Lessons Learned From Commissioning of IEC 61850-9-2 Process Bus-Based Busbar Protection System

Jerin Monzi Mathew, David Dolezilek, and Mahesh Katuru
Schweitzer Engineering Laboratories, Inc.

Rajnarayan Karmaker
Power Grid Company of Bangladesh

Presented at the
Protection, Automation & Control World Conference
Raleigh, North Carolina
August 29–31, 2023

Originally presented at the
16th International Conference on Developments in Power System Protection, March 2022

LESSONS LEARNED FROM COMMISSIONING OF IEC 61850-9-2 PROCESS BUS-BASED BUSBAR PROTECTION SYSTEM

Jerin Monzi Mathew[1], David Dolezilek[1], Mahesh Katuru[1], Rajnarayan Karmaker[2]*

[1]Schweitzer Engineering Laboratories, Inc., Pullman, Washington, USA
[2]Power Grid Company of Bangladesh, Jahurul Islam City, Dhaka, Bangladesh
**jerin_monzi_mathew@selinc.com*

Keywords: SOFTWARE-DEFINED NETWORK, IEC 61850, PROCESS BUS, SAMPLED VALUES, PRECISION TIME PROTOCOL.

Abstract

Distributed busbar protection systems are common these days compared to traditional centralized busbar protection systems. A digitally distributed busbar protection system is often implemented using the proprietary technology of the numerical relay's original equipment manufacturer. The IEC 61850-9-2 standard for process bus communication and the IEC 61850-9-2 Light Edition (LE) guidelines provide a standardized and interoperable IEC 61850-based distributed busbar protection system and digital secondary system (DSS). This paper introduces several of the necessary test processes and performance metrics sufficient for a DSS installation and the specific commissioning results for a DSS serving a large, distributed busbar protection application. This paper discusses an IEC 61850-9-2 process bus, Precision Time Protocol (PTP) power profile, and software-defined networking (SDN)-based busbar protection system, which was implemented at a 400 kV substation for the Power Grid Company of Bangladesh (PGCB). The implemented solution protects four diameters of a one-and-a-half breaker busbar scheme and has the capacity for future expansion to accommodate up to eight diameters. This paper also discusses lessons learned from the project and provides data and evidence of the health and performance of the process bus-based DSS protection system.

1 Introduction

Providing access to affordable and reliable electricity to all citizens is a national goal of the Government of Bangladesh (GoB). In 1996, the GoB split the transmission sector and formed the Power Grid Company of Bangladesh (PGCB). PGCB is responsible for the construction, operation, and maintenance of the national power transmission grid. PGCB has recently constructed a new 400 kV grid substation to transmit power from the thermal power plants located near the coal mines to the capital city of Bangladesh, Dhaka.

A redundant busbar protection scheme was chosen for the new substation. One of the redundant schemes is based on IEC 61850-9-2 process bus and the other scheme is based on a traditional distributed busbar protection solution, which is based on proprietary technology of the numerical relay manufacturer. This is the first IEC 61850-9-2 process bus-based busbar protection scheme implemented by PGCB and it has provided them with a great learning experience, which will help them design and implement more IEC 61850-9-2 process bus-based solutions in the future.

2 IEC 61850-9-2 Process Bus-Based Busbar Protection Scheme

In the process bus-based busbar protection project, three sets of phase-segregated 87B Sampled Values (SV) relays protect the two buses and ties of the one-and-a-half breaker busbar scheme. There are eight 400 kV diameters in the project, four of which are future diameters. Each diameter has three merging units (MUs), one each for Bus 1, Bus 2, and the tie. The busbar protection scheme consists of six 87B subscriber intelligent electronic devices (IEDs), twenty-four MUs, one Precision Time Protocol (PTP) clock, and four software-defined networking (SDN) switches. All SV IEDs in the project are IEC 61850-9-2 Light Edition (LE) compliant. 87B SV subscriber IEDs provide busbar differential protection and breaker failure protection for the corresponding buses and ties. All or part of the protection scheme for the corresponding bus or tie will be blocked if more than three SV packets are lost consecutively from any of the MUs the SV subscriber IED is receiving SV streams from. Also, if time synchronization is lost by the SV subscriber IED or by the MUs from which the SV subscriber IED is receiving SV streams, then protection will be blocked in that particular SV subscriber IED. Three-phase current transformers and digital inputs (DIs) required for the busbar protection scheme are wired to each bay's MU. MUs and 87B relays are dually connected to the SDN in failover mode. Additionally, a PTP clock is dually connected to the SDN network and each link is configured as a PTP grandmaster clock. SDN switches are connected in a mesh topology.

