-through messages is included in the DSS latency setting. It is a recommended practice to measure the SV network delay during commissioning and adjust this setting accordingly.

This setting value provides a consistent delay to protection functions, which overcomes the nondeterministic delays caused by the Ethernet process bus network. Since incoming SV streams are buffered for the period of DSS latency setting, protection and control operation times for the DSS relay are delayed by the same value compared to the times of conventional relays with hard wired CT/PT connections. If the load on the process bus network increases significantly, it can increase network delay. If the network delay exceeds the setting in the DSS relay, the system can no longer use the incoming SV stream and the SV stream will be lost. Therefore, it is extremely important to engineer the process bus network and monitor the network delay.

B. Selective Protection Disabling

A DSS relay subscribes to multiple SV streams from MUs to execute protection functions. For all protection functions to remain enabled, all SV streams must be available and all MUs and the relay must synchronize to the same time source. When an MU fails or a communication link breaks, the SV stream from that MU is unavailable in the relay. Similarly, when an MU loses its time synchronization signal, the relay is unable to time-align the data for protection. For these cases, a DSS relay selectively disables protection functions that operate on the SV stream from the faulty MU. Selective protection disabling maximizes the availability of protection functions that are not

impacted by lost SV streams. In a DSS line relay, when an SV stream carrying a voltage signal is unavailable, protection functions that need voltage (e.g., distance, directional, or loss of potential functions) are blocked. However, protection functions that do not require voltage (e.g., overcurrent, or breaker failure functions) remain available.

Most of DSS relays use predominantly fundamental frequency phasors of voltages and currents for protection function algorithms. Accurate measurement of phasor quantities typically takes a cycle. When a DSS relay starts subscribing to SV streams from a previously unavailable MU, it takes some time for the phasors to reach a steady state. The protection functions remain disabled until the steady state for phasors from the SV stream is reached. The DSS relay immediately disables selective protection functions when it detects the loss of an SV stream, and it keeps them disabled for a fixed time after the SV stream reappears. If protection functions are enabled immediately after the SV stream is available, it can result in protection function misoperation due to signal transients.

A DSS bus relay configured to protect three feeders is shown in Fig. 7. For simplicity, the details of the process bus network and time source are not included. For each feeder, overcurrent and breaker failure functions (PIOC, PTOC, and RBRF) are configured. A bus differential function, PDIF, is set to protect the bus. When SV streams from MU1 to MU3 are received by the bus relay, all protection functions are available.

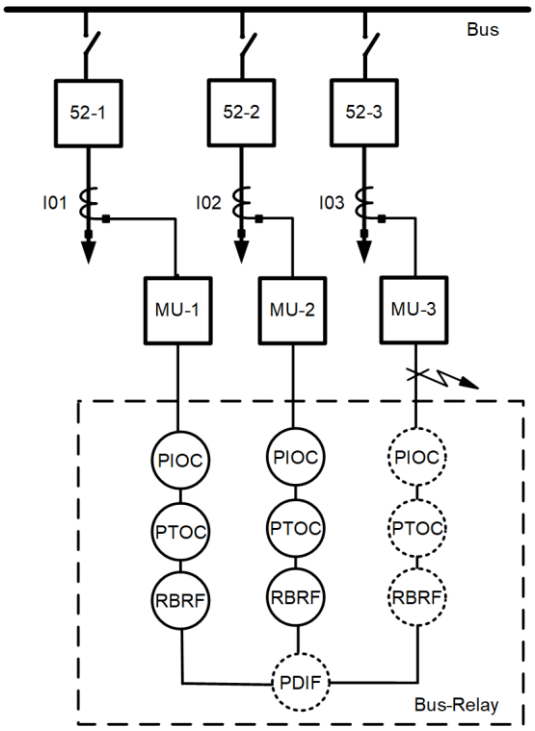

Fig. 7. Selective protection disabling in a bus relay during loss of MU-3.

In a case when MU-3 is temporarily unavailable due to communication link failure, the bus relay selectively disables the PDIF function and PIOC, PTOC, and RBRF functions associated with MU-3. Protection functions associated to MU-1 and MU-2 are still available and protect Feeders 1 and 2.

