Validation Testing of IEC 61850 Process Bus Architecture in a Typical Digital Substation

Michael Whitehead, Mital Kanabar and Hesam Hosseinzadeh
R&D Technology Department
GE Grid Automation
Markham Ontario, Canada

***Abstract*— This paper examines the challenges posed to protection devices in IEC 61850 process bus systems, and the impacts that the process bus architecture has on the reliability of protection. A hardware in the loop setup is used with merging units, communication networks, and test sets to establish a small-scale actual substation. Next, a software-based sampled values generator was built to examine the impacts of extreme delay, missing and invalid samples on a real protection IED. Solutions to minimize the impact of delayed, missing, and invalid samples are then proposed and evaluated for their impact on the protection device. This paper highlights the common issues with process bus systems and the effectiveness of some solutions to these challenges from the perspective of protection.**

Keywords—digital substation, IEC 61850, IEC 61869, IED, process bus, protection, sampled values

I. INTRODUCTION

The standardized fully digital substation is gaining momentum all over the world. With the proliferation of IEC 61850 to establish standards for communications and interoperability among substation devices, analog signals are quickly being replaced by digital signals. Building upon IEC 61850, as an application of that standard to instrument transformers, the IEC 61869 standard aims to replace the analog wiring from field CT/VTs with digital communications. Just as IEC 61850 eliminated much of the costs and complexities of point-to-point wiring between Intelligent Electronic Devices (IEDs), IEC 61869 promises to transform physical connections among field devices and the IEDs that consume the signals, to logical connections based on standardized protocols. IEC 61869 describes an Ethernet communications protocol carrying digitized Sampled Values (SVs) of process data, from devices such as Merging Units (MUs) connected to instrument transformers in the field, back to the protection and control IEDs. This communications network transporting process-level data is known as the process bus. As a communications-based system, process bus offers a great deal of flexibility by allowing data to be easily shared amongst IEDs, however it also poses a great number of new challenges to protection schemes.

II. INTRODUCTION TO PROTECTION CHALLENGES

Reliability is paramount for any protection system; the system must be both secure and dependable. A process bus system typically is comprised of merging units, clocks, Ethernet switches, and other sophisticated electronic devices. Each of these components can experience a fault, resulting in the component completely shutting down or operating in unexpected ways, compromising the data that the protection IEDs operate on. Without proper safeguards in place, these faults could impact the security and dependability of the protection system.

Protection speed is the second challenge. In a sampled values system, the IEDs must work with a sample rate defined by the IEC 61869 standard. Not only are IEDs forced to process data at this rate, but they must also handle the variability in the reception time of the samples from all subscribed MUs. Variations in individual MUs data sampling and network delays contribute to the overall variability. The protection system must consistently operate in a timely manner, even in the face of this variability.

III. CHALLENGES FOR PROTECTION DEVICES

Shifting the responsibility of digitizing the analog signals of instrument transformers, from the IED to merging units, creates a new paradigm for protection IEDs. The IEDs must now rely on externally supplied data from, potentially, multiple MUs rather than having control over the digitization process. This raises challenges in the time synchronization of samples, processing challenges to decode and reconstruct the original signal, and challenges in vetting the trustworthiness of the received samples. These challenges directly impact protection elements in a process bus system in terms of reliability and speed of operation.

Since the process bus carries sampled values from various parts of the system, any given IED is exposed to a high level of network traffic for which it is not the intended consumer. Therefore, the IED must be able to discern quickly which incoming frames are required for its applications and quickly drop the frames that are not required. All this must be done without overloading its processing capabilities, which may result in delayed protection. To avoid overloading and maintain protection integrity, some IEDs may impose a cap on the number of streams that can be present on the process bus. IEDs will also limit the number of streams its applications can subscribe to; this may be in the tens of streams, though typically less.

Taking the processing capability of the IED out of the equation, there are still inherent system challenges with

sampled value systems that the IED must address. From the perspective of the protection and control devices, the system challenges discussed so far can eventually manifest in delayed, missing, or unacceptable samples at the IED level. These items are possible failures from the IED perspective and must be handled appropriately to maintain the reliability of the overall protection scheme.

A. Delay

Delay from a process bus perspective is the difference between the time encapsulated in an SV frame and the time on the IED when the frame is received and timestamped. Delay is therefore a function of the timestamp accuracy in the MU, the speed at which the MU publishes the SV frame, the delays introduced by the communications network and delays internal to the processing IED.

Merging units are expected to comply with IEC 61850-5 class 4 and provide timestamped samples with an accuracy of +/- 4us [1]. For perspective, 4us represents almost 2% of the typical reporting period of 208us for IEC 61869 [2]. Samples, however, are not necessarily published with the same level of accuracy.

Delays in the communications network are a sum of transmission, propagation, queuing, and processing delays, which in turn establish the bandwidth of the network and maximum throughput. As a network's bandwidth gets consumed, communication delays become more varied and pronounced. It is therefore critical to have a network designed to support the required bandwidth. A SV frame with a stream ID length of 13 characters consumes around 5Mbps of network bandwidth, using a report rate of 4800 frames per second. Using multiple ASDUs in a single SV frame and using 1000Mbit switches can help alleviate bandwidth issues.