Each MU in the busbar protection scheme publishes SV messages into the system at a message rate of 4 kHz (4,000 samples/second) for the 50 Hz system. The busbar protection relays subscribe to the specific SV messages which carry the phase current values that are used in the relay's protection logic. Each MU also publishes Generic Object-

Oriented Substation Event (GOOSE) messages into the network. These GOOSE messages carry the statuses of DIs from MUs to the 87B relay for protection logic. The MUs in this design are intelligent merging units (IMUs) with local protection and breaker control functions and they subscribe to GOOSE messages containing protection trip signals. Each 87B publishes GOOSE messages that carry protection trip signals to the network. The corresponding MUs subscribe to these messages. All GOOSE messages in the network have a minimum time (MinTime) of 4 ms and a maximum time (MaxTime) of 1,000 ms, meaning that the sequence of a redundant burst of messages is published immediately after a data set change (4 ms, 8 ms, and 16 ms after the change followed by the heartbeat message every second). The IMUs and 87B relays are time-synchronized using the PTP power profile. The simplified data-flow diagram of the project is shown in Fig. 1.

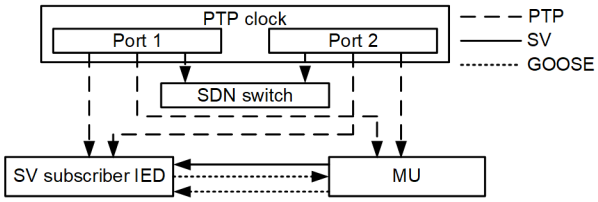

Fig. 1. Simplified data-flow diagram of the project.

3 Ethernet Communications Cabling

Serviceability is an expression of the ease with which a component, device, or system failure can be detected, diagnosed, and repaired. Early detection of potential problems in all parts of the design, including the communications cabling, is critical in this respect. Some systems detect and correct problems automatically before serious trouble occurs—such as operational technology (OT) SDN path failure reconfiguration [1]. Although popular, IEC 62439-3 Parallel Redundancy Protocol (PRP) is not actually redundant because it does not describe a fault detection mechanism. IEC 61508 is the international standard for electrical, electronic, and programmable electronic safety-related systems. The use of design tools described within this standard helped to design the new SV bus protection to be no less reliable, with the goal to be more reliable, than the traditional system that it replaced or the distributed system in parallel. This standard identifies the challenges of PRP by describing the failures of one side of the pair of PRP, GOOSE, or SV message receptions as a dangerous undetected failure that is not self-announced and does not generate alarms. These remain undetected until the failure of the second message in the pair, at which point the failure of both messages is detectable by standard IEC 61850 methods, and the total failure of data flow becomes a dangerous detected failure. Furthermore, IEC 61508 points out that the inability to detect the first failure and trigger corrective action reduces serviceability and the defect may remain dangerously undetected until a second failure, which may cause simultaneous protection failure. Dangerous undetected failures can only be verified during field testing by forcing failure of the second data flow and are often not even found if they are transitory in nature. IEC 61508 introduces numerous tools and processes that are used to make evidence-based decisions to support the use of failover connections and OT SDN in this design.

Using SDN, the system not only benefits from the deny-by-default security, but also from very fast data-flow fault detection and repair. Therefore, even if they occur, intermittent data-flow failures are not present long enough to affect signal message delivery to the extent that communication-assisted protection is disabled, and perhaps not at all.

