Network Engineering and Testing of an IEC 61850-Based Distributed Busbar Protection Scheme

Md Aamir Rahmani, Wesley Roberto, Ali Khan, Mauricio Silveira, and Arun Shrestha
Schweitzer Engineering Laboratories, Inc.

Presented at the
2026 PAC World Americas Conference
Raleigh, North Carolina
August 17–20, 2026

Network Engineering and Testing of an IEC 61850-Based Distributed Busbar Protection Scheme

Md Aamir Rahmani, Wesley Roberto, Ali Khan, Mauricio Silveira, and Arun Shrestha,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—IEC 61850-based digital secondary systems (DSSs) enable scalable implementation of distributed busbar protection but introduce a strong dependence on communications network performance. In large-scale applications, Sampled Values (SV) traffic combined with Generic Object-Oriented Substation Event (GOOSE) messaging leads to high bandwidth utilization, increased packet delay variation (PDV), and challenges in deterministic signal delivery. There is limited work that quantitatively links network traffic characteristics to protection operation speed and integrates analysis with system-level engineering, validation, and monitoring. This paper presents a comprehensive framework for network engineering and testing of a 21-bay IEC 61850-based distributed busbar protection system. An analytical model is developed to relate traffic intensity, multicast message forwarding, and link capacity to PDV and SV channel delay, considering IEC 61869-9 SV configurations. A system-level engineering approach is introduced to translate protection designs into repeatable network configuration using System Configuration Description Language (SCL) and centralized management. The analysis is validated using a real-time hardware-in-the-loop (RT-HIL) platform, measuring PDV, channel delay, and fault detection time under fault conditions. Monitoring techniques are also presented to supervise system performance. The proposed framework provides quantitative insight into the relationship between network design and protection behavior, supporting the engineering of reliable and deterministic DSS-based busbar protection systems.**

I. Introduction

Busbar protection is one of the most critical protection functions in a power system because faults on the bus can simultaneously affect multiple connected circuits and must be cleared rapidly to maintain system stability and equipment integrity [1]. The design of busbar protection schemes depends strongly on substation topology, including single bus, double bus, transfer bus, and sectionalized arrangements, as well as the ability of terminals to dynamically switch between protection zones. In complex configurations, such as double-bus systems with transfer buses and sectionalizers, protection systems must continuously adapt to changing switching states, resulting in increased protection complexity and multiple measurements, control signals, and protection zones [2].

The adoption of IEC 61850-based digital secondary systems (DSSs) has transformed the implementation of such protection schemes by replacing extensive copper wiring with Ethernet-based communications networks [3]. In DSS architectures, process interface units (PIUs) digitize analog current and voltage measurements at the primary equipment and publish these measurements as Sampled Values (SV) over the process bus, while status and control signals are exchanged among the PIUs and the protective intelligent electronic devices (IEDs) using Generic Object-Oriented Substation Event (GOOSE) messaging, and time synchronization is achieved through Precision Time Protocol (PTP). This transition significantly reduces wiring complexity and enables data sharing across devices, but it also makes protection performance dependent on the communications network, since SV and GOOSE messages carry the measurements, status information, and control commands required for protection functions [4] [5].

In large-scale distributed busbar protection systems, SV traffic typically dominates process bus bandwidth due to the continuous transmission of high-rate sampled measurements from multiple PIUs [6]. This traffic is combined with GOOSE messaging, particularly during switching operations and fault conditions, resulting in high traffic intensity on shared communications paths. Under these conditions, network performance is governed by bandwidth utilization, multicast traffic distribution, link capacity, and queuing behavior. These factors directly influence packet delay variation (PDV) and end-to-end communications delay, which, in turn, affect the protection operation speed and reliability of busbar protection [7].

IEC 61869-9 recommends flexible SV configurations that allow multiple application service data units (ASDUs) to be aggregated within a single Ethernet frame, providing tradeoffs between bandwidth utilization and data delivery delay [7]. At the same time, inadequate traffic engineering may result in unnecessary multicast message forwarding, increasing network loading and reducing deterministic communications performance [8]. Therefore, process bus design must consider not only bandwidth capacity but also traffic control mechanisms, redundancy strategies, and system-level supervision.

While existing standards and prior work provide guidance on process bus communications, network optimization, and protection system design, these aspects are often addressed independently [9] [10] [11] [12]. There is limited published research that quantitatively links process bus traffic characteristics, PDV, and the resulting protection operation time, particularly for large-scale busbar protection systems. In addition, there is a lack of integrated methodologies that connect analytical modeling with system-level configuration, validation, and operational monitoring.

Traffic control is required to prevent unnecessary forwarding of multicast SV and GOOSE traffic. This paper evaluates how traffic engineering affects bandwidth utilization, PDV, and protection operation speed. In this work, software-defined

networking (SDN) is adopted to centrally manage traffic forwarding, prioritization, and monitoring across both the process bus and station bus networks [4].

Reliability in DSSs requires both redundancy and observability. Observability in DSS refers to the continuous monitoring of communications paths, applications, and device statuses to ensure that redundant systems function correctly and that hidden failures are detected before they affect protection reliability. Protocols such as Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR) protocol improve availability by transmitting duplicate frames over independent communications paths, enabling continued operation during a single network failure [13]. However, failures in one communications path may remain undetected without proper supervision [14]. Therefore, communications paths, applications, and device statuses must be continuously monitored to ensure that redundant systems operate as intended and that latent failures do not compromise protection dependability [15]. These requirements highlight the importance of system-level monitoring and diagnostics in addition to network design.

The engineering complexity increases further in large-scale systems that include numerous PIUs, protective IEDs, network switches, Global Navigation Satellite System clocks, and communications streams. Manual configuration of these elements is time consuming and increases the risk of inconsistent or incorrect settings. IEC 61850 System Configuration Description Language (SCL) provides a structured mechanism to define communications relationships between devices, enabling consistent and automated configuration of communications systems. The availability of this description motivates the need for a system-level engineering approach that translates protection design into repeatable and scalable network configuration.

These challenges demonstrate that process bus design requires a coordinated approach that integrates traffic engineering, system configuration, validation, and monitoring into a unified workflow. The scope of this approach is illustrated in Fig. 1, which summarizes the key engineering elements required for large DSS-based busbar protection systems.

As shown in Fig. 1, reliable protection performance in DSS environments cannot be achieved through isolated design steps, but through a structured framework in which network modeling, configuration, implementation, testing, and monitoring are treated as interdependent components. Network design decisions, such as link speed selection and SV configuration, directly influence traffic intensity and delay behavior. These effects must be accounted for in system-level configuration, validated through testing, and continuously verified through monitoring during operation.

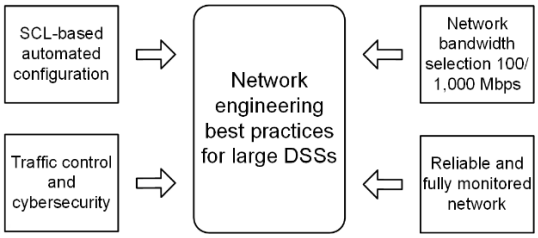

Fig. 1. Network engineering elements for large DSS-based busbar protection systems

To address these challenges, engineering and testing of IEC 61850-based distributed busbar protection systems are necessary. The proposed approach connects network design decisions to protection system performance through analytical modeling, system-level configuration, experimental validation, and operational supervision.

The remainder of the paper describes the studied busbar protection architecture, develops the process bus traffic and PDV model, presents the system-level configuration approach, validates the results using real-time hardware-in-the-loop (RT-HIL) testing, and discusses monitoring methods for operational supervision.

II. System Architecture and Design

A. Electrical Topology and Protection Zones

A substation with 21 current terminals comprising 13 feeder bays, 2 transfer bays, 2 sectionalizers, 2 bus-coupler bays, and 3 bus bars is modeled as shown in Fig. 2. Two busbars increase operational flexibility and reduce the consequences of busbar faults by not tripping all circuit breakers, while the transfer bus can be used to bypass the feeder circuit breaker as required for maintenance while keeping the feeder live. Each bay has its own circuit breaker and a current transformer. The feeders and transfer bays each have four disconnect switches that enable them to select the parent busbar. The two main busbars are divided into two sections by means of sectionalizer breakers, also to facilitate maintenance.

B. Protection Philosophy and Zones

A busbar protection scheme monitors the statuses of disconnect switches in feeders and transfer bays to determine which feeders are connected to a particular section of the busbar. These sections are referred to as bus-zones. A typical bus-zone will include a section of the busbar and the feeders that are connected to it at any given time. Bus-zones improve selectivity of the system. If two bus-zones are not merged, a fault in one of the zones would be limited to the feeders and bus sections included in the respective bus-zone only. The other bus-zones remain energized.

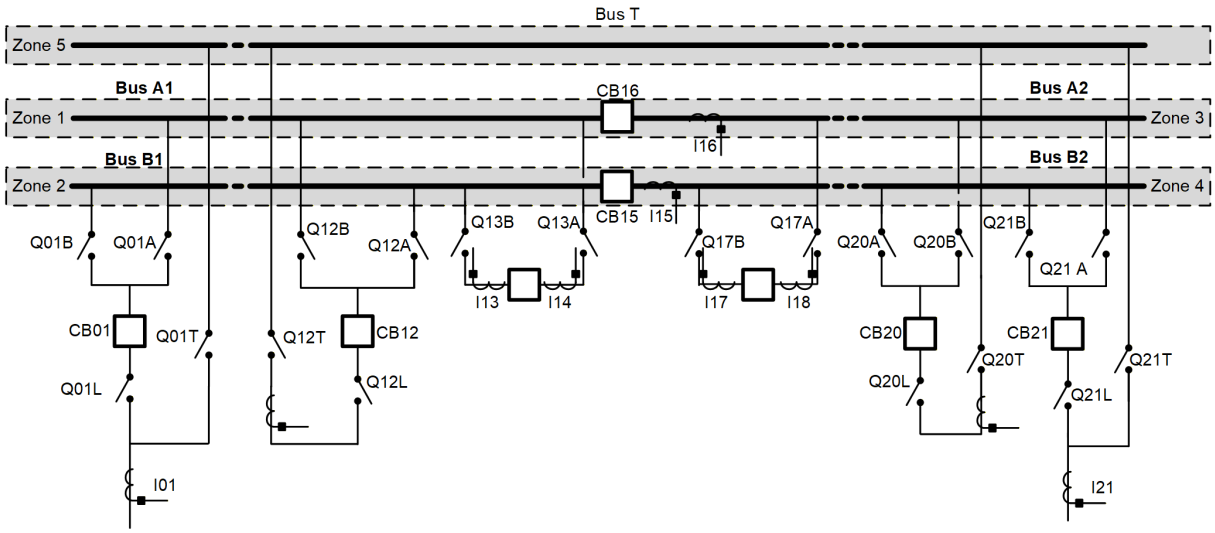

Fig. 2. Single-line diagram of 21-bay double bus with transfer bus, bus couplers, and sectionalizers.