Fig. 8 shows the bus relay event record for the case after the MU-3 communication link issue is resolved. Before I03 current from MU-3 is available, there is a fictitious differential current seen by the bus relay. In this state, the 87R bit asserts as the operating current (IOP1) exceeds the restraining current (IOP1(IRT1)). The selective protection disabling feature in the bus relay prevents the 87R bit from asserting the differential protection bits (87Z1 and 87Z2). Next, we consider two cases. In the first case, differential protection is enabled immediately after MU-3 is available (indicated by deassertion of the 87BLK1 bit). In the second case, differential protection is enabled after a fixed delay to ensure that phasor transients have died down (indicated by deassertion of the 87BLK2 bit). Immediately after the relay starts subscribing to MU-3, the fictitious operating current is still higher than the restraining current. Next, the operating current starts to decrease and the restarting current increases. If differential protection, PDIF, is enabled immediately after the relay subscribes MU-3, the PDIF function misoperates, as indicated by assertion of the 87Z1 bit. When protection elements are enabled after a fixed delay, it keeps the PDIF function secure, as indicated by no assertion of 87Z2 bit. Hence, for security, it is critical to delay the enabling of protection functions after the resumption of the lost MU.

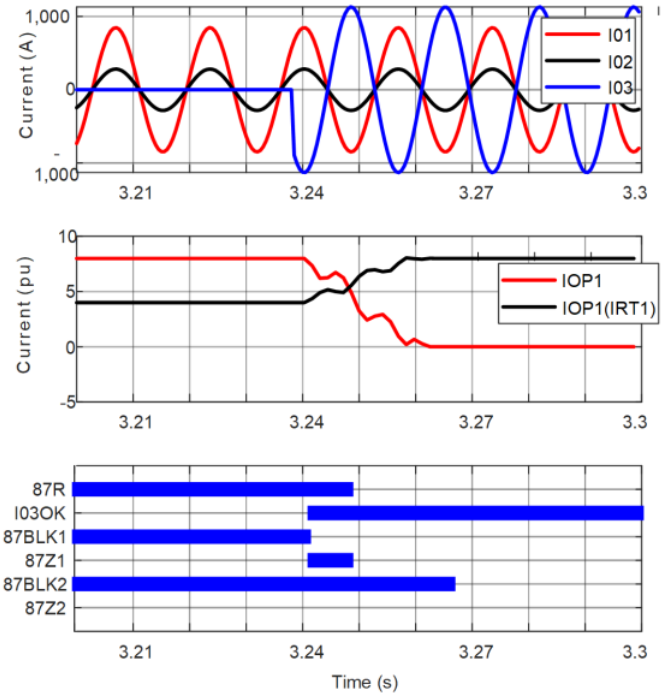

Fig. 8. Selective protection disabling of PDIF function for MU-3 loss case.

V. Impacts on Protection Functions

For executing protection functions, an IEC 61850-based DSS relay subscribes to all required SV streams and time-aligns these streams. When one or more SV streams is unavailable, it impacts the protection functions that require those SV streams. Similarly, when an MU loses its time synchronization signal, a DSS relay cannot use its signal for time alignment, which in turn affects protection functions. These issues can result from a faulty MU, a communication link failure, poor network design,

an unreliable satellite clock, the synchronization behavior of protective relays, or using MUs from multiple manufacturers. The next section provides specific examples of how protection functions can be affected.

A. Impacts of Time Synchronization on Protection

In a traditional substation, an absolute time source is not required to run local protection functions. However, a time source, usually an IRIG-B or 1 PPS signal, is connected to provide accurate time stamps for Sequence of Events (SOE) and relay event records. As a result, typically one satellite clock is used to distribute time in a traditional substation.

When a process bus based on IEC 61850 is implemented, a common time synchronization source is required for all MUs and DSS relays. The common time source allows DSS relays to time-align incoming SV streams from multiple MUs and execute protection functions. PTP is the preferred time synchronization method for a process bus.