Issues in a network device, such as a switch or redundancy box, may delay sample transmission. Any equipment found to be defective or unreliable should be replaced immediately. Network traffic bursts can also be a source of intermittent delay since the bursts consume significant amount of the network bandwidth and, therefore, impact the transmission of the sampled values. In most types of traffic, such delays may not be noticeable, however, due to tight requirements of sample delays, this delay can impact protection. This is one of the main reasons that the traffic on a process bus should be restricted.

Delay is a major concern for protection because a protection IED cannot run functions relying on the sampled data until it has arrived. This may result in the entire IED waiting for new data to arrive before running protection or the IED may just delay impacted elements and functions. In either case, there is some impact to protection, which may or may not be meaningful depending on the amount of delay.

B. Missed Samples

Missed samples are samples that never arrive or that are discarded by the IED for any reason, such as arriving out of order or arriving after a predetermined timeout period. There are several factors in an SV system that may result in missed samples in the IED. As mentioned previously, intermittent issues in a network device or burst of traffic, can result in either missing samples or a long delay in sample transmission that may cause the IED to assume the sample is missing. Moreover, if the received frames are not compliant to the standard, are missing mandatory fields or part of the frame is not readable, then the IED drops this traffic as invalid. These frames are also considered missed from the IED's perspective.

Environmental factors, such as ambient temperature or humidity, can impact the hardware of the process bus devices and infrastructure. Harsh conditions can accelerate hardware failure and cause improper operation. Additionally, software errors may also cause a temporary or complete failure of a device. These issues can contribute to missed samples. Manufacturers of critical substation equipment make every effort to prevent these failures.

The missed sample rate is an important factor that shows the health of the network. This rate should ideally be zero or a significantly small value since in the SV system, and according to IEC 61869 standard, there is no mechanism for detecting and resending missed samples by the publisher. IEDs must be able to take actions to deal with missed samples in a way that does not compromise the security and dependability of the protection system.

C. Unacceptable Flags

Digital solutions tend to have a wealth of internal diagnostics to self-check if the system is functioning correctly. IEC 61869 uses quality flags with each sampled value to communicate to subscribers if there are potential inaccuracies in the measurements. If a merging unit detects an internal issue that can impact the accuracy of the measurements, it indicates via these quality flags that the data published may be compromised. There are quality bits for specific causes, such as data that is out of bounds, but also a general validity field to state whether the data is valid, invalid, or questionable.

The use of quality flags also helps with maintenance on the system. Test and simulation flags in the sampled value frame allow for devices to be logically removed from the system, rather than physically, as subscribing devices can use these flags to ignore a stream.

Additionally, there are fields defined in the SV frame to indicate whether the merging unit's timestamps are synchronized globally or locally. This can help to determine if all devices are using the same grandmaster clock. Being able to configure the behavior of the IED for this flag, provides the user flexibility to ignore sampled values, that are not synchronized to the same reference as other devices on the network.

Generally, an IED should detect unacceptable quality flags for each sampled value and then treat them as if they are missing, ensuring there is no compromise to the reliability of the protection functions. Some IEDs provide settings that give the user the flexibility, to decide whether questionable data should be accepted or rejected. Diagnostics on the protection IED may display these quality flags to allow for system trouble to be easily identified.

IV. Sampled Values Diagnostics

Modern IEDs generate a wealth of diagnostic information and this extends to statistics critical for process bus systems. Useful diagnostics assist with troubleshooting issues during commissioning and with detecting transient or permanent changes in the system.

Diagnostics derived from the quality and other fields of the SV streams help to pinpoint if there is currently anything abnormal going on with the MU. For instance, if the protection relay is expecting the MU to be synchronized globally but the MU reports to be running from a local time source this could result in the relay dropping the stream. The diagnostics can be used to quickly determine if this is the case. Table 1 shows some typical diagnostics useful for understanding the status of the subscribed SV streams.

Table 1 - Common Real-Time Diagnostics

Diagnostic	Description
Status	A high-level description of the stream's health
Sim Flag	Indication if the stream is simulated
Delay	Real-time delay measurement
Missed Frames	Indication of any recently missed samples
Quality	Indication if any quality flags are active
Clock Statistics	Indication of clock source and jitter

It is also useful to monitor occurrences of excessive delays or missed samples to understand if there are intermittent issues on the process bus. Protection IEDs generally have mechanisms to handle small amounts of delay and missed samples, but efforts should be made in the design of a process bus system to prevent these situations from occurring. Table 2 shows some typical diagnostics to help detect intermittent issues with the stream, clock synchronization and quality.

Table 2 - Common Long-Term Diagnostics

Diagnostic	Description
Delay	Average delay of a stream
Delay Alarm	Number of instances where a delay threshold has been passed
Sample Estimation Counter	Number of samples that have been missed but the IED can estimate the values
Sample Fail Counter	Number of times that samples have been missed but the IED cannot estimate the missed samples' values
Stream Diagnostics	Record of any system events such as change in quality or simulation mode

V. Process Bus test setup and simulation of Sampled Values discrepancies

If delayed, missing, or invalid samples are present, it is important to understand the impact of these factors on the protection system. To do this in a controlled environment, it was necessary to generate SV streams that can be manipulated precisely to simulate conditions that test the limits of the IED's algorithms for handling these errors. Commercial MUs and test sets are expected to produce valid SV streams and therefore are not useful for evaluating the algorithms in negative test case scenarios. Commercial systems may allow for the setting of test or simulation mode, but generally do not allow for complete manipulation of the SV frames, so a Linux-based software SV generator was developed.