Fig. 2 illustrates a double-bus, single-breaker busbar arrangement with a transfer bus, where the protection scheme is divided into five dynamic zones based on disconnector status. Zone 1 (Z1) and Z3 correspond to sections of Bus A (Bus A1 and Bus A2) and are selected when disconnector Q*xx*A is closed, while Z2 and Z4 correspond to sections of Bus B (Bus B1 and Bus B2) and are selected when disconnector Q*xx*B is closed. Here, *xx* denotes the bay number ranging from 01 to 21. Zone Z5 represents the transfer bus (Bus T) and is selected through the transfer disconnector Q*xx*T. Each zone includes a set of current inputs associated with the feeders connected to the respective bus section. When both disconnectors A and B are closed for a given bay, the corresponding zones are dynamically merged. In this condition, Z1 and Z2 are combined into a single Zone Z1, incorporating all associated feeder currents, while Z2 is disabled; similarly, Z3 and Z4 are merged into Zone Z3 while Z4 is disabled. This dynamic zone selection mechanism ensures that the protection scheme correctly adapts to switching configurations and maintains proper association of currents with the active protection zones.

C. *Differential Protection Algorithm*

The characteristic of the busbar differential element (87B) as referenced in [1] defines the operating region above the intersection of two straight lines:

$$y = \text{Operating Current Threshold}$$
$$y = \text{Slope} * \text{Restraining Current}$$

where the operating current (I_{op}) is the sum of currents entering and leaving the busbar, whereas the restraining current (I_{res}) is the sum of the absolute values of the current entering and leaving the busbar. Slope is a user-configured variable that is often expressed as a percentage. The differential algorithm has two configurable slopes, 1 and 2. Slope 1 is effective for internal faults, and Slope 2 is effective for external faults. A separate internal fault detection logic switches the slope to Slope 2 if an external fault is detected. Slope switching adds an additional layer of security against misoperation during external faults [1].

As shown in Fig. 3, a trip is issued if:

$$\frac{I_{op}}{I_{res}} > \frac{\text{Slope 1 or Slope 2}}{100} \quad \text{and} \quad I_{op} > \text{Operating Current Threshold} \tag{1}$$

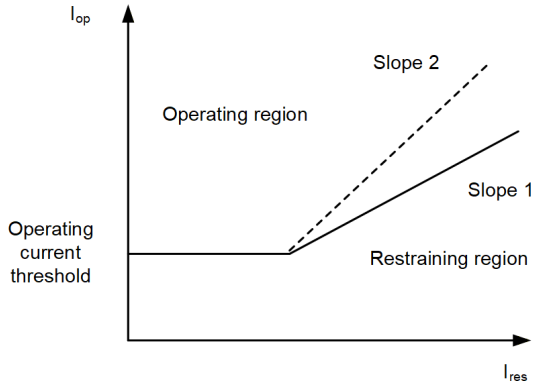

Fig. 3. Operating characteristic of the 87B element.

D. *Network Architecture*

The network shown in Fig. 4 is divided into process bus and station bus. Process bus is used for essential protection Ethernet traffic, like SV between the PIU and protective IEDs, PTP packets for nanosecond time synchronization from clocks to IEDs, and GOOSE messages that carry the trip signal from the protection IEDs to the PIU and disconnect and breaker status from the merging unit to the protective IEDs [7].

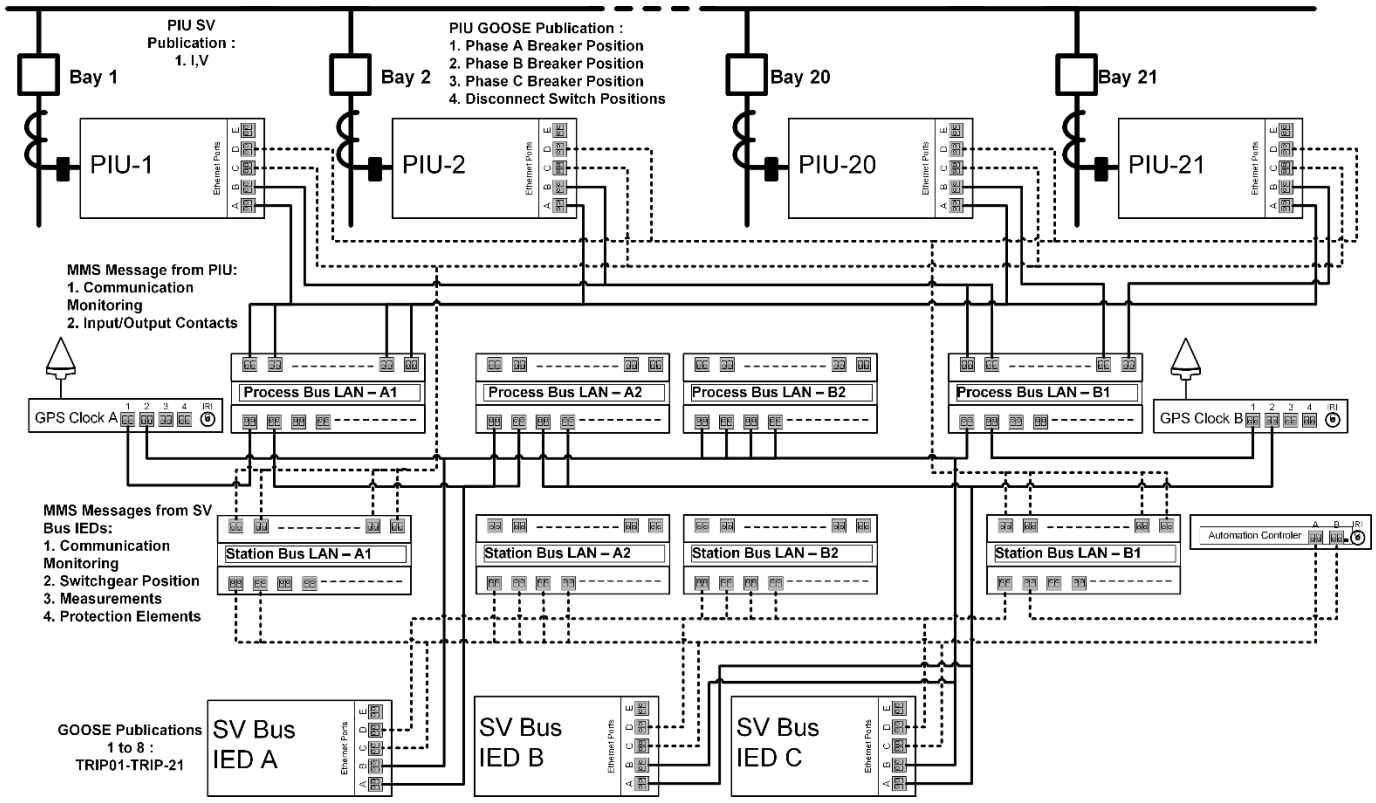

Fig. 4. Network architecture for process and station bus for a phase-segregated busbar differential protection.

The process bus and station bus exhibit dual networks: LAN A and LAN B in a PRP-compliant network. This ensures that if one of the networks, e.g. LAN A, is subject to packet loss, critical traffic will still reach the target IED from LAN B and vice versa.

The station bus carries disconnect statuses, breaker statuses, supervision information for GOOSE messaging, supervision information for SV, and time synchronization information for supervisory control and data acquisition (SCADA) monitoring from the PIU and IEDs to the automation controller. The station bus uses IEC 61850-based Manufacturing Message Specification (MMS) protocol to transmit these messages from PIUs and IEDs to the automation controller.

E. Real-Time Simulation Setup

The laboratory setup consisted of a RT-HIL simulation platform interfaced with 21 PIUs and three bus protection IEDs to validate the IEC 61850-based distributed busbar protection system under realistic operating conditions. The simulated power system corresponds to the 21-bay substation shown in Fig. 2. Primary components, including circuit breakers, disconnectors, current transformers, bus sections, and fault locations, were modeled in the real-time simulator.

The PIUs and protection IEDs were connected using the process bus and station bus architecture described in Section II.D. The interface between the real-time simulator and the DSS was implemented using a combination of analog, hardwired digital, and IEC 61850 communications signals. Currents for all 21 terminals were generated by the real-time simulator and applied to the PIU current inputs through low-level analog output interfaces.

Breaker statuses and control signals were exchanged between the real-time simulator and the PIUs using hardwired connections. This arrangement allowed the simulator to emulate breaker opening and closing operations while receiving trip commands issued by the protective IEDs through the PIUs. Disconnector status signals, which are required for dynamic zone selection, were transmitted from the real-time simulator to the PIUs using GOOSE messaging and then forwarded from the PIUs to the protective IEDs. In a field installation, these disconnector positions would typically be hardwired directly to the PIUs.

The simulation model included configurable fault and switching conditions to support repeatable testing of the protection system. Fault simulation capabilities included fault location, fault type, fault resistance, point-on-wave initiation, and evolving fault scenarios. Circuit breaker operation was modeled to interrupt at current zero crossing, representing practical interruption behavior. In addition, control logic was implemented in the simulator to operate disconnectors and sectionalizers, enabling dynamic reconfiguration of protection zones under the conditions described in Section II.B.

This setup provides a controlled environment for evaluating the interaction between power system behavior, communications network performance, and protection logic. It enables measurement of SV communications performance, PDV, SV channel delay behavior, and busbar fault detection time under steady-state and transient conditions. The validation results obtained from this setup are presented in Section V.