Table IX lists the holdover accuracy for various PTP clocks available from different manufacturers. The table also lists the time interval for which the PTP clock can maintain a time accuracy of 1 µs or lower. As per IEC 61850-5, T5 time synchronization class (1 µs accuracy) is recommended for SV applications. If only one satellite clock is used for the station and the antenna fails, the best PTP clock from the table can keep the system within 1 µs of GPS time for a maximum of 28.36 hours (PTP Clock E with rubidium oscillator). There is a short time window to find a replacement and replace the antenna for most unmanned substations and remote substations. Once time inaccuracy exceeds T5 time synchronization class, some protection functions may be blocked (for example, Synchrophasor based wide-area protection schemes) while others may continue in an islanded mode. This example shows the necessity of using at least two clocks when implementing IEC 61850-based process bus protection. Even if the end user has only a small distribution substation, for protection to remain enabled following a clock or an antenna failure, two PTP clocks are required. In [24], the authors describe using dual-antenna, dual-clock architecture to achieve high resiliency. Redundancy increases availability but increases complexity and costs.

The next example shows the impact on protection functions when two MUs behave differently during a time synchronization event. Fig. 9 shows the test setup where MU-1, MU-2, an SV relay, and a PTP clock are connected to a process bus network. Two MUs from different manufacturers are used and both support IEEE C37.238 Power System PTP Profile. The SV relay is configured to subscribe SV streams from both MUs. The antenna is connected to the clock for some time to reach GM clockClass of 6. The GM ID is set to 100.

Table X provides the relationship between the GM clockClass described in IEEE 1588 and the SmpSynch attribute described in IEC 61850-9-2. As per IEC 61850-9-2 (and IEC 61869-9-2016), when SV are synchronized to a global area clock, the SmpSynch value should be 2 [25]. Similarly, when SV are synchronized by a local area clock, the SmpSynch value should be one (or GM ID if IEEE C37.238-2011 Power System Profile is used).

TABLE IX
HOLDOVER ACCURACY FOR VARIOUS PTP CLOCKS

PTP Clock	Oscillator Type	Holdover Accuracy	Time Accuracy of <1 µs
Clock A	TCXO	±36 µs/24 hr	40 min
	OCXO	±5 µs/24 hr	4.8 hr
Clock B	TCXO	±800 µs/24 hr	108 s
Clock C	TCXO	±100 µs/4 hr	144 s
	OCXO	±5 µs/8 hr	1.6 hr
	Rubidium	±1 µs/24 hr	24 hr
Clock D	TCXO	±4.3 ms/24 hr	20 s
	OCXO DHQ	±4.5 µs/24 hr	5.33 hr
	Rubidium	±1.1 µs/24 hr	21.8 hr
Clock E	Quartz	±1.1 µs/4 hr	3.63 hr
	Rubidium	±1.1 µs/1.3 days	28.36 hr
Clock F	OCXO	1 ms/24 hr	86.4 s

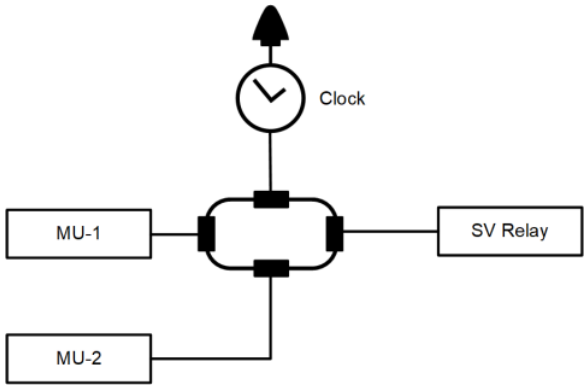

Fig. 9. Setup to study the impact of time synchronization on protection.