The simulator allows for up to eight independent SV streams to be configured. The reporting rate and number of Application Service Data Units (ASDUs) is global for all streams, however each stream has a user-definable destination MAC, sampled value ID, dataset, and configuration revision. The values of the measured quantities in the datasets also are configured independently for each stream. Additionally, the simulator can be used to playback COMTRADE captures to allow for the injection of complex signals from real systems. To prevent drifting and to synchronize the SV streams to the IED under test, an IEEE 1588 clock is run on the computer generating the SV streams. The clock can act as either a master or slave.

Each stream may independently have the smpSync, quality, and simulation fields of the SV frames configured. These parameters may be set globally for a stream, or on a per-channel basis for the case of quality. These parameters are useful for validating that the IED accepts or rejects samples based on the configuration of the IED.

Network errors may also be simulated independently on each stream including delays, duplicated, missing, and invalid frames. These can be introduced on a periodic interval or as a one-time occurrence. These parameters are used to test how well the IED recovers or responds to stream errors or abnormal conditions. Figure 1 shows the main application window of the simulator software.

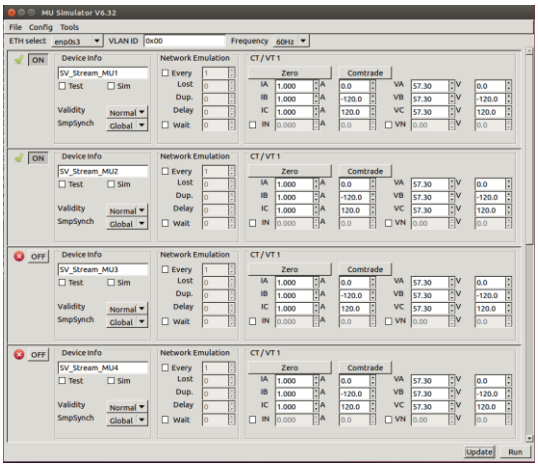


Fig. 1 MU Simulator main form

A small-scale substation, as shown in Figure 2, was created with three protection relays, an external clock, two simulated MUs and a real MU connected to an injection set. The simulated MUs were used to generate streams with errors introduced while the physical MU was used with testing network redundancy. The topology of the process bus was converted between different redundant and non-redundant configurations to assess the impacts of these configurations.

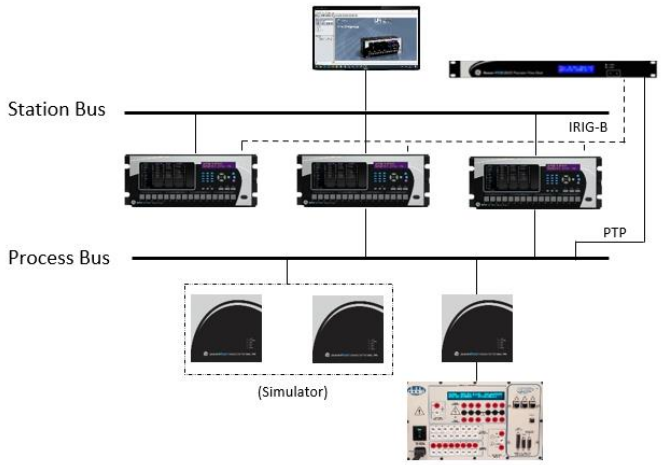


Fig. 2 - Test setup

VI. IMPACT OF SYSTEM CHALLENGES

Using the SV Simulator, it was possible to simulate some of the adverse conditions that an IED may experience. It is important to understand how protection on an IED will behave under abnormal conditions and how it will recover so that the reliability of the protection system can be maintained.

A. Impact of Delayed Samples

To test the impact of a constant delay in the SV streams, two SV streams were injected by the simulator. One stream was generated with a specific delay as compared to the other. Two IEDs were configured with a Phase Instantaneous Overcurrent (IOC) element operating on the SV stream with no intentional delay, and a GOOSE message was set to trigger on the operation of that element. One of the IEDs also had a second IOC element configured to operate on the delayed stream and a GOOSE message was set to trigger on the operation of that element too. A third IED was configured to subscribe to all three GOOSE messages. A depiction of the signal flow is shown in Figure 3.