The mean path delay of a packet traveling from the PTP clock to the subscriber is calculated with compensation for cable length and interposing switches, and represents the time taken for a packet to travel that path. Each path in the network, from publisher to subscriber, primary, and backup, is tested in this fashion. By connecting the PTP clock at each publisher position and observing the mean path delay calculated in each subscriber, the performance of the entire local-area network is measured and documented.

4 Network and Processing Latencies

Protection operation time of a process bus-based system includes the processing latency of SV and GOOSE messages in MUs and SV subscriber IEDs, communication link latency, and latency of Ethernet switches. As shown in Fig. 2, t_{f1} is the time taken by an IED to detect a physical input's status change. t_a is the time taken by the communication processing algorithm once a status change is observed to update the messaged payload, encode, and publish the message out of the IED. t_b is the total transmit time taken by a packet between the publisher and subscriber IEDs and is a combination of dwell time between the packet in Ethernet switches and the time the information takes to traverse the communication link between switches or between switch and IED. Once the packet reaches the subscriber IED, the packet is parsed and decoded by the communication processing algorithm. This time, t_c, represents the processing effort required for each received message; those expected by configuration are processed further, and unexpected messages are discarded. t_{f2} is the time taken by the IED to trigger an output after processing a valid status change message.

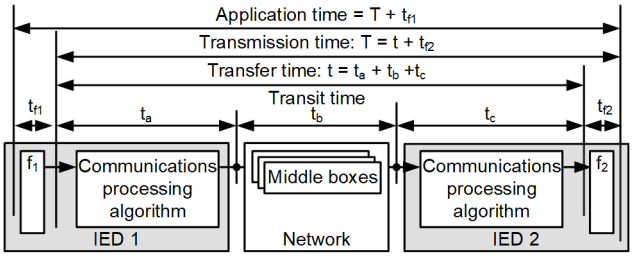

Fig. 2. Application, transmission, transfer, and transit time based on IEC 61850-5.

Some of the listed latencies can be measured in the field using the data available from the process bus protocols. This is detailed in the next section of this paper.

5 Testing IEC 61850 Process Bus-Based Protection System

As IEC 61850 process bus-based protection involves communication protocols, time synchronization, and an Ethernet network, it functions differently than a traditional protection system. Therefore, it is important to use different methods to measure the performance of various aspects of the process bus-based protection system. The project lessons learned include the thorough list of statuses, alarms, and diagnostics necessary to test, commission, diagnose, and service an SV system according to the numerous international standards related to GOOSE, SV, PTP, and Ethernet technologies. This paper details many, but not all, of these elements as part of specific tests described herein. The total quantity of elements required in the IEDs, clocks, and switches to describe data-flow behavior and self-announce alarms and diagnostics is large. It is also used to replace the many physical tools and test equipment in traditional systems. A subset of these elements is used within the devices in the system to describe and supervise the various dataflows, detect and self-announce anomalies, and provide diagnostic information, as illustrated in Table 1. The table contents show the quantity of necessary and sufficient elements for a single-status GOOSE, SV, and trip GOOSE data flow and many of the status and diagnostics are per-message. The total quantity of elements for the actual system is proportionally larger.

Table 1 Quantity of status, alarms, and diagnostics within the IEDs for protection system with single-status GOOSE, SV stream, and trip GOOSE

Monitored Technologies	MU Publisher	Clock, Port	Switch and Ports	Relay Subscriber
Ethernet and GOOSE	78	—	22	100
Above plus PRP	84	—	22	107
Above plus PTP	161	105	22	181
Above plus SV	304	105	22	339
Above plus GOOSE trip to IMU	349	105	22	384

5.1 Protection Testing

For protection testing of process bus-based protection schemes, currents and voltages are injected to the MU from the protection test set, and the protection trip feedback is wired from the MU to the protection test set if the trip command output to the breaker is hardwired from the MU. This process is similar to conventional protection scheme testing, but there are several other steps in process bus-based protection testing to ensure reliability of the system. The GOOSE subscription, SV subscription, and PTP time-synchronization status of each IED in the process bus need to be verified to ensure that all communications are normal. Accuracy of the current and voltage values published by the MU can be verified by comparing magnitude and phase angles of these values available in Common Format for Transient Data Exchange (COMTRADE) reports of the protection test set, MU, and SV subscriber IED. Another method to calculate the accuracy is by comparing the root-mean-square (rms) value of injected currents and voltages to that of the rms value of the subscribed SV currents and voltages [2].