TABLE X
RELATIONSHIP BETWEEN IEEE C37.238-2011 CLOCKCLASS AND SMPSYNCH

GM State	GM clockClass	SmpSynch
GM is synchronized to the primary reference time source and in a steady state.	6	2
GM has lost synchronization to the primary reference time source and is operating within holdover specification.	7	1 or (GMID*)
GM is operating outside its holdover specification.	187	0

* Power System Profile

While the PTP clock was connected to the GPS, both MUs and the SV relay reported SmpSynch value as 2. As a result, the SV relay subscribed to SV streams from both MUs. Next, the antenna from the PTP clock was removed. This resulted in the change of GM clockClass from 6 to 7, as shown in the table. After the holdover period of the SV relay elapsed, its SmpSynch value changed from 2 (Global) to 100 (GM ID). Similarly, the SmpSynch value of MU-1 followed the SV relay after its own holdover period elapsed. However, the SmpSynch value of MU-2 stayed at 2 throughout the test.

Fig. 10 shows the event report captured by the SV relay during the test. The SV relay is configured to drop all SV streams, except for the first SV stream (MU-1), when there is a difference between its SmpSynch value and the incoming SV streams. Soon after the SV relay SmpSynch updated to 100, the relay dropped the MU-2 SV. Both the SV relay and MU-1 SmpSynch value changed to GM ID. Since MU-2 SmpSynch never changed to GM ID, the SV relay did not subscribe to the MU-2 SV stream. This led to selective disabling of protection functions in the SV relay that used the MU-2 SV stream.

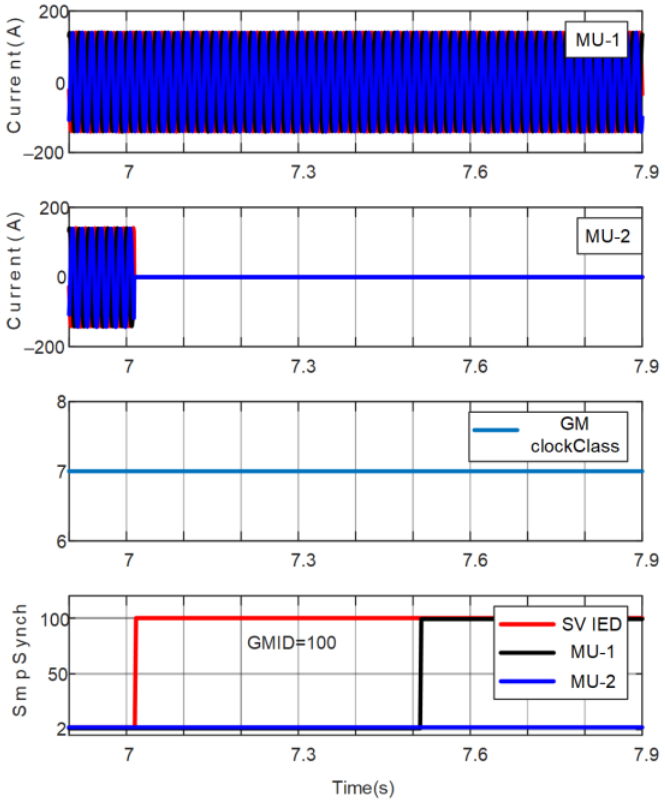

Fig. 10. Change in SmpSynch value following GM antenna failure test.

IEEE 1588 has been revised multiple times in the last decade, and both IEEE and IEC standards related to process bus and time synchronization are becoming interdependent and muddled. When standards are not clear, it can result in different types of implementation among manufacturers which can lead to an interoperability issue, as explained in the previous example. In addition, the IEC 61850 interoperability testing final reports list eleven issues related to time synchronization and PTP in 2017 and four issues in 2019 [26]. Clearly, when devices from different manufacturers are used and the implementation of standards is not uniform, it can result in the blocking of protection functions.

B. Impacts of Network Delay on Protection

Since time synchronization information and SV streams pass through the common process bus, an engineered process bus network is essential for protection function reliability. Several network architectures, such as PRP, HSR, and SDN, are widely used for process bus redundancy. When a network is not engineered correctly or is highly congested, it can lead to packet loss. Packet loss can also result from a bad splice or bad connector, link loss, a hardware issue in the switch, and environmental influences like electrostatic discharge. As described earlier, SV relays are typically designed to ride through the loss of three consecutive SV messages without impacting protection functions. When additional SV messages are dropped, the SV relay selectively disables protection to avoid any undesired operation. Fig. 11 shows laboratory test results for the momentary loss of an SV stream in a congested network.