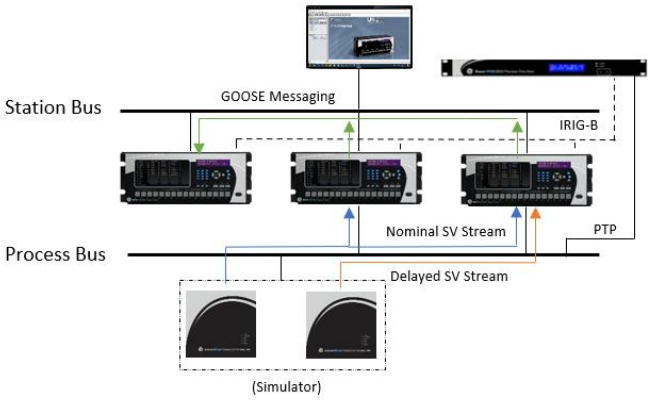
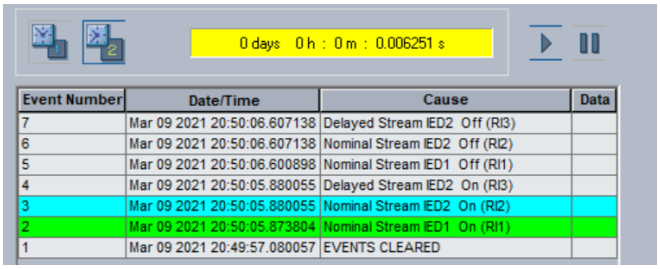


Fig. 3 - Simulator used to delay sample streams

The time of reception of each message was logged to measure the operation time delta of the two IOC elements in the first IED as compared to the second. This test determines if all protection on the IED is affected by the delayed stream or if only the protection elements using the delayed stream are delayed. Figure 4 shows an example of the event record from IED 3. In this example the delayed stream is intentionally delayed by 6.24ms.



Event Number	Date/Time	Cause	Data
7	Mar 09 2021 20:50:06.607138	Delayed Stream IED2 Off (RI3)	
6	Mar 09 2021 20:50:06.607138	Nominal Stream IED2 Off (RI2)	
5	Mar 09 2021 20:50:06.600898	Nominal Stream IED1 Off (RI1)	
4	Mar 09 2021 20:50:05.880055	Delayed Stream IED2 On (RI3)	
3	Mar 09 2021 20:50:05.880055	Nominal Stream IED2 On (RI2)	
2	Mar 09 2021 20:50:05.873804	Nominal Stream IED1 On (RI1)	
1	Mar 09 2021 20:49:57.080057	EVENTS CLEARED	

Fig. 4 - Event timestamps of IOC operation on two IEDs

The IOC elements of the second IED operate at the same time regardless of whether their operating signal is based on a delayed stream or not. This indicates that, for this IED, all protection elements are delayed proportionally to the amount of delay experienced on any of the subscribed streams. This is important as the protection function outputs are configured in various logical schemes before it results into circuit breaker control. All protection functions experiencing the same delay do not cause inappropriate logic condition to affect reliability (dependability or security) of the protections within the same application.

Measurements of delays can be found in diagnostics like in Figure 5 where there are repeated substantial delays in one subscribed stream, as shown in the SV Delay Alarm Counter and the magnitude of the worst cases shown in the processing delay statistics. This is not a situation of a permanently delayed stream though as the average and current delay are reasonable.

Sample Value Stream Statistics

Sample Value processing delay (uSec):		
RxSV Streams:	RxSV1	RxSV2
Min	-833.33	-833.33
Max	21250.00	1458.33
Avg	70.76	58.99
count	569876.00	569876.00

SV processing statistics

RxSV Streams:	RxSV1	RxSV2
SV Delay Alarm Counter	691	0

SETTING	PARAMETER
All RxSV Online	Yes

PARAMETER	RxSV 1	RxSV 2
Status	On	On
Sync Status	Global	Global
Sim Flag	Off	Off
Delay	82 us	13 us
Missed Frames	No	No

Fig. 5 - Diagnostics example with intermittent delay

B. *Impact of Missing or Invalid Samples*

When samples are missing (not received), received with unacceptable quality flags, or received but discarded for other reasons, the IED should have capability to estimate a tolerable number of intermittently missing samples, if good samples are also received. Well-designed digital IEDs are tolerant of missing consecutive samples too. To observe the impact of missing samples, two IOC elements were configured in one relay. A pickup of 1% above nominal was set to catch any potential unexpected operation of the element due to the estimation. Each IOC element was assigned to a unique simulated SV stream with several consecutive samples dropped every 3 power system cycles. These streams are assigned to channels shown as I7A, and I8A in Figure 6 with IOC1 for bays 1 and 2 assigned to each of these streams respectively.

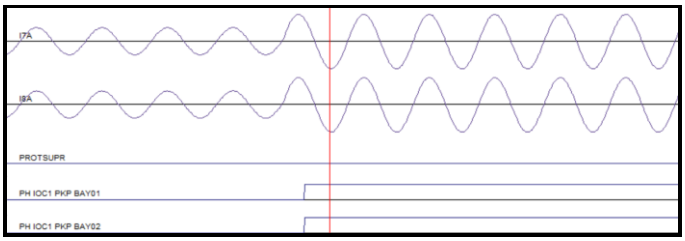


Fig. 6 - IOC operation with missing samples

In this test, channels I7A and I8A show identical measurements, although channel I8A is missing three consecutive samples every three cycles. The signal PROTSUPR (protection supervision) is a global flag that blocks all protection in the case of a serious error with the IED, and it remained off during this test. The result shows reliability as there is no impact on dependability of the protection functions when sampled value estimation is performed on signals just 1% below pickup, and the elements remain operated on the overcurrent (no drop of protection due to loss of SVs).