III. Network Traffic Modeling and Dimensioning

Communications networks in IEC 61850-based digital substations must be engineered to support high volumes of time-critical multicast traffic while maintaining predictable timing behavior. In distributed busbar protection systems, the process bus carries continuous SV streams together with GOOSE messaging over shared Ethernet infrastructure. Under such conditions, network behavior is governed by the interaction between traffic characteristics, bandwidth utilization, and delay mechanisms along communications paths.

SV traffic originating from multiple PIUs increases loading across network segments, directly influencing queuing behavior and delay variability. Therefore, evaluating system performance requires a structured approach that links traffic generation and network loading, and results in delay analysis. Accordingly, this section develops a consistent analytical framework connecting these factors to protection operation speed. Section III.A establishes the timing model and key performance parameters, Section III.B quantifies the traffic inventory and bandwidth distribution for the studied system, and Section III.C evaluates PDV and derives the resulting SV channel delay setting values that will be observed at the protective IEDs.

A. Process Bus Timing and Performance Criteria

In IEC 61850 process bus networks, communications performance is determined by device processing behavior, frame transmission characteristics, and network loading conditions. The total delay experienced by an Ethernet frame at a network node can be expressed as (2):

$$d_{total} = d_{proc} + d_{queue} + d_{trans} + d_{prop} \quad (2)$$

where:

d_{proc} represents processing delay.

d_{queue} represents queuing delay.

d_{trans} represents transmission delay.

d_{prop} represents propagation delay. [7] [16]

In substation environments, propagation delays are negligible due to short communications distances. Consequently, processing, transmission and queuing delays dominate overall network behavior. Transmission delay depends on frame size and link speed and can be expressed as (3):

$$d_{trans} = \frac{L}{R} \quad (3)$$

where:

L is the frame length in bits.

R is the link transmission rate.

Network loading is characterized by using traffic intensity, (4):

$$\rho = \frac{L \bullet a}{R} \quad (4)$$

where a is the packet arrival rate, and ρ is the traffic intensity. As traffic intensity approaches unity, queuing delays increase rapidly, resulting in higher variability in frame delivery.

The end-to-end delay along a communications path is given by (5):

$$d_{end\text{-}to\text{-}end} = \sum_{i=1}^{N} \left(d_{proc,i} + d_{queue,i} + d_{trans,i} + d_{prop,i} \right) \quad (5)$$

where N represents the number of nodes along the communications path [13]. Among these components, queuing delay is the dominant variable term and is directly influenced by traffic intensity.

The achievable throughput along a communications path is limited by the slowest link and can be expressed as (6):

$$\text{Throughput} = \min(R_1, R_2, \ldots, R_N) \quad (6)$$

where $R_1, R_2, \ldots, R_N$ represent the transmission rates of the individual links forming the communications path between the PIUs and the protective IEDs. The minimum of these link rates defines the bottleneck that constrains the overall data transfer capability.

In process bus applications, SV frames are transmitted continuously without retransmission. Any delay or loss is compensated for by interpolation; however, excessive delay may lead to data invalidity or blocking of protection elements. Therefore, network performance must be evaluated under worst-case loading conditions, particularly when traffic intensity approaches the limits of the available bandwidth.

The relationships presented previously show that queuing delay and throughput limitations are directly governed by traffic intensity and link capacity. However, these parameters depend on the actual traffic generated within the system and how it is distributed across the network. Consequently, a detailed evaluation of traffic inventory and bandwidth utilization is required.

B. Traffic Inventory and Bandwidth Analysis

Process bus dimensioning requires a detailed characterization of traffic sources and their impact on bandwidth utilization across the network. The four major traffic sources in any DSS network are SVs, GOOSE messages, PTP time synchronization traffic, and PRP supervision frames for redundancy monitoring. Table I summarizes the traffic inventory created by these four sources for the 21-bay system under analysis in both engineered and unengineered networks. An engineered switch applies traffic control mechanisms, such as virtual local-area network (VLAN) segmentation and multicast filtering, to ensure that only required messages are forwarded to intended subscribers, thereby reducing network loading and improving timing consistency. Whereas an unengineered switch forwards multicast traffic broadly across the network, leading to unnecessary congestion, higher PDV, and reduced communications performance [12].

TABLE I
PROCESS BUS TRAFFIC INVENTORY FOR THE 21-BAY SYSTEM COMPARING ENGINEERED AND UNENGINEERED SWITCHES

Message type	Number of control blocks/messages	Total number of messages in the process bus network	Total number of messages on each PIU port (ingress and egress traffic) with engineered switch	Total number of messages on SV bus IED port (ingress and egress traffic) with engineered switch	Total number of messages on each PIU and SV bus IED port (ingress and egress traffic) with unengineered switch
SV per PIU	1	21	1	21	21
GOOSE from PIU: breaker positions	3	63	3	21	63
GOOSE from PIU: disconnect positions	1	21	1	21	21
GOOSE per SV Bus IED: trip	8	24	3	8	24
PTP from PIU, IED, and Ethernet switch[1]	3	72	3	3	3
PTP from GPS clock[2]	3	3	3	3	3
PRP supervision frames	1	28	28	28	28

[1] The type of PTP messages considered here are: Peer delay request, Peer delay response, and Peer delay response follow up messages.
[2] The type of PTP messages considered here are: Sync, Announce, and Follow up messages.

Table II provides a theoretical quantification of the network inventory in terms of the traffic bandwidth present on each port of the engineered and unengineered network (since multicast traffic is routed on all ports by the switch). The bandwidth calculation in Table II excludes the 12 bytes of interframe gap (IFG), consistent with the device used to measure the bandwidth in the subsequent analysis, which excludes the IFG bytes from each packet. However, for network design and theoretical bandwidth estimation, this additional 12 bytes per packet must be considered because the IFG contributes to the total bandwidth occupied on the Ethernet link.

As SV forms the largest component of bandwidth, changing SV configurations can have considerable impact on system bandwidth because these configurations differ in data set structure, number of samples per frame, and frame size, which directly influence bandwidth utilization, transmission delay, and overall network loading. Hence three SV configurations according to IEC 61869-9 profile and 4,800 Hz sampling rate are analyzed in detail in this section as it is the preferred choice for protection applications supporting both 50 and 60 Hz power system frequencies.

The notation F4800S1I3U3 corresponds to a single ASDU per frame configuration, while F4800S2I3U3 corresponds to two ASDUs per frame [17]. In addition, the F4800S1I4U4 profile represents the widely adopted IEC 61850-9-2 LE implementation for 60 Hz system aligned with IEC 61869-9 [18]. Although typical bus protection does not require voltage signals, SV profiles including voltages are also used since the same streams are shared with feeder protection, which requires both current and voltage measurements.

Table II shows a significant difference in the bandwidth observed at the PIU port for the engineered and unengineered switch configurations. In the engineered switch configuration, the PIU port carries only the required ingress and egress traffic. As a result, the bandwidth consumption at the PIU port remains relatively low. In contrast, the PIU port on the unengineered switch also receives SV bus IED traffic. Therefore, the PIU port bandwidth exceeds 100 Mbps for several SV configurations. Consequently, a 1,000 Mbps Ethernet port should be selected for the PIU connection when an unengineered switch is used. However, a 100 Mbps port is sufficient for the PIU connection in the engineered switch configuration.

Table II also shows the bandwidth impact at the SV bus IED port. For a sampling rate of 4,800 Hz, the one ASDU SV configuration results in approximately 106 Mbits/s, while the two ASDU configuration results in approximately 86 Mbits/s. This indicates that SV traffic alone can approach the practical capacity of a 100 Mbits/s link. Therefore, limited margin remains at the SV bus IED port for additional GOOSE and PRP traffic generated during system events, including protection trip signals and changes in breaker or disconnect switch positions.

TABLE II
PER-STREAM AND PER-PORT BANDWIDTH CONTRIBUTION DURING STEADY STATE (EXCLUDES 12 BYTES OF IFG FROM EACH PACKET)[4]

Message type	Data size of each packet in bytes	Total frames/s	Consumed bandwidth by one message in Mbits/s	Consumed bandwidth in Mbits/s on each SV bus IED port (ingress and egress traffic)[5] with engineered switch	Consumed bandwidth in Mbits/s on each PIU port (ingress and egress traffic)[5] with engineered switch	Consumed bandwidth in Mbits/s on each PIU and SV bus IED port (ingress and egress traffic)[5] with unengineered switch
SV- F4800S1I3U3	132[1, 2, 4]	4,800	5.0688	106.4480	5.0688	106.4480
SV- F4800S1I4U4	138[1, 4]	4,800	5.2992	111.2830	5.2992	111.2830
SV- F4800S2I3U3	215[1, 2, 4]	2,400	4.1280	86.6880	4.1280	86.6880
SV- F4800S1I3	108[1, 2, 4]	4,800	4.1472	87.0910	4.1472	87.0910
SV- F4800S2I3	165[1, 2, 4]	2,400	3.1680	66.5280	3.1680	66.5280
GOOSE from SV bus IED: Trip[3]	224[4]	1	0.001792	0.01430	0.0053	0.0430
GOOSE from PIU: disconnect positions[3]	254[4]	1	0.0020	0.0420	0.0020	0.0420
GOOSE from PIU: breaker positions[3]	165[4]	1	0.0013	0.0277	0.0039	0.0831
PRP supervision frame	82[4]	1	0.0006	0.0170	0.0170	0.0170

[1]SvID of 4 bytes.
[2]Includes Grand Master Identity field as well.
[3]GOOSE messages were configured for the application discussed in Section II.
[4]Includes PRP Trailer, Cyclic Redundancy Check (CRC), VLAN ID fields, Preamble and Start Frame Delimiter. This table excludes the 12 bytes of IFG from each packet.
[5]Numbers of stream taken from Table I

Table III summarizes the aggregated steady-state bandwidth requirements of the system. The results show that, under steady-state conditions, the shared communications paths require a link capacity of 1,000 Mbits/s for 1 ASDU and IEC 61850 9-2 LE traffic, and 100 Mbits/s for 2 ASDU traffic. The traffic inventory and bandwidth calculations presented in Table I, Table II, and Table III represent the intended application. If simulation devices are introduced to inject additional SV or GOOSE messages, the resulting traffic and associated bandwidth requirements should be considered separately and incorporated into the overall bandwidth assessment.