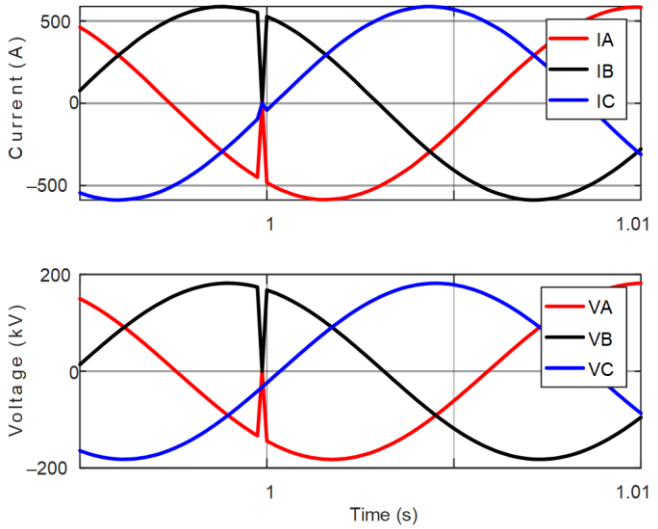

Fig. 11. Momentary SV stream loss in congested network.

The next example shows the impact of process bus network delay on the overall fault-clearing time using the setup shown in Fig. 12. Two identical power system models are developed

in a real-time digital simulator (RTDS). Each power system consists of a feeder connected to a bus via a breaker with a two-cycle interrupting time. Analog signals from the RTDS are connected using a low-level signal interface to the traditional relay and the MU. The DSS relay receives power system signals from the MU via an Ethernet switch. A simple time overcurrent function is set in both relays. A DSS latency of 3 ms is set in the DSS relay to emulate a congested network with multiple network hops. The output contact from the traditional relay is wired directly to the RTDS breaker trip input. The DSS relay sends the trip signal to the MU via GOOSE message and the MU output contact is wired to the RTDS.

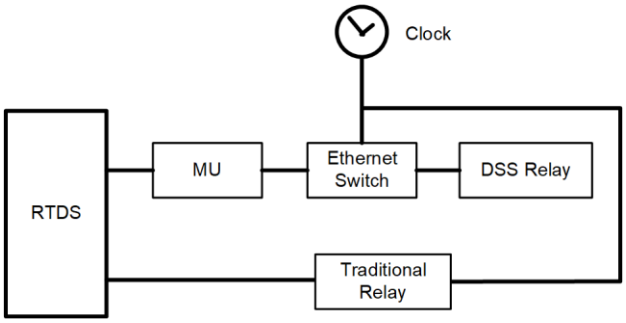

Fig. 12. Test setup to compare fault-clearing time between traditional and SV relays.

Time-aligned event reports from the traditional relay and the MU for a CA phase-to-phase fault are shown in Fig. 13. The difference in trip time between the traditional relay and the MU is approximately 5 ms. This time difference is the result of the 3 ms DSS latency setting in the SV relay and the GOOSE message transfer times. When the breaker current in Phase A and Phase C is analyzed, it becomes clear that the breaker associated with the SV system took an additional half-cycle to open. This test shows the impact of network delay for an SV system on overall fault-clearing time. Faster fault-clearing enhances personnel safety, limits equipment wear and property damage, and improves power quality. Similarly, when faults are cleared faster than the critical clearing time, it improves transient stability and increases the amount of power that can be transferred [27]. In conclusion, a long network delay impacts the relay operating time, which in turn affects the overall fault-clearing time.

VI. P2P-Based DSS

A P2P-based DSS uses the simplest network architecture to exchange process data. A P2P-based DSS does not require any network switches and clocks for operation. This removes the complexity of configuring switches and clocks during the engineering phase. As a result, it greatly simplifies the engineering labor required to set up the DSS. Unlike an Ethernet-network-based DSS, protection function availability is not impacted by issues in clocks and switches.