The diagnostics may be used to determine the severity of the issue. Figure 7 shows an example where samples were missing, but the IED was able to estimate values for the missing data. It also shows instances where the data loss was significant and beyond the ability of the IED to estimate successfully.

SV processing statistics

RxSV Streams:	RxSV1	RxSV2
SV Delay Alarm Counter	0	0
Sample Estimation Counter	60	0
SV 3 of 5 fail	102	0

Fig. 7 - Diagnostics example with intermittent missing samples

VII. SOLUTIONS TO SYSTEM CHALLENGES

There are multiple solutions to the challenges of missing, delayed, or rejected samples. To demonstrate the various solutions, failures in the network communications, merging units, and clock synchronization were introduced.

A. *Loss of Network*

The network can be responsible for dropping packets. This can be for intentional reasons, such as removing a device for maintenance, or unintentional in the case of device malfunction. Several solutions are available to overcome this challenge.

1) Solution a: Parallel Redundancy Protocol

The Parallel Redundancy Protocol (PRP) adds network redundancy to a system by introducing a second network that operates simultaneously with the first and carries the same network traffic. PRP networks should be built with separate hardware to avoid potential for a common point of failure. The process bus network from Figure 4 was converted into a PRP topology by using two Ethernet switches and configuring the IEDs for PRP mode. The Ethernet connection was physically broken between the IED and one of the switches as shown in Figure 8.

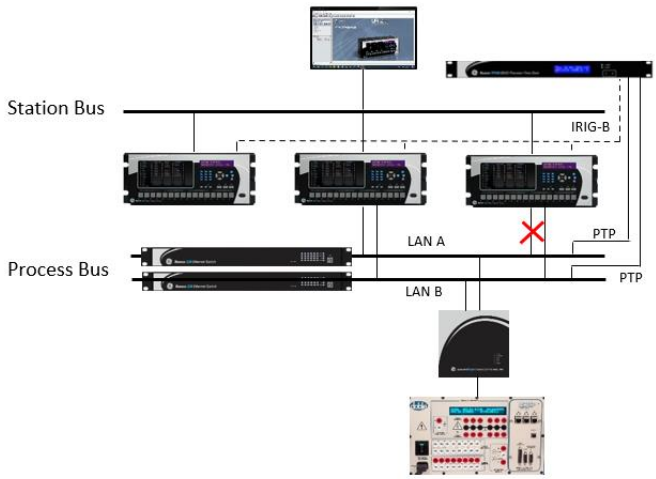


Fig. 8 - Parallel Redundancy Protocol network

Breaking the Ethernet connection on LAN A triggers the process bus Ethernet port (PBETHPORT) supervision flag of the port that is offline. This capture is shown in Figure 9.

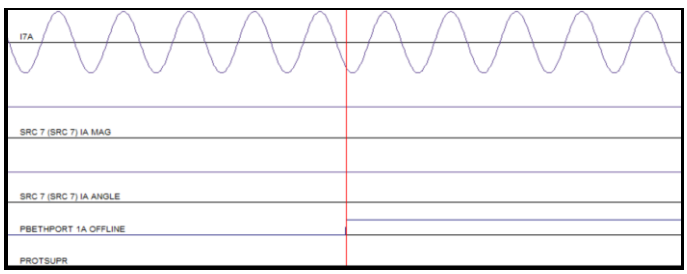


Fig. 9 - Sampled waveform at time of one network failure

Results of this test show no disruption or distortion of the IED's metering at the time the IED recognizes a network failure on one of its process bus ports. The diagnostics in Figure 10 demonstrate that the process bus messages over PRP are processed without even a single sampled value interruption.

	SV processing statistics	
RxSV Streams:	RxSV1	RxSV2
SV Delay Alarm Counter	0	0
Sample Estimation Counter	0	0
SV 3 of 5 fail	0	0

Fig. 10 - Diagnostics showing no missed samples with PRP

2) Solution b: High-availability Seamless Redundancy

High-availability Seamless Redundancy (HSR) is another network redundancy architecture to guard against a failure of a single node. HSR is a ring topology where duplicate data is transmitted in opposite directions around the ring such that one copy of the data still arrives at the destination node in the event of a break in the ring. The process bus network from Figure 4 was converted to a simple HSR network by configuring the IEDs to HSR mode and using HSR capable redundancy boxes to connect the devices that do not have native HSR capability. The Ethernet connection is physically broken between the IED and the next device as shown in Figure 11.