5.2 Network Testing

For network testing, the user should verify whether each IED in the network is time-synchronized with PTP and whether the GOOSE and SV subscriptions are healthy. The user should then force failover to the backup port and check whether all communications are stable. Similarly, the user should test each available path between SDN switches and verify IED communication health. Also, SDN paths should be tested before deployment at the site using a tool to simulate traffic [3]. Using this tool, each Ethernet frame's primary and failover paths are validated by simulating link and switch failure. For security testing, spoofed frames are injected into the network using the tool to confirm that without an engineered SDN flow, they do not enter the system or reach any device. In this manner, tests confirm that only valid Ethernet frames enter and reach their expected destinations, even during network disruptions.

Evidence of in-service switch-to-switch link failover time is often measured as message delay or failed delivery at the subscriber IED. Other methods include a dedicated tool set, with one tool to send messages into the network, and a second tool to receive them to measure the distortion or disturbance of message delivery during the OT SDN path failover. SDN controller Ethernet port in-service test statistics document active ingress (received traffic) and egress (transmitted traffic) including: packet counts, byte counts, error counts, multicast message count, collision count, PTP packet count, GOOSE packet count, and SV packet count.

5.3 Time Synchronization

SV IEDs require high-accuracy time sources to function. Time-synchronization status of SV IEDs is indicated by SmpSynch. Time sources and their corresponding SmpSynch values are listed in Table 2.

Table 2 SmpSynch values

Time-Synchronization Source	SmpSynch Values
Global area clock	2
Local area clock with unique identifiers	5–254
Local area clock	1
No time synchronization	0

If an SV subscriber IED subscribes to only one SV stream, then time synchronization is required only for the SV MU. In this case, the SV subscriber IED will be in freewheeling mode. However, in protection schemes like busbar protection, SV subscriber IEDs subscribe to multiple SV streams and time synchronization is required for all SV IEDs. In this case, the SmpSynch of all SV streams subscribed by the SV subscriber IED must match with its own SmpSynch value. SmpSynch values of all IEDs in the process bus network should be logged during commissioning testing.

5.4 SV Delays

The SV stream network delay is calculated by the SV subscriber IED and is a sum of the MU processing delay and process bus network delay. SV subscriber IEDs buffer the SV messages received from MUs for a specified time called SV channel delay. SV channel delay is calculated by (1).

$$\text{SV channel delay} = \text{MAX (SVND)} + (N + 1) \bullet \text{sample period} \quad (1)$$

where:

MAX(SVND) is the maximum network delay out of all received streams.
N is the number of lost packets user wants the relay to ride through by interpolating data.

An allowable range of N is between 1 to 3, and an N value of 3 is a good choice for typical applications, because it allows the relay to ride through a loss of three packets.

The sample period is 0.2083 ms for a 60 Hz system, or 0.25 ms for a 50 Hz system.

An allowable range of SV channel delay is from 1 to 3 ms, which means the maximum network delay for an SV stream can be 2 ms for a 50 Hz system and 2.1668 ms for a 60 Hz system.

SV subscriber IEDs wait to start resampling until samples arrive for the configured channel delay. This provides a consistent delay to protection and control operations, which overcomes the nondeterministic delays caused by the Ethernet process bus network. SV message delivery delays are made visible and useable by internal calculations and statuses within the SV IED subscribers as network delays. These values are compared against the baseline done with PTP mean path delay testing during commissioning. The SV network delay observed in the process bus-based busbar protection system project was 0.75 ms and the channel delay set in 87B SV subscriber IEDs was 1.75 ms.