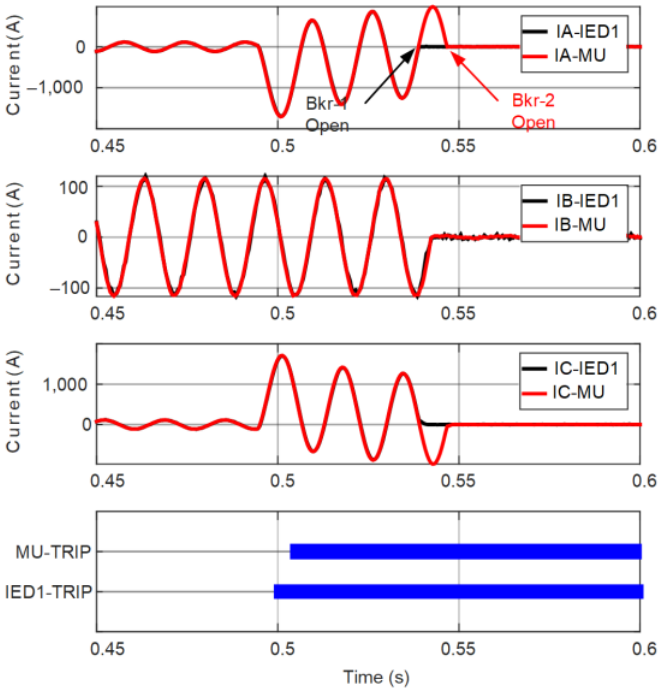

Fig. 13. Difference in fault-clearing time between a traditional relay and an SV relay.

Fig. 14 shows both the network-based and P2P-based DSS solutions. The network-based DSS requires four devices (MU, Ethernet switch, Clock, IEC 61850 DSS relay), whereas a P2P-based DSS needs two (MU, P2P DSS relay). Having fewer devices greatly improves the availability of the system. If we assume the same mean time between failures (MTBF) for all devices, the overall MTBF of a P2P-based DSS is twice that of that a network-based DSS. Lower device count results in increased reliability at lower cost.

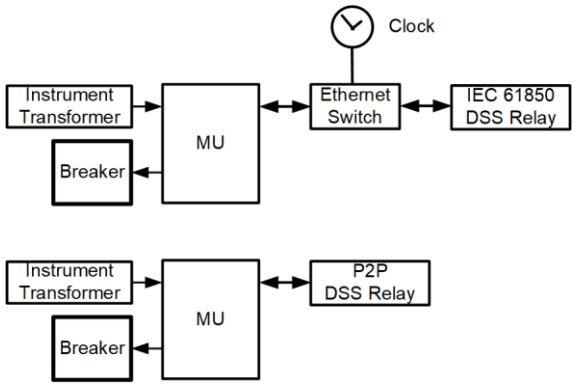

Fig. 14. Network-based and P2P-based DSS solutions.

A P2P-based DSS can use a standard protocol or a manufacturer-specific protocol [28] [29]. A P2P network architecture can be used for local protection as well as centralized substation protection and control. Various centralized protection and control (CPC) architectures based on P2P connections are described in [30]. Table XI provides a summary of the various benefits and challenges of a traditional system, a network-based DSS, and a P2P-based DSS [1].

TABLE XI
COMPARISON BETWEEN THREE DIFFERENT SUBSTATION SYSTEMS

Attribute	Traditional System	Network-Based DSS	P2P-Based DSS
Safety from high-energy cables	No	Yes	Yes
Electromagnetic interference	Yes	No	No
Substation construction costs	High	High	Low
Self-monitoring of the secondary circuitry	No	Yes	Yes
Wiring errors	High	Low	Low
Data loss ride through capability	Not possible	Possible	Possible
Network engineering requirement	No	Yes	No
Unavailability	Low	High	Medium
Protection speed	Fast	Slightly slower than P2P-based system	Slightly slower than traditional system
High accurate time source requirement	No	Yes	No
Network latency	NA	High	Low
Network jitter	NA	High	Low
Interoperability	Yes	Yes	Possible