Fig. 5, Fig. 6, Fig. 7, and Fig. 8 present the total network bandwidth measured on the SV bus IED port for various SV profiles. Since the measurement device excludes the IFG bytes from each packet, as noted previously, the bandwidth values reported in these figures exclude the IFG contribution.

Fig. 5 and Fig. 6 illustrate the measured bandwidth under steady-state and fault conditions for the evaluated SV configurations. The measured bandwidth results confirm the analytical calculations and demonstrate that occurrence of system events leads to a temporary increase in traffic, contributing to queue buildup at network nodes. Fig. 5 and Fig. 6 also illustrate the bandwidth difference between an engineered and unengineered configuration.

TABLE III
TOTAL STEADY-STATE BANDWIDTH REQUIREMENTS

Operational parameters	F4800S1I3U3	F4800S2I3U3	F4800S1I4U4
Required bandwidth for SV messages in Mbits/s	106.448	86.688	111.283
Total required bandwidth for SV bus IED port for engineered switch in Mbits/s	106.575	86.800	111.410
Total required bandwidth for SV bus IED port for unengineered switch in Mbits/s	106.619	86.920	111.522

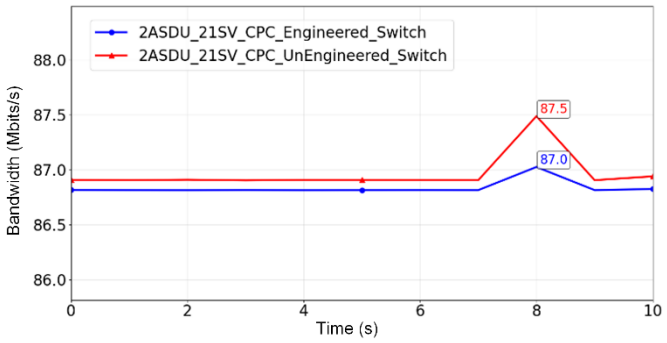

Fig. 5. Comparison between engineered and unengineered switch for F4800S2I3U3 (2ASDU).

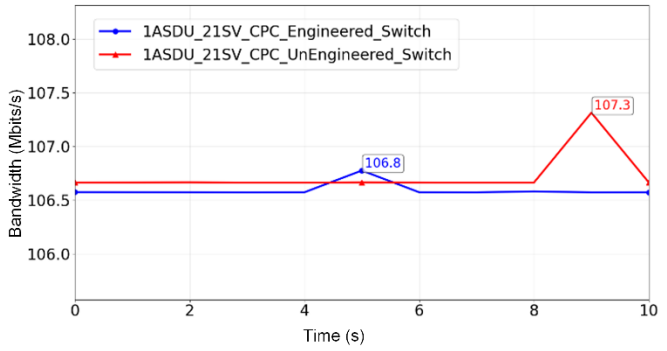

Fig. 6. Comparison between engineered and unengineered switch for F4800S1I3U3 (1ASDU).

Fig. 7 compares configurations with 21 and 42 SV streams, corresponding to shared and function-dedicated SV transmission approaches, respectively. In the shared configuration, a single SV stream per bay is utilized by multiple protective devices, whereas in the function-dedicated configuration, separate SV streams are published for individual protection applications, resulting in duplication of measurement data across the network.

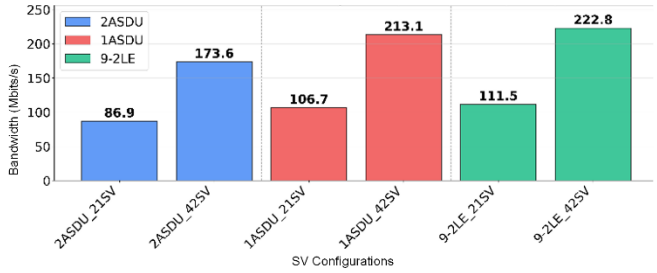

Fig. 7. Data bandwidth measured on network for F4800S2I3U3 (2ASDU), F4800S1I3U3 (1ASDU), and F4800S1I4 (9-2 LE) SV configuration.

As shown in Fig. 7, increasing the number of SV streams increases the total network traffic, leading to higher loading of shared communications paths, such as trunk links and switch fabrics. This increase in traffic raises traffic intensity and contributes to increased queuing delay in heavily loaded portions of the network. However, the bandwidth observed at the protective IEDs remains largely unchanged, since multicast filtering ensures that only the required signals are received. This distinction highlights the importance of evaluating both system-level traffic distribution and subscriber-level bandwidth.

Fig. 8 compares SV bandwidth for different data set configurations in a 21-bay application. Each case includes 21 SV streams for busbar protection and 21 SV streams for bay protection. In SV Configurations I and III, the busbar protection streams include only current measurements, while the bay protection streams include current and voltage measurements. Configurations II, IV, and V include current and voltage measurements for both busbar and bay protection. Configuration E corresponds to the IEC 61850-9-2 LE fixed data set configuration and includes neutral current and neutral voltage channels for both protection functions, resulting in the highest bandwidth.

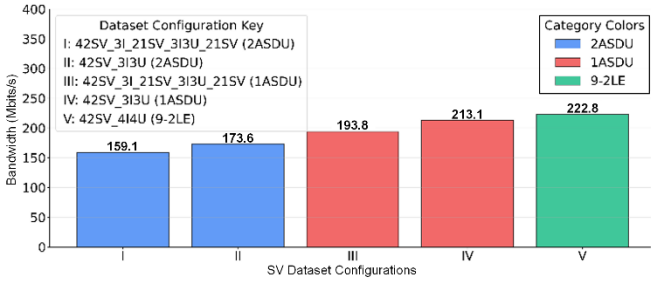

Fig. 8. Data set flexibility for selective signal transmission with IEC 61869-9.

By limiting the data set to only the necessary measurements, SV frame size and corresponding bandwidth utilization are reduced. This reduction directly decreases transmission delay and contributes to lowering overall traffic intensity within the network.

As illustrated in Fig. 9, data set aggregation reduces the number of transmitted frames, improving bandwidth efficiency and lowering overall traffic intensity. However, the increase in frame size results in longer transmission durations, which can contribute to higher queuing delays under heavily loaded conditions. These results illustrate the tradeoff between bandwidth optimization and delay performance.

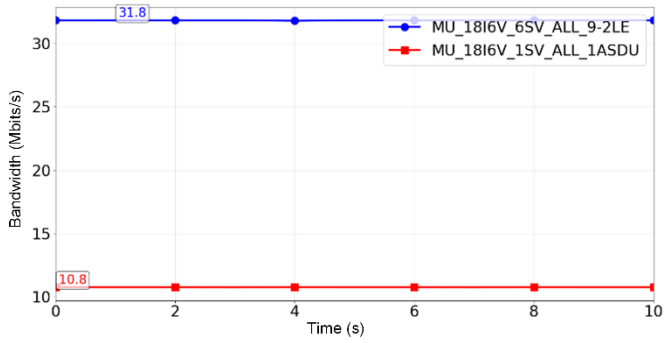

Fig. 9. Impact of data set aggregation on bandwidth with IEC 61869-9.

This bandwidth analysis quantifies how traffic distribution and configuration choices affect network loading and link utilization. As established in Section III.A, increased traffic intensity leads to higher queuing delay and variability in frame delivery. Therefore, it is necessary to evaluate how these loading conditions translate into PDV and how this variability impacts the effective delay experienced by the protection function.

C. PDV and SV Channel Delay

PDV represents the variation in arrival times of Ethernet frames due to queuing and contention [7]. It can be estimated as (7):

$$PDV = N \bullet \left(\frac{L \bullet 8}{R}\right) \bullet 10^6 \quad (7)$$

where:

PDV is the packet delay variation in microseconds.
N is the number of interfering frames.
L is the frame size in bytes.
R is the link transmission rate in Mbits/s.

Table IV shows that for a 100 Mbits/s network, PDV reaches approximately 704 µs for the engineered network and 1,557 µs for the unengineered network. Increasing link speed to 1,000 Mbps reduces these values to approximately 70 µs and 156 µs, respectively. These results confirm that both link speed and traffic engineering significantly influence delay variability.

TABLE IV
WORST-CASE PDV FOR ENGINEERED AND UNENGINEERED CONFIGURATIONS

Network Type	Traffic Composition	PDV (µs) at 100 Mbits/s	PDV (µs) at 1,000 Mbits/s
Engineered	21A[1] + 21B[1]	704	70
Unengineered	63A[1] + 21B[1]	1,557	156

[1] A is 254 Bytes and B is 165 Bytes

Fig. 10 shows the timing path for analog data in a digital secondary system. The figure separates the delay introduced by the merging unit, the communications network, and the subscriber device [7] [8]. This breakdown is important because the SV protective IED does not operate on instantaneous analog quantities; instead, it operates on sampled data that has been processed at the source, transmitted over the Ethernet network, and aligned at the SV protection IED.

By explicitly distinguishing these stages, Fig. 10 provides a clear representation of how individual delay components contribute to the overall timing performance of the system. It therefore serves as the conceptual basis for the SV channel delay formulation used in this subsection.

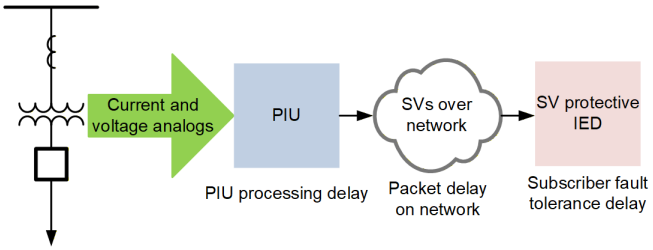

Fig. 10. Analog signal delays in a DSS.

Therefore, the effective delay experienced by the protection IEDs includes PIU processing delay, network-induced delay variation, and subscriber tolerance as shown in equation (8).

$$T_{delay} = T_{PIU} + T_{PDV} + T_{SFT} \quad (8)$$

where:

T_{delay} represents the total SV channel delay.
T_{PIU} is the PIU processing delay.
T_{PDV} denotes the PDV.
T_{SFT} corresponds to the subscriber fault tolerance delay and is a configurable packet loss ride-through value.