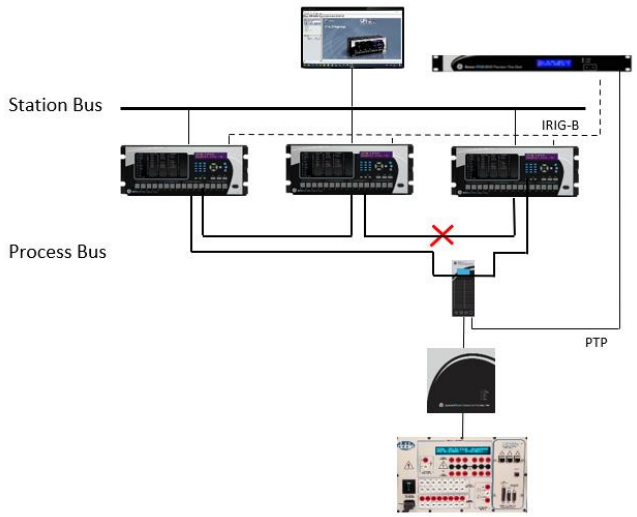


Fig. 11 - High-availability Seamless Recovery network

Similar to the PRP example, breaking the HSR ring triggers the process bus Ethernet port (PBETHPORT) supervision flag of the port that is offline. This capture is shown in Figure 12.

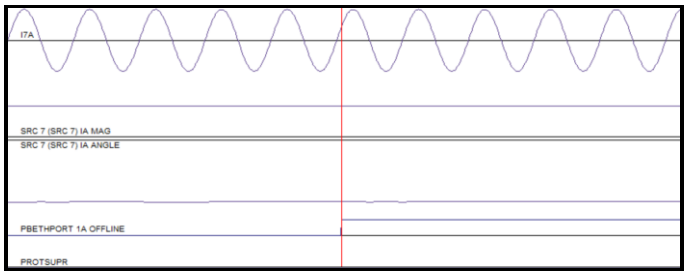


Fig. 12 - Sampled waveform at time of one network failure

Results of this test show no disruption or distortion of the IED's metering at the time the IED recognizes a network failure on one of its process bus ports. The diagnostics in Figure 13 demonstrate that the process bus messages over HSR are processed without even a single sampled value interruption.

	SV processing statistics	
RxSV Streams:	RxSV1	RxSV2
SV Delay Alarm Counter	0	0
Sample Estimation Counter	0	0
SV 3 of 5 fail	0	0

Fig. 13 - Diagnostics showing no missed samples with HSR

B. Loss of Stream or MU Failure

An SV stream may be lost, for several reasons: a merging unit may be removed from the system for maintenance, the device may have malfunctioned, or perhaps a self-test on the merging unit produces data with invalid quality. Figure 14 shows the diagnostics when a stream is failing due to invalid quality.

	Sample Value Stream Diagnostics	
RxSV Streams:	RxSV1	RxSV2
Stream Status	invalid	valid
Latest Unacceptable Quality	2021/02/06 01:38:21.737205	1970/01/01 00:00:00.000000
Latest Sim Bit Change	1970/01/01 00:00:00.000000	1970/01/01 00:00:00.000000
SmpSync Latest Update Time	1970/01/01 00:00:00.000000	1970/01/01 00:00:00.000000
SmpSync Changes in Past 24hrs	0	0
Sample Estimate Fail-Last 10s	159836	0
Sample Value Trouble Counter	1	0

Fig. 14 - Diagnostics example with unacceptable quality

1) Solution a: Crosschecking

Crosschecking is a form of application redundancy whereby the SVs are compared among multiple merging units and the preferred stream is selected automatically. To verify the performance of crosschecking, the simulator was used to generate two identical streams. The IED was programmed to use the first stream as a preferred source when both streams are healthy. The first stream was then disabled by the simulator forcing the IED to switch over to the redundant stream. This is depicted in Figure 15.

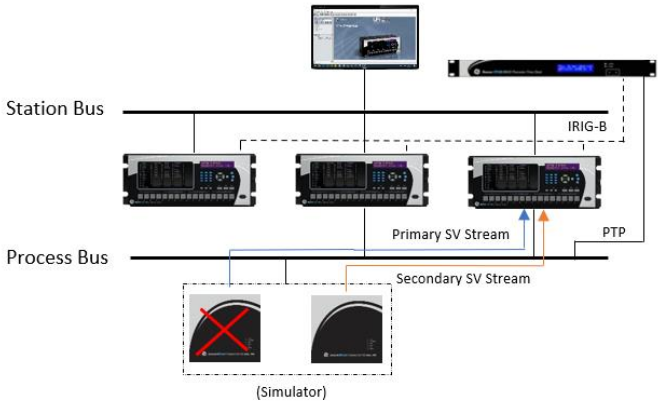


Fig. 15 - Crosscheck application redundancy

The waveform in Figure 16 was captured when the relay detects the preferred stream as unavailable and switches to the secondary.

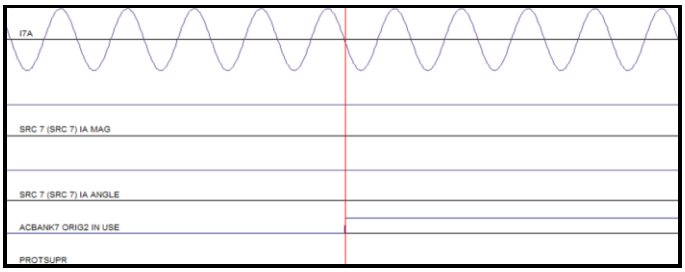


Fig. 16 - Sampled waveform at time of one stream failure

These captures show that when a stream is disabled, the IED automatically switched to the second stream without any disruption to the metering.