VII. CONCLUSION

DSS solutions eliminate copper cables between the primary equipment and the protective relays, leading to improved personnel safety and lower substation construction costs. IEC 61850-based DSS solutions use switched network architecture to communicate between MUs and relays. The process bus network is used to transfer SV, GOOSE, and time synchronization messages between the connected devices. Since SV from multiple MUs arrive at different times in a DSS relay, it is designed to handle variable network delay and has ride-through capability for the loss of a few SV messages. Loss of an SV stream due to a network issue or an incorrect device time synchronization state adversely impacts protection function availability. The selective protection disabling feature in a DSS relay is designed to maximize the availability of protection functions that are not impacted by lost SV streams. IEC 61850 standards allow interoperability between devices from multiple manufacturers. However, when the implementation of standard is not uniform between manufacturers, it can result in unavailability of protection functions following an event that impacts the process bus network or the time source.

P2P-based DSS solutions are equally worthy alternatives that take advantage of the benefits offered by a DSS. This type of solution uses the simplest P2P architecture to exchange information between devices. Protection function availability is independent of an external time source in a P2P-based DSS.

VIII. REFERENCES

[1] G. Rzepka, S. Wenke, and S. Walling, "Choose Simplicity for a Better Digital Substation Design," proceedings of the 70th Annual Conference for Protective Relay Engineers, 2017.

[2] B. Kasztenny, D. McGinn, W. Ang, R. Mao, D. Baigent, N. Nazir, S. Hodder, and J. Mazareeuw, "An Architecture and System for IEC 61850 Process Bus," GE Digital Energy Protection and Control Journal, pp.19-29, October 2008.

[3] IEC 61850-9-2, Communication Networks and Systems for Power Utility Automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3, Section 5.3.3.4.4, Figure 3, 2011.

[4] IEEE Std 1588-2019 - IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, in IEEE 588-2019 (Revision of IEEE 1588-2008) , pp.1-499, 16 June 2020.

[5] J. Peer, E. Sagen, S. Achanta, and V. Skendzic, "The Future of Time: Evolving Requirements for Precise Time Synchronization in the Electric Power Industry," Schweitzer Engineering Laboratories, Inc., 2011.

[6] E. O. Schweitzer, III, D. Whitehead, S. Achanta, and V. Skendzic, "Implementing Robust Time Solutions for Modern Power Systems," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

[7] IEEE C37.238-2011 - IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications, 2011.

[8] IEC/IEEE International Standard - Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation, in IEC/IEEE 61850-9-3 Edition 1.0 2016-05, pp.1–18, May 2016.

[9] IEC 61850, Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models, 2013.

[10] M. Silveira, D. Dolezilek, S. Wenke, and J. Yellajosula, "Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation," proceedings of the 74th Annual Conference for Protective Relay Engineers, 2021.

[11] K. Fodero, C. Huntley, and P. Robertson, "Secure and Reliable GPS-Based Time Distribution," in Wide-Area Protection and Control Systems: A Collection of Technical Papers Representing Modern Solutions, 2017.

[12] IEC, Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), 2012.

[13] Q. Yang and R. Smith, "Improve Protection Communications Network Reliability Through Software-Defined Process Bus," proceedings of the Grid of the Future Symposium, Reston, VA, October 2018.

[14] B. Falahati, M. J. Mousavi, and M. Vakilian, "Latency Considerations in IEC 61850-Enabled," in IEEE, 2011.

[15] Q. Yang, D. Keckalo, D. Dolezilek, and E. Cenzon, "Testing IEC 61850 Merging Units," proceedings of the 44th Annual Western Protective Relay Conference, Spokane, WA, October 2017.

[16] G. Aceto, F. Palumbo, V. Persico, and A. Pescapé "Available Bandwidth vs. Achievable Throughput Measurements in 4G Mobile Networks," proceedings of the 14th International Conference on Network and Service Management, 2018.