Table V shows that the lowest delay occurs with a 1,000 Mbits/s engineered network using one ASDU configuration, resulting in approximately 0.989 ms, while the highest delay occurs with a 100 Mbits/s unengineered network using two ASDU configuration, resulting in approximately 2.806 ms. The PIU processing delay and the subscriber fault tolerance delay vary based on manufacturer-specific implementation. In this example, the PIU processing delay is approximately 625 µs for one ASDU and 833.33 µs for two ASDU, while the subscriber tolerance delay is 208 µs and 416 µs, respectively. These results demonstrate that although the two ASDU configuration reduces bandwidth, it increases the total delay due to higher processing and tolerance requirements.

TABLE V
CALCULATED SV CHANNEL DELAY FOR DIFFERENT LINK SPEEDS, SV CONFIGURATIONS, AND ENGINEERING CONDITIONS

Link speed (Mbits/s)	100	100	1,000	1,000	100	100	1,000	1,000
Network configuration	Eng	Eng	Eng	Eng	Uneng	Uneng	Uneng	Uneng
Number of ASDU	2	1	2	1	2	1	2	1
Average PIU delay (µs)	833.33	625	833.33	625	833.33	625	833.33	625
Worst-case PDV (µs)	704	704	70	70	1,557	1,557	156	156
SV sample fault tolerance delay (µs)	416	208	416	208	416	208	416	208
SV channel delay (ms)	1.953	1.537	1.319	0.903	2.806	2.39	1.405	0.989

Overall, the results show that SV channel delay is governed by the combined effects of PIU processing delay, PDV, subscriber tolerance, link speed, multicast forwarding, and SV configuration. The two ASDU profile reduces bandwidth utilization but increases processing and tolerance delay, while higher link speed reduces the PDV contribution. Therefore, SV channel delay should be selected using the SV profile and the worst-case network delay margin.

These results also show that PDV should be considered during process bus design rather than only during validation. Accurate traffic inventory, appropriate link capacity, controlled multicast forwarding, and sufficient margin between offered load and link capacity are required to maintain deterministic performance. The bandwidth and delay analyses presented in this section provide the basis for the system-level network implementation discussed in the following section.

IV. System-Level Network Configuration

After the process bus traffic and timing requirements are established, the next step is to translate those requirements into a repeatable system-level network configuration. For a large IEC 61850-based busbar protection scheme, this analysis requires more than configuring individual devices. The network configuration must consistently implement the intended data flows, VLAN and multicast filtering rules, traffic priorities, redundancy paths, monitoring points, and traffic-limiting policies across all switches and IEDs.

To move a project from design to deployment, three main engineering inputs are required: the network architecture, the logical architecture, and the IEC 61850 System Configuration Description (SCD) file. The network architecture defines all hosts in the network and the physical topology of their interconnections. The logical architecture, referred to in this paper as the data flow diagram, defines how applications interact across hosts to achieve protection, control, automation, monitoring, and supervision objectives. The SCD file defines the IEC 61850 communications relationships, including GOOSE, SV, and MMS communications between publishers and subscribers.

Together, these files provide the information required to move from a device-by-device configuration process to a repeatable system-level configuration process. This is important for large DSSs because manual configuration of each switch port, VLAN, multicast rule, priority setting, and traffic control policy is time consuming and increases the risk of inconsistent settings. A system-level workflow reduces manual effort, supports offline preparation before factory acceptance testing (FAT), and provides a basis for site acceptance testing (SAT) verification.

A. Automated Configuration From Design Files

In a device-level configuration approach, the aforementioned files serve as references for generating individual configuration files for each network device. For example, the SCD file is used to retrieve the IEEE 802.1Q VLAN identifiers, which are then applied to configure VLAN-based traffic control on each switch.

In a system-level configuration approach, switches are centrally configured through a network management system (NMS). The NMS utilizes the design files as input to automatically generate configuration settings for network devices, as illustrated in Fig. 11 [19].

This centralized automatic configuration helps improve configuration efficiency. Furthermore, the ability to perform it offline, without requiring hardware, also contributes to reducing FAT time. In addition, a SAT report can be generated to guide the commissioning team on what and how to test the network, ensuring that everything operates according to the design.

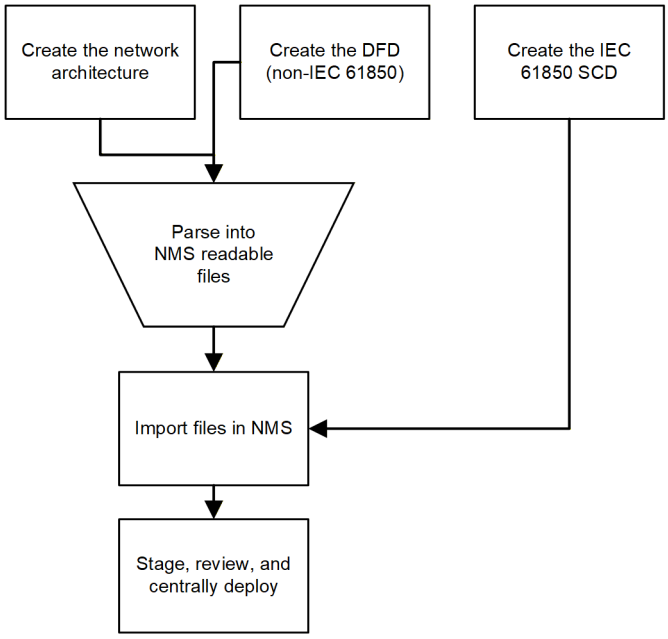

Fig. 11. System-level network configuration workflow.

B. Switch Configuration Best Practices

The analysis in Section III showed that process bus performance depends on traffic intensity, PDV, packet loss, and subscriber SV channel delay. Therefore, switch configurations must do more than provide basic Ethernet connectivity. The switch configuration must enforce the intended data flows, limit unnecessary multicast traffic, preserve priority for time-critical applications, and prevent abnormal traffic from affecting protection communications.

In SDN operation, every application is inherently controlled to ensure forwarding only to the required destinations. Traditional switches can control traffic based on the IEEE 802.1Q tag or multicast media access control (MAC) filters, whereas SDN switches perform traffic control using any field from Open Systems Interconnection (OSI) layers 1 through 4, regardless of whether the message has a VLAN tag or is multicast [20]. This capability also enables the creation of flexible tap destinations for both planned and unplanned traffic, which will be further discussed in Section VI.A.

Furthermore, each application is prioritized and assigned to the appropriate egress queue. Traditional switches prioritize traffic based on the IEEE 802.1Q Priority Code Point (PCP) field at Layer 2 or the Differentiated Services Code Point

(DSCP) field at Layer 3. Similarly to traffic control, SDN allows prioritization based on any field from OSI Layers 1 through 4, regardless of whether the messages include PCP or DSCP fields. Additionally, when parsing the SCD file to automatically configure the IEC 61850 applications, the user can assign by default higher priorities for GOOSE messaging, SV, and MMS individually, reducing configuration time.

These controls are essential but not sufficient on their own to prevent frame loss due to buffer overflow [17]. Therefore, to maximize dependability, every GOOSE and SV stream was baselined, and appropriate per-message traffic throttling was configured in the SDN switches. For instance, Fig. 12 shows two GOOSE messages in a steady state within the system: one sends the breaker status, and the other sends the disconnect statuses from the PIU to the busbar relay (IED). To establish a safe baseline, events must be generated under worst-case conditions, ensuring that a legitimate event is never throttled.

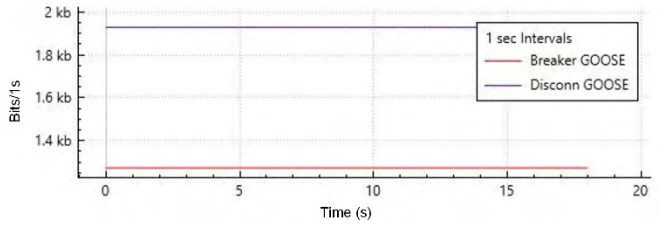

Fig. 12. Steady-state GOOSE messages.

Fig. 13 simulates traffic on the breaker GOOSE message that is higher than the baseline, with no traffic throttling configured on the switches.

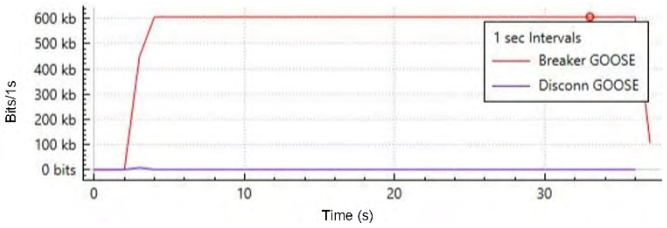

Fig. 13. Breaker GOOSE traffic higher than baseline.

Traditional and SDN switches can throttle traffic; however, traditional switches apply throttling per port, which does not differentiate between message types. In contrast, SDN switches can throttle on a per-message basis. Fig. 14 illustrates an example where a 20-kbps throttle is applied individually to each breaker GOOSE message. The scenario shown in Fig. 14 illustrates that the disconnect GOOSE message is not affected by the throttling, and no events are lost—unlike when using per-port throttling [20].

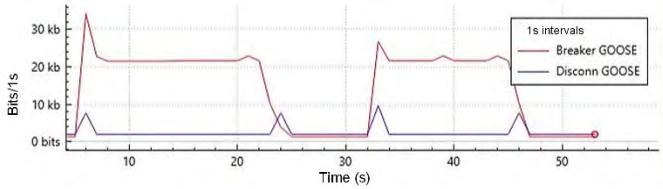

Fig. 14. 20 kbps throttling in breaker GOOSE message.

V. Process Bus Delay and Protection Performance Evaluation

Validation of IEC 61850-based DSS requires consideration of protection behavior, communications performance, time synchronization, and interactions among devices [21] [22]. This section focuses on validating the network performance and delay characteristics developed in Section III using the RT-HIL platform described in Section II.E. The tests evaluate SV packet loss, PDV, and busbar fault detection time under different SV channel delay settings, network configurations, and link speeds.