5.5 GOOSE Transmission Time and Application Time

Transmission time duration, as shown in Fig. 2, is calculated using the time difference between the time stamp in the Sequential Events Recorder (SER) for the contact input detection in IED 1 and the time stamp in the SER of the signal reception in IED 2. When an external trigger is synchronized to the top of the second, the error in the transmission time duration (based on the delta time-stamp method) includes a physical input time-stamp processing error on the publisher and a digital message processing time-stamp error on the subscriber. The application time test is performed via an additional application timer test element in the actual signal GOOSE message. Using the actual signal GOOSE message provides vital performance information and acts as a persistent confidence check. The application timer test element provokes an SER in the subscriber and is used to trigger subscriber logic to publish a return GOOSE message that contains a second application timer test element. IEEE refers to this as a ping-pong test, but it uses GOOSE messages rather than a ping command. Ping time is the duration of one direction, and pong time is round-trip [4].

Although the method of using SER time stamps to calculate transmission time is useful and relatively easy, the error introduced by the asynchronous processing cycles is statistically large compared to the expected values. Therefore, with existing IEDs it is possible to get an accurate understanding of application times, but it is not possible to get a precise time-duration calculation. Since change-of-state of a payload is often published in a burst of four messages between 0 to 16 ms after the event, the network must detect the failed path and restore path flow in under 15 ms to make sure the change is detected by the receiver. The IEDs have the resolution to perform time-duration calculations within the IEDs with enough accuracy to confirm when the applications are working correctly and—more importantly—when they are not [4]. Also, communications-assisted logic should be designed to work as fast as possible, but also work correctly even if there is a 14 ms delay in the signal delivery from the publisher.

5.6 Switch Latency and Physical Link Latency

Latency introduced by the switch and physical communication link can be calculated using the PTP log available in IEDs. Mean path delay in PTP indicates the physical communication link latency. Network time inaccuracy indicates the dwell time of the PTP packet in the switch or the switch latency. The SDN switches and PTP clock of in the process bus-based busbar protection project were adjacent, and the cable length between these devices were small. Physical link latency and switch latency was calculated and verified using the following procedure and Fig. 3.

1. When the IED active port is Port A, and the PTP source is the PTP grandmaster clock connected to SDN Switch 1, then the path taken by the PTP packet is 1-2-A. In this case, PTP network time inaccuracy equals SDN Switch 1 latency, and mean path delay equals the latency of the communication path 1-2-A. Since the IED does not know the number and type of switches, PTP calls for each switch to calculate and provide a network time inaccuracy value so that the IEDs can correctly synchronize. Another lesson learned is that many information technology (IT)-focused switches simply do not update this field and the SV protection eventually fails due to incorrect (zero) values being used by the PTP subscribers attempting to synchronize.
2. When the IED active port is Port B, and the PTP source is the PTP grandmaster clock connected to SDN Switch 2, then the path taken by the PTP packet is 5-6-B. In this case, PTP network time inaccuracy equals SDN Switch 2 latency, and mean path delay equals the latency of the communication path 5-6-B.
3. When the IED active port is Port A, and the PTP source is the PTP grandmaster clock connected to SDN Switch 2, then the path taken by the PTP packet is 5-4-3-2-A. In this case, PTP network time inaccuracy includes SDN Switch 1 and SDN Switch 2 latency, and mean path delay equals the latency of the communication path 5-4-3-2-A.
4. When the IED active port is Port B, and the PTP source is the PTP grandmaster clock connected to SDN Switch

1, then the path taken by the PTP packet is 1-3-4-6-B. In this case, PTP network time inaccuracy includes SDN Switch 1 and SDN Switch 2 latency, and mean path delay equals the latency of the communication path 1-3-4-6-B.

5. The mean path delay observed in Step 1 and Step 2 should be approximately equal, since the physical communication link length is almost the same. Similarly, the mean path delay observed in Step 3 and Step 4 should be approximately equal.
6. Network time inaccuracy observed in Step 1 and Step 2 must be equal, since the SDN switches have the same properties. Also, the network time inaccuracy observed in Step 3 and Step 4 should be twice the network time inaccuracy observed in Step 1 and Step 2, since the PTP packets flows through two SDN switches.