2) Solution b: Blocking of Impacted Funtions Only

In this test two IOC elements were configured in the same relay with a pickup of 1% above nominal to catch any potential misoperation due to the sampled value estimation. Each IOC element was assigned to a unique simulated SV stream. One simulated stream was set to go offline just before a fault was introduced. Figure 17 shows the reconstructed SV waveforms.

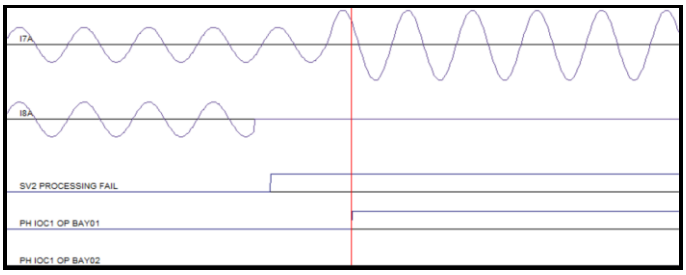


Fig. 17 - IOC operation with missing samples in partial block scheme

In this test, the IED recognizes the failure of a subscribed stream and blocks the IOC element, PH IOC1 OP BAY02, assigned to this failed stream. The IOC element, PH IOC1 BAY01, assigned to the healthy stream still operates. This result demonstrates that the reliability of the protection functions with a normal operating sampled value stream is ensured although another sampled value stream may be interrupted within the same IED.

C. Loss of Synchronization Source

Without a synchronization source, the internal clocks on the merging units and IEDs will drift over time and at different rates, causing delays between the streams that will grow over time. Eventually the delays will become too great and samples will be dropped. A method to keep the components in the SV system synchronized is therefore important and there are several solutions.

1) Solution a: IED as a PTP Master Within a Protection Zone

In an IEEE 1588, or Precision Time Protocol (PTP), network the best master algorithm automatically selects the best available clock on the network, within the same protection zone. Should the primary clock fail, any additional clocks on the network will detect this and automatically decide amongst the remaining clocks which should become the new master. By configuring the IED PTP master priority value, the IED can be assigned to be the PTP master within a protection zone process bus network.

In the following test the IED is synchronized through IRIG-B while the MU is synchronized through PTP. Both the IRIG-B and PTP signals originate from a single clock. In this setup, the IED has PTP master and slave functionality. When the power is removed from the clock, the IED registers an IRIG-B failure event and becomes a PTP master to synchronize the MU. This is shown in Figure 18.

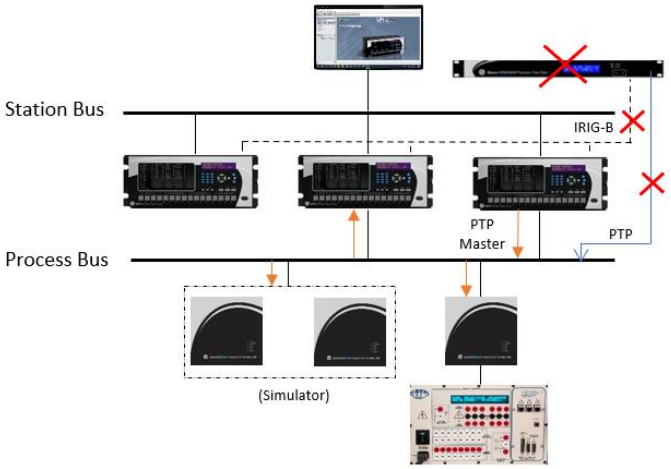


Fig. 18 - Loss of station clock

Figure 19 shows the captured waveform when the IED declares the external clock lost.

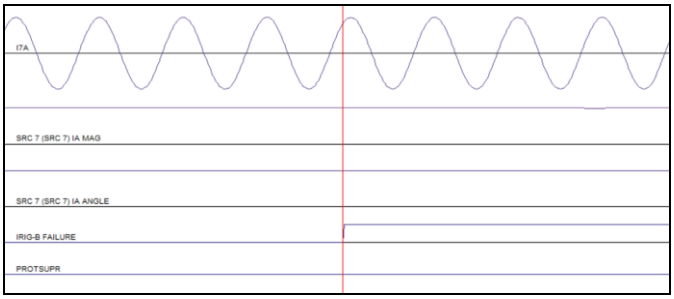


Fig. 19 - Sampled waveform at time of external clock failure

In this test, the switch over from the PTP global master clock to the IED protection zone master was seamless with no disturbance observed on the waveform. The diagnostics, as shown in Figure 20, indicate that the IED has now become its own time reference and that of the bus.

Clock Sync Source	PBM Internal Clock
PTP Grandmaster ID	C4 B5 12 A0 F4 00 85 01
Clock Accuracy	100 ns

Fig. 20 - Diagnostics showing the IED has become the PTP grandmaster

2) Solution b: Run Asynchronously

For some IEDs, being synchronized to an external clock, or acting as a master itself, is unnecessary. If the IED can operate asynchronously a loss of the station clock at the IED will have no impact on the processing of SVs. The caveat here is that even though the IED does not require synchronization, all the MUs must remain synchronized to the same time reference.