A. SV Packet Loss

Packet loss occurs when Ethernet frames arrive at a switch or subscriber queue with no available buffer capacity or due to the late arrival of the packets. In an IEC 61850 process bus, SV frames are not retransmitted. Therefore, repeated loss or late arrival of samples can result in data invalidity or protection blocking.

This behavior directly relates to the traffic intensity and delay relationships established in Section III, where increased network loading leads to queuing delay and PDV. The calculated SV channel delay values derived in Section III.C were used to evaluate both correct and incorrect subscriber configurations.

Fig. 15 illustrates the impact of configuring the SV channel delay below the required value. Under this condition, valid SV frames are interpreted as late or missing because the subscriber timing window is smaller than the actual delay present in the process bus. As a result, the relay detects apparent packet loss and blocks the protection function.

The binary elements shown in the upper plot of Fig. 15 provide insight into the behavior of the protection IED during SV packet loss. The *I_BLKD* bit indicates that the current measurement input is blocked from being used in protection calculations due to invalid or missing data. The *PR_BLKD* bit indicates that the protection function itself is blocked as a consequence of invalid or unreliable input signals.

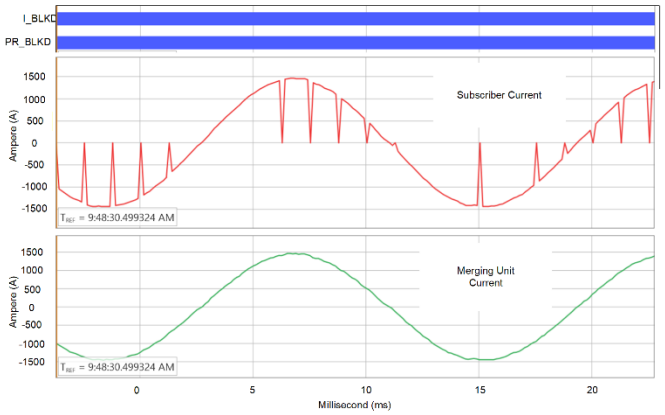

Fig. 15. Incorrect SV channel delay setting resulting in packet loss and protection blocking.

However, when the SV channel delay is configured based on the calculated worst-case delay margin, the SV stream is accepted correctly, without packet loss or blocking. This confirms that the observed behavior is caused by an incorrectly configured SV channel delay that does not account for the total communication delay in the system. It therefore supports the analysis presented in Section III.C, where the SV channel delay must be determined based on the combined effects of PIU processing delay, PDV, and subscriber tolerance to ensure correct operation.

B. PDV

The PDV analysis in Table V calculated the maximum packet delay based on the amount of configured traffic; however, under actual circumstances, the calculated value will exhibit some variability, depending on traffic intensity, link speed and network engineering. This relationship is validated through measured PDV under different network configurations and operating conditions in this section.

Fig. 16 shows the PDV behavior for an unengineered 100 Mbits/s network. The upper plot in Fig. 16 shows the current during both steady-state and fault conditions, while the lower plot presents the measured delay for SV streams SV_01 and SV_07, published from PIU1 and PIU7, respectively. Fig. 16 shows that the measured delay values for the two streams differ. This difference arises because PIU1 and PIU7 are connected to different Ethernet switches, leading to variations in the communications paths and resulting in different delay characteristics for each SV stream.

During steady-state operation, the delay remains relatively stable. However, during cyclic GOOSE message transmission, as well as during fault inception and fault clearing events, the measured delay increases significantly. During fault clearing, the PDV reaches approximately 800 µs, which aligns with the high PDV values predicted in Table IV.

The increase in delay is primarily caused by the transmission of multiple GOOSE messages during breaker opening, which increases the instantaneous traffic load on the network. This rise in traffic intensity leads to queue buildup at switch egress ports, resulting in increased delay variation. These observations confirm that uncontrolled traffic distribution and insufficient bandwidth selection can directly degrade timing performance, particularly during event triggers.

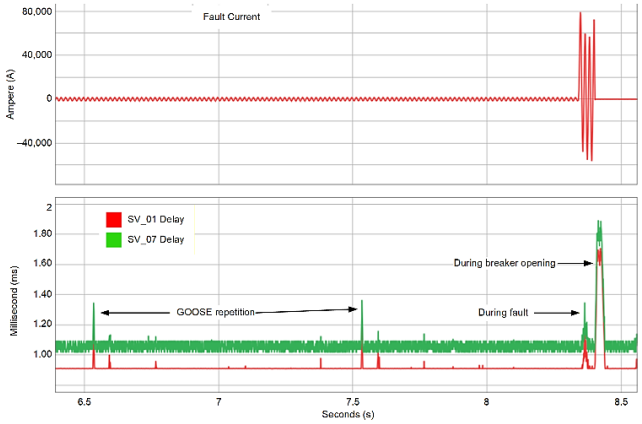

Fig. 16. PDV for unengineered 100 Mbits/s network (2 ASDU).

This behavior provides experimental validation of the relationship between traffic intensity, queuing delay, and PDV established in Section III.

Fig. 17 shows the PDV for the same network after applying traffic engineering. In this configuration, only the required traffic is forwarded to the corresponding subscriber, reducing unnecessary load on switch ports. As a result, the increase in PDV during fault inception and fault clearing events is lower and more controlled compared to the unengineered case.

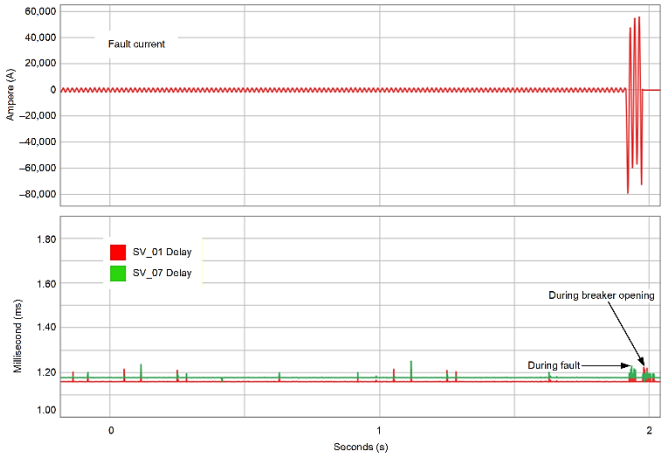

Fig. 17. PDV for engineered 100 Mbits/s network (2 ASDU).

This improvement demonstrates that traffic engineering reduces queue occupancy and improves determinism, directly validating the bandwidth and traffic distribution analysis presented in Section III.B. However, it can also be observed that the PDV still increases significantly during breaker opening events. This increase indicates that, despite proper traffic engineering, the 100 Mbits/s link capacity remains a limiting factor under event triggers, where multiple GOOSE messages are transmitted simultaneously.

Therefore, while traffic engineering mitigates unnecessary congestion, the available link bandwidth ultimately governs the achievable timing margin. This observation confirms that both traffic control and link speed must be considered together to achieve deterministic communication performance, as established in Section III.

Fig. 18 shows the PDV after increasing the process bus link speed to 1,000 Mbits/s while maintaining engineered traffic forwarding. In this configuration, both traffic distribution and link capacity are optimized. The measured PDV reduces significantly, remaining close to approximately 20 µs even during fault inception and fault clearing events.

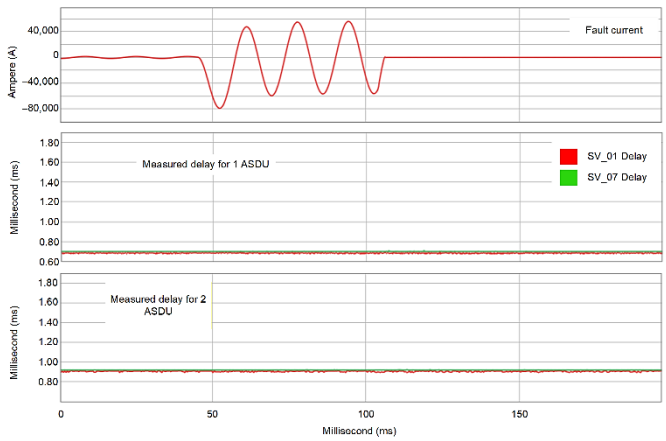

Fig. 18. PDV for engineered 1,000 Mbits/s network.

This reduction confirms that increasing link speed substantially limits queue buildup during increased traffic conditions, such as the transmission of multiple GOOSE messages during breaker operation. The higher bandwidth reduces frame serialization time and increases the available capacity at switch egress ports, preventing congestion even when traffic temporarily increases.

Compared to the engineered 100 Mbits/s case in Fig. 17, the results show that while traffic engineering alone reduces unnecessary load, it is not sufficient to maintain low delay variation under all operating conditions. By combining traffic engineering with higher link speed, the system achieves consistently low PDV and improved timing determinism across both steady-state and transient conditions.

These results validate the analytical conclusions of Section III by demonstrating that deterministic communications performance requires both controlled traffic distribution and sufficient link capacity, with the engineered 1,000 Mbits/s configuration providing the highest timing margin among the evaluated cases.

C. Busbar Fault Detection Time.

The ultimate objective of process bus communications design is to ensure reliable and fast protection operation. To evaluate this objective, the busbar fault detection time is measured using a RT-HIL platform. The results presented in this subsection are obtained from 50 identical single-phase-to-ground (AG) bolted faults applied in Bus Zone 1, ensuring repeatability and statistical relevance of the observed protection operation speed.

Fig. 19 illustrates the methodology used to measure the busbar fault detection time on the SV bus protective IED using the RT-HIL simulator. The fault detection time is measured entirely within the RT-HIL environment. An input is configured on the RT-HIL simulator to monitor the pickup of the busbar protection element in the subscriber relay. The detection time is defined as the time interval between the initiation of the fault in the simulator and the instant at which the corresponding trip signal is received in the RT-HIL system.