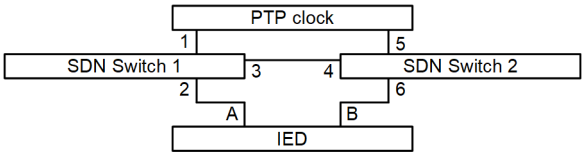

Fig. 3. Switch and physical link latency calculation.

Network time inaccuracy and mean path delay measured for a single IED following the above listed steps during commissioning is given in Table 3.

Table 3 Network time inaccuracy and mean path delay

IED Switch	Clock Switch	Network Time Inaccuracy (ns)	Mean Path Delay (ns)
SDN 1	SDN 1	49	30
SDN 2	SDN 2	49	29
SDN 1	SDN 2	98	28
SDN 2	SDN 1	98	28

5.7 Process Bus Traffic

A typically configured UCA IEC 61850-9-2 LE-compliant SV Ethernet packet with a single application service data unit (ASDU), an SV identifier (SVID) of 10 bytes, the Ethernet preamble (7 bytes), the start frame delimiter (1 byte), and the interpacket gap (12 bytes), is 146 bytes [2]. Since a 50 Hz system SV stream has a publication rate of 4,000 messages per second, each stream requires a bandwidth of 4.672 Mbps. Therefore, as few as 22 SV streams will aggregate to 103 Mbps. This immediately causes oversubscription and buffer delays followed by link saturation and message loss on a 100 Mbps link. In the process busbar protection project, 24 MUs are available in the system, and each MU will publish one SV stream into the network; therefore, it is important to engineer the network so that only the required number of SV streams are received by the SV subscriber. A poorly designed network may result in congested network traffic and intermittent loss of Ethernet messages at the switch level. Also, it can lead to the subscription of unwanted GOOSE messages and SV streams, which delays the processing of important GOOSE messages and SV streams.

To verify the process bus traffic which ingresses into an IED, the corresponding switch port can be mirrored and monitored using a network traffic capture tool. Also, the user should verify whether the SV stream and GOOSE message settings are based on the best practices using the SV and GOOSE logs in IEDs.

6 Process Bus-Based System Monitoring

Process bus-based system monitoring can be carried out using the built-in tools available in the IEDs or by using supervisory control and data acquisition (SCADA). These tools can simplify the monitoring process and quickly identify errors in the system.

6.1 Light-Emitting Diode (LED) Indications and Liquid Crystal Display (LCD) Points

SV stream quality, GOOSE message quality, high-accuracy time-synchronization status, and SV protection health can be shown as LED indications on the SV subscriber IED so that the substation operator can easily identify if there are any errors in the system. Also, the LCD rotating display of the SV subscriber IED can show details like SV coupled-clocks-mode status, SV network delay, SV channel delay of each stream, SmpSynch value of subscriber and each stream, details of PTP, and Ethernet link status. If an operator notices any LED indication alarm, he or she can further refer to the display points to quickly check the status of the process bus-based system. Similarly, suitable LED indications and display points can be shown in SV MUs.

6.2 GOOSE Ping-Pong Tests

As described in Section 5.5, a GOOSE ping-pong test can be used to measure the transmission time and application time of GOOSE messages. These tests can be configured in the relay logic and an operator can periodically test the transmission time and application time of GOOSE messages by pressing a pushbutton. Alternatively, these tests can also be configured to run periodically and latch an output contact or generate a SCADA alarm when the threshold value is crossed. This can help to ensure GOOSE transmission time requirements are met by the system when in service.

6.3 Relay SV, GOOSE, and PTP Logs

If there is an error in the process bus-based system, analyzing the SV, GOOSE and PTP logs in process bus IEDs can help. SV and GOOSE logs indicate whether there is any warning or error in the subscribed messages; some examples are listed below:

- An out-of-sequence warning is displayed when the SV stream or GOOSE message is not received in the correct sequence of SV sample count or GOOSE sequence number; this may indicate a network issue.
- A SmpSynch mismatch error is displayed when the subscribed SV stream SmpSynch does not match with the SmpSynch value of the subscriber; this indicates an issue with time synchronization.

- An SV stream lost error is displayed when four or more consecutive SV messages are not received by the SV subscriber IED; this indicates a loss of communication.