[17] P. Franco, G. Rocha, and D. Dolezilek, "Improving Reliability and Security of Protection Algorithms Via Signal Message Supervision," proceedings of the 13th International Conference on Developments in Power System Protection, 2016.

[18] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, "Design and Validation Practices for Ethernet Networks to Support Automation and Control Applications," proceedings of the Power and Energy Automation Conference, 2014.

[19] R. Meine, "A Practical Guide to Designing and Deploying OT SDN Networks," proceedings of the Power and Energy Automation Conference, Spokane, WA, 2019.

[20] J. L. Blackburn and T. J. Domin, *Protective Relaying: Principles and Applications*, Fourth Edition, CRC Press, 2014.

[21] M. Silveira and P. Franco, "IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities," proceedings of the 6th Annual PAC World Americas Conference, 2019.

[22] M. Cabral, M. Silveira, and R. Urie, "SDN Advantages for Ethernet-Based Control," Schweitzer Engineering Laboratories, Inc., 2019.

[23] D. Dolezilek, J. Dearien, A. Kalra, and J. Needs, "Appropriate Testing Reveals New Best-in-Class Topology for Ethernet Networks," proceedings of the 13th International Conference on Developments in Power System Protection, 2016.

[24] D. Maragal and F. Ronci, "Redundancy in Time Synchronization System," proceedings of the PAC World Conference, 2020.

[25] IEC 61850-9-2, Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3, 2011.

[26] IEC 61850 2019 IOP Final Report 20200122–UCAIug, Available: ucaiug.org/IOP_Registration/IOP%20Reports/IEC%20 61850%202019%20IOP%20Final%20Report%2020200122.pdf

[27] E. O. Schweitzer, III, B. Kasztenny, A. Guzmán, V. Skendzic, and M. V. Mynam, "Speed of Line Protection – Can We Break Free of Phasor Limitations?" proceedings of the 41st Annual Western Protective Relay Conference, Spokane, WA, October 2014.

[28] IEC 61850-9-1, Communication networks and systems in substations-Part 9-1: Specific communication service mapping (SCSM) - Sampled values over serial unidirectional multidrop point to point link.

[29] SEL-421 Protection, Automation, and Control System Instruction Manual. Available: selinc.com.

[30] IEEE PSRC, WG K15, "Centralized Substation Protection and Control," 2015.

IX. Biographies

Arun Shrestha received his BSEE from the Institute of Engineering, Tribhuvan University, Nepal, in 2005, and his MS and PhD in electrical engineering from the University of North Carolina at Charlotte in 2009 and 2016, respectively. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2011 as an associate power engineer in research and development. He is presently working as a development lead engineer. His research areas of interest include power system protection and control design, real-time power system modeling and simulation, wide-area protection and control, power system stability, and digital substations. He is a senior member of IEEE and is a registered Professional Engineer. He is a member of IEEE PSRC and a U.S. representative to IEC 61850 TC 57 WG 10.

Mauricio Gadelha da Silveira is an electrical engineer with a BS earned from São Paulo State University in 2013. Since 2014, he has been with Schweitzer Engineering Laboratories, Inc. (SEL), where he has held positions in SEL Engineering Services, Inc. (SEL ES), sales and customer service, and research and development. He is currently a lead integration and automation engineer. His work includes development of protective relay protocols and communications, network design for critical infrastructures, power system modeling, and cybersecurity assessment.

Jaya Yellajosula received his MSc and PhD in electrical engineering in 2016 and 2019, respectively, from Michigan Technological University, Houghton, MI. He worked as an integration and automation engineer at Schweitzer Engineering Laboratories, Inc. (SEL), from 2019 until 2021. Currently he is a power system studies engineer at SEL. His research interests include power system protection, automation, and control in smart grids.

Sathish Kumar Mutha received his MS degree in electrical engineering in 2020 from the University of North Carolina at Charlotte. Prior to earning his M.S degree, he worked as a power plant operation engineer in India. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2019 as an engineer intern. Currently he is a power engineer at SEL.