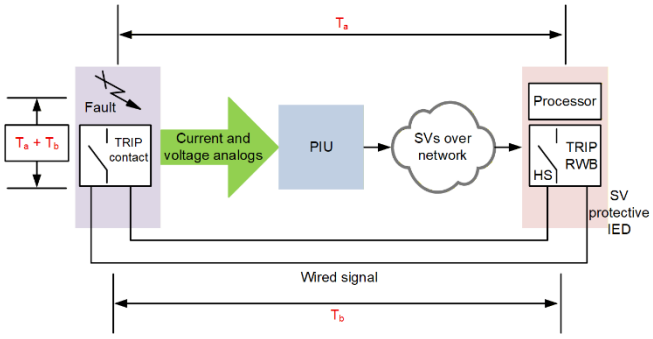

Fig. 19. Fault detection time ($T_a + T_b$) measurement using RT-HIL simulator.

This measurement captures the combined effect of PIU processing delay, network-induced delay, and relay processing, and therefore provides a direct validation of the communications and timing relationships developed in Section III.

Fig. 20 presents the distribution of busbar fault detection time for different SV configurations and SV channel delay settings. The figure shows how the detection time varies as a function of the configured SV channel delay and the selected SV profile. For lower SV channel delay settings, the relay processes SV data earlier, resulting in faster fault detection. However, the margin against delay variation is reduced. As the SV channel delay is increased, the relay waits longer before processing the sampled data, resulting in increased detection time.

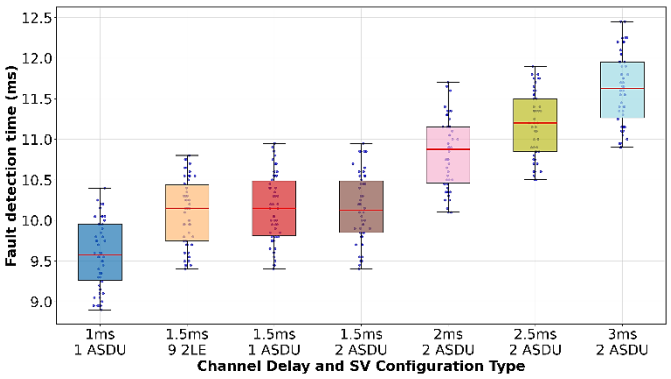

Fig. 20. Impact of SV channel delay and SV configuration on fault detection time.

The spread of values shown in the figure reflects the variability introduced by PDV and processing differences. The results demonstrate that although the variation remains relatively small, the absolute detection time shifts consistently with SV channel delay. This confirms that the SV channel delay parameter acts as a direct offset in the protection operating time.

Table VI summarizes the statistical results for multiple fault simulations performed under different SV configurations and SV channel delay settings. The results show that for an SV channel delay close to 1 ms, the average detection time is approximately 9.58 ms, while increasing the SV channel delay to 3 ms increases the detection time to approximately 11.62 ms.

These results confirm that SV channel delay introduces a direct tradeoff between robustness and speed. A higher SV channel delay improves tolerance to PDV, while a lower SV channel delay improves protection speed but reduces margin against communications variability.

TABLE VI
SV SUBSCRIBER FAULT DETECTION TIME STATISTICS

SV configuration	Link speed in Mbits/s	SV channel delay (ms)	Mean (ms)	Min (ms)	Max (ms)
F4800S1I3U3	1,000	1	9.581	8.9	10.4
F4800S1I4U4	1,000	1.5	10.094	9.4	10.8
F4800S1I3U3	1,000	1.5	10.15	9.4	10.95
F4800S2I3U3	1,000	1.5	10.148	9.4	10.95
F4800S2I3U3	100	2	10.83	10.1	11.7
F4800S2I3U3	100	2.5	11.176	10.5	11.9
F4800S2I3U3	100	3	11.62	10.9	12.45

Overall, the measured fault detection times validate the analytical framework developed in Section III by demonstrating that traffic loading, PDV, link speed, and SV configuration collectively determine the achievable protection operation speed in distributed busbar protection systems.

VI. SYSTEM-LEVEL NETWORK MONITORING

The NMS discussed in Section IV not only provides centralized configuration but also enables centralized network monitoring. Fig. 21 shows the topology view, where the user can visualize the network topology and monitor the statuses of devices and links. Additionally, Ethernet switch path charts can be overlaid on the topology to display the primary and failover paths for each switch in the network.

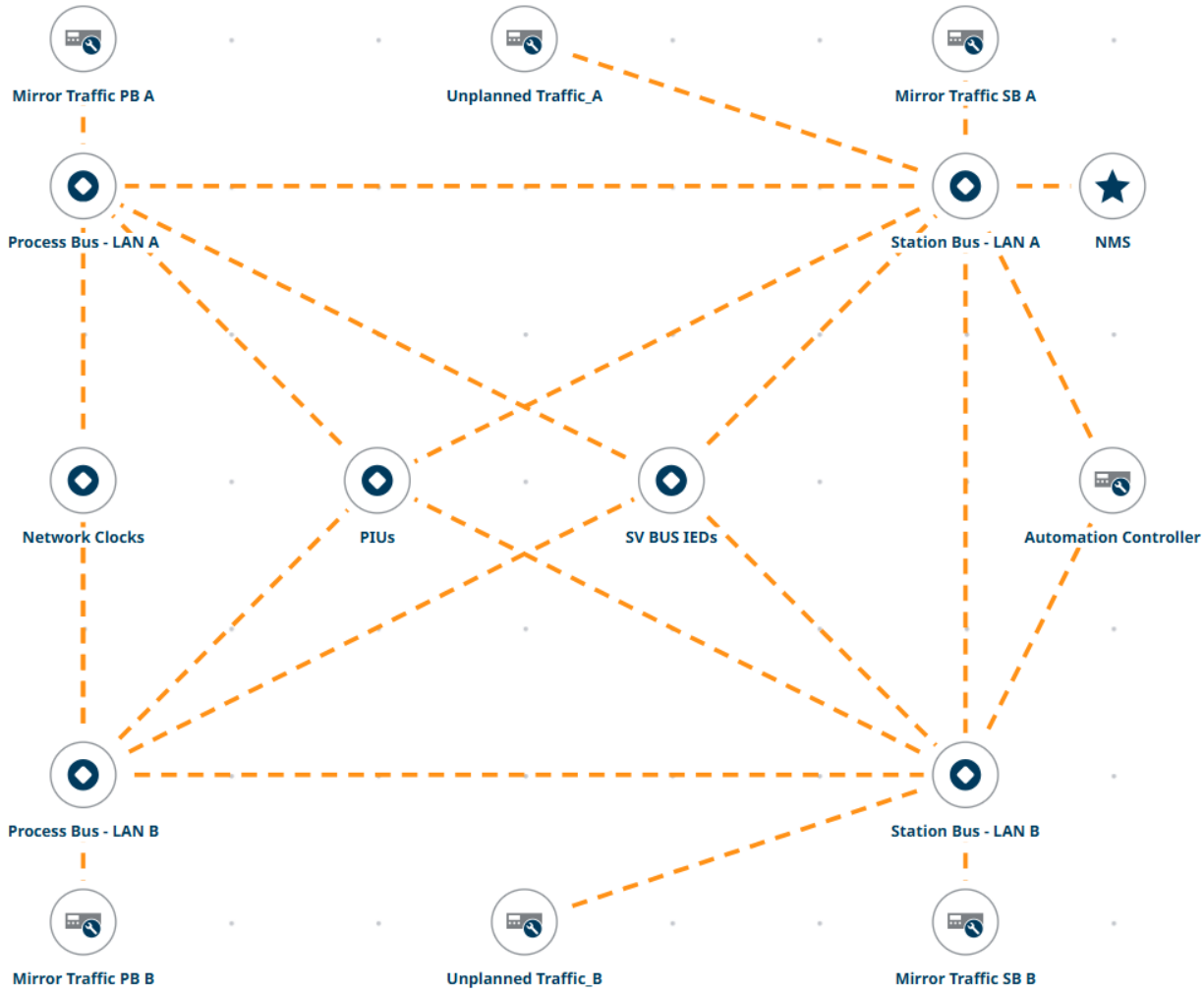

Fig. 21. NMS topology view.

A. *Monitoring Planned and Unplanned Traffic*

The system supports flexible configuration and tagging of traffic taps. For example, in Fig. 22, the tap destination "Mirror Traffic PB A" receives all planned GOOSE, SV, and PTP messages from process bus LAN A. Each traffic tap can be assigned a unique additional VLAN tag, allowing the user to easily identify the network from which the planned traffic originates, as depicted in Fig. 21.

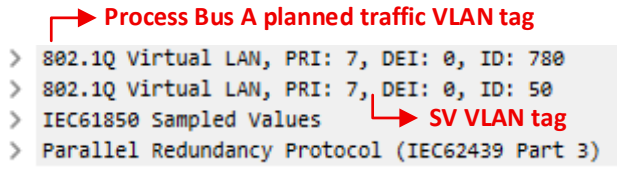

Fig. 22. Planned traffic tagging.

Conversely, in Fig. 23 "Unplanned Traffic_A" captures all unplanned or nonconfigured network traffic from LAN A. Each traffic tap can be tagged with two unique additional VLANs: one to indicate that the traffic is unplanned and another to identify the switch and port from which the traffic originates, as depicted in Fig. 23. These traffic taps facilitate network troubleshooting and strengthen the cybersecurity posture when combined with intrusion detection and prevention systems (IDS/IPS).

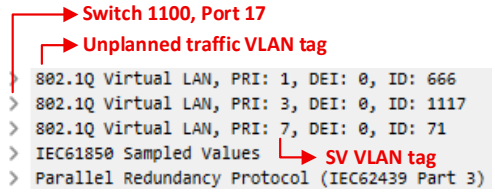

Fig. 23. Unplanned traffic tagging.

B. *DSS System Monitoring*

Effective monitoring should cover not only the network devices and the traffic passing through them but also the end devices [15]. The DSS system monitor provides human-machine interface screens displaying: GOOSE and SV subscriptions and statistics; time synchronization; device operation; process bus, station bus, and engineering access statistics; PRP monitoring; and GOOSE performance. Fig. 24 illustrates the SV subscription and statistics that are being monitored.