For testing asynchronous operation, the IED is synchronized through IRIG-B while the MU is synchronized through PTP. Both the IRIG-B and PTP signals originate from a single clock. When the IRIG-B output is disabled on the clock the IED registers an IRIG-B failure event and is left without any synchronization source. This is shown in Figure 21.

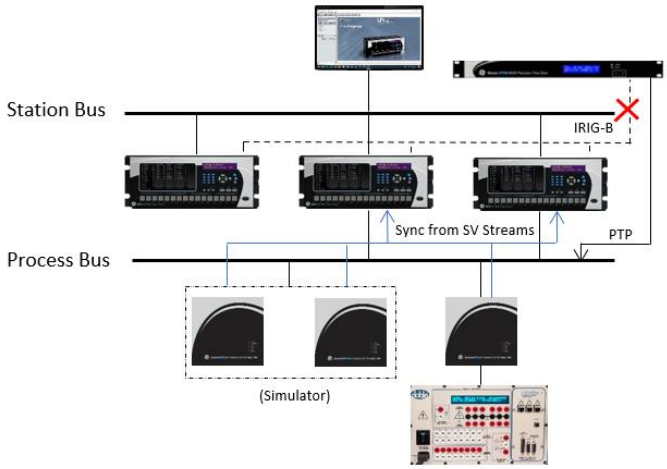


Fig. 21 - Loss of IED time synchronization

In this asynchronous mode, the IED continues to operate based on the sample stream. The waveform of the sampled stream as seen on the IED is shown in Figure 22.

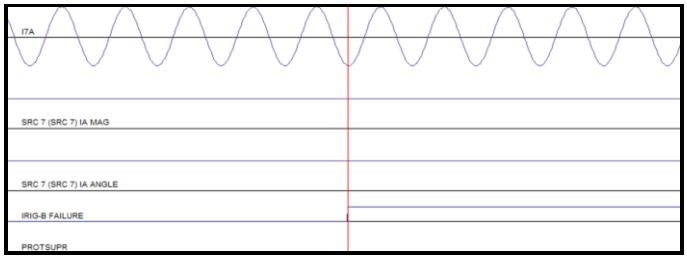


Fig. 22 - Sampled waveform at time of external clock failure

When the IRIG-B signal was lost and the IED was left unsynchronized there was no noticeable impact to the waveform or metered values. This demonstrates that the IED without synchronization can run asynchronously with a single MU stream. Asynchronous mode is useful when there is one MU or all MUs are synchronized using One Pulse Per Second (1PPS) independently. The diagnostics in Figure 23 show the clock is not synchronized and is deriving its own 1PPS signal.

Clock Sync Source	PBM Internal Clock
PTP Grandmaster ID	00 00 00 00 00 00 00 00
Clock Accuracy	999999999 ns

Fig. 23 - Diagnostics showing the IED is operating in asynchronous mode

VIII. SUMMARY

The introduction of process bus networks is an important progression for the fully digital transformation of the substation but is not without its challenges. It is imperative for substation designers working with process bus to understand how each of their devices will behave in a variety of situations relating to delayed samples, missing samples, questionable or invalid samples, and loss of equipment on the process bus. The test cases presented in this paper demonstrate that the technology is available now to build safe and reliable protection schemes using open communication standards such as IEC 61850 and IEC61869-9/13 over PRP/HSR or point-to-point network architectures. The advanced algorithms of protection and control IED ensures reliability of protection applications for various open standard process bus networks discrepancy scenarios.

REFERENCES

[1] UCA International Users Group, Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2. Raleigh, NC.

[2] Digital interface for instrument transformers, IEC Standard 61869-9, 2016

AUTHORS

Michael Whitehead is an embedded software quality test specialist at GE Grid Automation in Markham, Ontario, Canada. He has almost a decade of experience working with embedded software and developing test tools for firmware validation. His primary focus in on test and validation of IEEE C37.118, IEC 61850 and IEC 61869 on protection relays. Michael received his B. Eng. In electrical engineering from the University of Ontario Institute of Technology, Oshawa, Ontario and an MBA from Wilfrid Laurier, Waterloo, Ontario.

Mital Kanabar is leading the Office of Innovation and is Chief Applications Architect at GE Grid Automation in Markham, Ontario, Canada. He has 14 years of industrial R&D experience in the area of power system protection, automation and monitoring. Mital received his Ph.D. from University of Western Ontario, Canada; and M.Tech. from IIT Bombay, India. Mital holds 12+ international patent applications, contributed to 50+ journal/conference papers, 5 industrial magazine articles. He also serves as a Chair/vice-chair of technical working groups at IEEE Power System Relaying Committee (PSRC) and active member at other international standard committees.

Hesam Hosseinzadeh is an Engineering Manager at GE Grid Automation in Markham, Ontario, Canada. He leads a global engineering team responsible for validation and verification of the GE Universal Relay (UR) platform in power transmission applications. With a decade of experience, He has worked on a wide range of applications in Protection & Control, IEC 61850 and Substation Communications, Sampled Values and Digital Substations, Substation Automation Systems, Microgrid Control Systems and System Interoperability. He holds a master's degree in Electrical Engineering from the University of Western Ontario, Canada.