Total downtime duration and maximum downtime duration is available for each SV stream and GOOSE message subscribed by the IED. PTP logs provide details such as time-synchronization accuracy, PTP grandmaster clock details, network time inaccuracy, and mean path delay. Details available in PTP log are helpful for troubleshoot PTP time-synchronization issues. Also, it is important for adding SV-, GOOSE-, and PTP-related signals to SERs and relay event reports, and it can be used to troubleshoot issues observed in the process bus-based system.

6.4 SCADA

IEC 61850 Manufacturing Message Specification (MMS) logical nodes for SV and GOOSE subscriptions (LSVS and LGOS) in process bus IEDs provide useful information about SV and GOOSE messages. Process bus-based systems where process bus IEDs are also connected to the station bus can communicate with SCADA and send the LSVS and LGOS data for display in a SCADA human-machine interface (HMI). The user can develop an SV and GOOSE matrix in SCADA to give an overview about the process bus-based system with indications for SV and GOOSE message health. A detailed screen can also be developed for each process bus IED that displays the detailed statuses of SV and GOOSE subscriptions of that IED. Also, PTP time-synchronization details can be displayed for each IED.

7 Key Performance Indicators (KPIs)

Measuring and logging process bus-based system parameters over a period of time provides great insight about the performance of the system. Table 4 describes the KPI metric, which can be developed using data obtained from logging and reporting features available in process bus IEDs.

Table 4 KPI metric

KPI Component	Description
Metric	Performance of IEC 61850-9-2 process bus-based protection system
Target Performance Level	Zero protection blocking due to loss of SV, GOOSE, and PTP since last IED reset
Format1, Interval1	SV, GOOSE, and PTP failure indication updated in real time as IED front-panel HMI alarm or SCADA updated in real time
Format2, Interval2	SV and GOOSE updated in real time and PTP logs on demand
Format3, Interval3	SV and GOOSE downtime updated in real time and details on demand
Format4, Interval4	SV and GOOSE and PTP fail in real time and count on demand
Format5, Interval5	Protection system operation event in real time and report on demand

KPIs are a great tool to measure and evaluate a system's performance over time. They can help an end user develop a database on the process bus-based system, which can be a great tool when designing future IEC 61850-9-2 process bus-based systems.

8 Conclusion

Protection schemes using IEC 61850-9-2 process bus-based protection might appear complex to design, develop, test, and deploy. However, with the right tools, testing procedure, and understanding, process bus-based systems can be successfully deployed. Logs that are available in the process bus IEDs provide great insight about the system performance and help users develop KPI metrics. These KPI metrics help customers gain confidence in IEC 61850 process bus-based protection solutions, identify any shortcomings, and rectify them in future implementations. The dependence of the process bus-based system on an Ethernet network and high-accuracy time synchronization is considered a disadvantage of a process bus-based solutions, but by using SDN and by designing the appropriate redundancy required for the system, end users can confidently deploy process bus-based solutions.

9 References

[1] Dolezilek, D.: "Using Software-Defined Network Technology to Precisely and Reliably Transport Process Bus Ethernet Messages," proceedings of the 14th International Conference on Developments in Power System Protection, Belfast, United Kingdom, March 2018.

[2] Yang, Q., Keckalo, D., Dolezilek, et al.: "Testing IEC 61850 Merging Units," proceedings of the 44th Annual Western Protective Relay Conference, Spokane, WA, October 2017.

[3] Kalra, A., Dolezilek, D., Mathew, J. M., et al.: "Using Software-Defined Networking to Build Modern, Secure IEC 61850-Based Substation Automation Systems," proceedings of the 15th International Conference on Developments in Power System Protection, Liverpool, United Kingdom, March 2020.

[4] Dolezilek, D., Dearien, J.: "Lessons Learned Through Commissioning and Analyzing Data From Ethernet Network Installations," proceedings of the 5th International Scientific and Technical Conference "On Actual Trends in Development of Power System Relay Protection and Automation," Sochi, Russia, June 2015.

20211110 • TP7039