SV SUBSCRIPTION | SV_SUB_A_19

Application	Reference	Value	Description
Message Information	SvCBRef.setSrcRef (SP)	MU_19_421_011CFG/LLN0.MSVCB19	Control block reference
	DatSet.setSrcRef (SP)	MU_19_421_011CFG/LLN0.PhsMeas1	Dataset reference
	SvID.setVal (SP)	4001	SV identification
	Addr.setVal (SP)	01-0C-CD-04-00-01	Multicast MAC address
	VlanID.setVal (SP)	19	VLAN identification
	VlanPri.setVal (SP)	7	VLAN priority
	AppID.setVal (SP)	16403	Configured APPID
Reception Status	St.stVal (ST)	TRUE	Reception status
	ErrSt.stVal (ST)	No Errors	Reception error code
	SimSt.stVal (ST)	FALSE	Processed simulation message
	NetwDly.instMag.f	0.625	Network delay (ms)
	SmpSynch.stVal	2: Global Area Clock	Synchronization state for SV stream
	ConfRevNum.stVal (ST)	1	Expected ConfRef
	RxConfRevNum.stVal (ST)	1	Received ConfRef
	NdsCom.stVal (ST)	FALSE	Needs commissioning
Subscription Statistics	TotDwnTm.instMag.f (MX)	0.0	Cumulative inactivity time (s)
	MaxDwnTm.instMag.f (MX)	0.0	Maximum continuous inactivity time (s)
	OosCnt.stVal (ST)	0	Number of messages received out of sequence (OOS)
	DscdCnt.stVal (ST)	0	Number of discarded messages
	IntpCnt.stVal (ST)	0	Number of interpolated messages
	RsStat.t (ST)	2025-10-05-20:43:32.917500	Last reset of stats
	RsStat.Oper.ctVal (CO)	RESET >	Reset reception statistics (commands)

Fig. 24. DSS SV subscriptions monitoring.

VII. Conclusion

This paper presented a framework for engineering and testing IEC 61850-based distributed busbar protection systems. The framework connects process bus traffic modeling, bandwidth utilization, PDV, SV channel delay, system-level configuration, validation, and monitoring.

The results show that protection performance is strongly influenced by SV configuration, link speed, traffic engineering, and SV channel delay. Engineered traffic forwarding reduces unnecessary multicast traffic and improves timing consistency. Increasing process bus link speed to 1,000 Mbits/s reduces queuing effects and improves PDV margin during event-driven GOOSE traffic. SV channel delay must be selected with sufficient margin for PIU processing delay, PDV, and subscriber tolerance, because the setting directly affects both packet acceptance and fault detection time.

Overall, recommendations of the proposed approach are:

- Use adequate SV channel delay to avoid missing packets and compromise protection.
- Use IEC 61869-9 to tailor the SV streams to the application requirements.
- Use 1,000 Mbits/s link to the SV bus IEDs and Ethernet switch backbone uplink ports to speedup data transfer and reduce protection operating time.
- Engineer the network to minimize data traffic according to the application.
- Use SDN switches for centralized network management, network monitoring, and ease of configuration.

These recommendations establish a clear relationship between network design, communications performance, and protection behavior, providing practical guidance for the engineering, configuration, validation, and monitoring of large-scale IEC 61850-based busbar protection systems.

VIII. References

[1] A. Guzmán, C. Labuschagne, and B. L. Qin, "Reliable Busbar and Breaker Failure Protection With Advanced Zone Selection," proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, USA, October 2004.

[2] S. Chase, D. J. Hawaz, J. Pope, and C. Labuschange, "Bus Protection Considerations for Various Bus Types," in 40th Annual Western Protective Relay Conference, Spokane, Washington, 2013.

[3] V. Skendzic, and D. Dolezilek, "News From the Editor – Updates and Enhancements to Process Bus IEC 61850-9-2," in 14th International Conference on Developments in Power System Protection (DPSP 2018), 2018.

[4] Q. Yang and R. Smith, "Improve Protection Communications Network Reliability Through Software-Defined Process Bus," in Power and Energy Automation Conference, Spokane, WA, 2019.

[5] A. Shrestha, M. Silveira, J. Yellajosula, and S. K. Mutha, "Understanding the Impacts of Time Synchronization and Network Issues on Protection in Digital Secondary Systems," in PAC World Global Conference 2021, Virtual Format, August/September, 2021.

[6] S. B. Ladd, T. I. Raffield, A. Shrestha, M. A. Rahmani, and M. Silveira, "Distributed Bus Protection Using Process Bus for a Large Transmission Substation at Duke Energy," in 79th Annual Georgia Tech Protective Relaying Conference, Atlanta, Georgia, April, 2026.

[7] M. Silveira, A. Rash, D. Dolezilek, and A. Shrestha, "Understanding the Impacts of Networks and Parallel Redundancy Protocol for Process Bus Applications," in 17th International Conference on Developments in Power System Protection (DPSP 2024), Manchester, UK, 2024.

[8] M. Silveira, M. A. Rahmani, E. Goncalves, and A. Shrestha, "Optimizing IEC 61850 Sampled Values for Large-Scale Centralized Protection Schemes," in 20th International Conference on Developments in Power System Protection (DPSP 2026), London, UK, 2026.

[9] J. Mendez, I. Otarola, J. Uzcategui, J. Escurra, M. Diaz, and H. Tapia, "Experiences in the Commissioning of IEC 61850 Digital Busbar Protection Systems" in 2023 CIGRE Canada Conference and Exhibition, Vancouver, BC, September 2023.

[10] D. Lellys, P. Flores, A. Dierks, A, Melo, I. Ferrero, R. Goblirsch, M. Mohemmed, R. Toledo, C. Redondo, H. Faramawy, R. Leone, and S. Vijayaraghavan, "Interoperability Tests in a Multivendor Platform of Busbar Protection Using IEC 61850 Process Bus applied by CIGRE Working Group B5.74," in CIGRE SC B5 2025 Osaka Colloquium, Osaka, Japan, June/July, 2025.

[11] L. Xu, H. Li, L. Chen, C. Patterson, and P. Mohapatra, "Assessment and Analysis of Different Process Bus Redundancy Networks Performance for IEC 61850-Based Digital Substation," in 14th International Conference on Developments in Power System Protection (DPSP 2018), 2018.

[12] IEC TR 61850-90-4, *Communication Networks and Systems for Power Utility Automation* - Part 90-4: Network Engineering Guidelines," Edition 2.0, May 2020.

[13] IEC 62439-3, *Industrial Communication Networks – High Availability Automation Networks* – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), 2021.

[14] G. S. Antonova, S. Paduraru, H. Faramawy, and J. Groat, "Engineering Challenges in Digital Substations," in 79th Annual Georgia Tech Protective Relaying Conference, Atlanta, Georgia, April 2026.

[15] A. Kotryk, E. Goncalves, R. Abboud, M. Silveira, P. Lima, and V. Ferrari, "Complete Monitoring Solution to Improve Reliability and Performance of Digital Secondary Systems," in Protection, Automation and Control World Conference, 2023.

[16] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed., Pearson, 2017.

[17] IEC 61869-9:2016, *Instrument Transformers* - Part 9: Digital Interface for Instrument Transformers, 2016.

[18] 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, 2020.

[19] W. Roberto, E. Goncalves, P. Lima, T. Bordim, and D. Dolezilek, "How to Successfully Isolate and Shield In-Service Communications-Assisted Protection From Ethernet Packet Storms," in 78th Annual Conference for Protective Relay Engineers at Texas A&M, Texas, 2025.

[20] Schweitzer Engineering Laboratories, Inc., "SEL-5056 Network Management System Instruction Manual," 2026.

[21] J. Mathew, J., D. Dolezilek, M. Katuru, and R. Karmaker, "Lessons Learned from Commissioning of IEC 61850-9-2 Process Bus-Based Busbar Protection System," in 16th International Conference on Developments in Power System Protection (DPSP 2022), 2022.

[22] S. Chase, E. Jessup, M. Silveira, J. Dong, and Q. Yang, "Protection and Testing Considerations for IEC 61850 Sampled Values-Based Distance and Line Current Differential Schemes" in 72nd Annual Conference for Protective Relay Engineers at Texas A&M, College Station, Texas, March, 2019.

IX. Biographies

Md Aamir Rahmani holds a Diploma in electrical engineering from Jamia Millia Islamia in 2008, India, BS in electronics and instrumentation engineering from Uttar Pradesh Technical University in 2011, India, and MS and PhD in electrical engineering from Michigan Technological University in 2021 and 2024, respectively. He joined SEL in May 2024 where he is a development lead engineer with the protection systems department in R&D. Aamir began his career in the power industry as a project engineer with Schneider Electric in 2011, where he specialized in substation automation systems and has since gained 15 years of experience in various roles across industry and academia. He is a member of IEEE and IEEE PSRC and has authored 5 technical papers.

Wesley Roberto received his bachelor's degree in automation and control engineering from the Federal University of Itajubá in 2020. He was certified as a Global Industrial Cyber Security Professional by GIAC in 2023. He has worked at Schweitzer Engineering Laboratories, Inc. (SEL), in Brazil since 2019 as an automation application engineer. He develops technical applications for power system automation and is an instructor at SEL University.

Ali Khan, MS. currently works as an integration and automation engineer at Schweitzer Engineering Laboratories, Inc. (SEL), where he is involved in developing and testing robust communications systems and investigating their emerging applications in digital protection, automation and control for the SEL leading 4xx product line. He received his MS in electrical engineering from Washington State University and BE from National University of Sciences and Technology, Islamabad. He is the recipient of the prestigious IEEE Outstanding Graduate Student award of 2022.

Mauricio Gadelha da Silveira is an electrical engineer who earned his Bachelor of Science degree from São Paulo State University in 2013. He joined Schweitzer Engineering Laboratories, Inc. (SEL), in 2014 and has since held roles in engineering services, sales and customer services, and research and development (R&D). He is currently a senior engineer in R&D. His work focuses on the development of protective relay protocols and communications, network design for critical infrastructure, power system modeling, and cybersecurity assessment. He is a U.S. TAG member of IEC TC 57 WG 10 and IEC TC 38 WG 37.

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 principal engineer. His research areas of interest include power system protection and control design, real-time power system modeling and simulation, 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 of IEC 61850 TC 57 WG 10. He has authored 21 technical papers and holds 7 U.S. patents.