Complete Monitoring Solution to Improve Reliability and Performance of Digital Secondary Systems

Adilson Kotryk, *Companhia Paranaense de Energia*

Eduardo Goncalves, Ricardo Abboud, Mauricio Silveira, Paulo Lima, and Vinicius Ferrari
Schweitzer Engineering Laboratories, Inc.

Revised edition released September 2023

Originally presented at the
Protection, Automation & Control World Conference, August 2023

Complete Monitoring Solution to Improve Reliability and Performance of Digital Secondary Systems

Adilson Kotryk, *Companhia Paranaense de Energia*
Eduardo Goncalves, Ricardo Abboud, Mauricio Silveira, Paulo Lima, and Vinicius Ferrari,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—Solutions based on digital secondary systems (DSS) distribute protection and control functions across multiple devices that exchange protection signal information via communication networks. In such systems, effective monitoring plays a prominent role, since when properly designed, it provides complete visibility into operational statuses and guides troubleshooting of diagnostic alarms. Yet, DSS designs recurrently prioritize the practice of network redundancy, relegating the monitoring capabilities to the background. Effective monitoring of a DSS-based protection system includes both physical interfaces and application services. Operational data associated with physical interfaces consist of behavioral metrics such as operating temperatures, receive and transmit power, activity counters, and link status. Application services metrics include real-time machine-to-machine communications and data flow characteristics, time-synchronization status and accuracy, and status of logical redundant paths and links. It is essential that all these data are available in DSS devices and can be collected by a communications monitoring system with the use of standardized data models and communication protocols.**

This paper presents a comprehensive monitoring solution for a DSS-based protection system, operational in a 138 kV substation. It explores the concepts of redundancy and repair, highlighting the challenges created by misconceptions around them, as well as the benefits when they are properly considered. Further, it details the data points necessary for implementing an effective solution, with the end goal to increase the reliability of a DSS.

I. Introduction

Reliability comprises one of the essential facets of an energy protection and control system and consists in the assurance that it will perform correctly [1]. Protection and control systems supervise, protect, and control the primary system that, in turn, consists of equipment that generates, transmits, transforms, distributes, and consumes electric power. The transition of protection and control systems into digital secondary systems (DSSs), also known as digital substation solutions, brings new challenges with regard to the operational and maintenance standpoints as applications are now distributed across multiple components, which exchanges protection- and control-related information through a local communication network. In this approach, it is necessary to ensure that all devices and the local communication network are operational and ready to perform their intended functions when requested by the protection system. For textual simplicity, this paper refers to the terms of DSS-based protection and control systems or digital substation solutions simply as DSS.

Devices in a DSS include protective relays, merging units, Ethernet switches, and time reference clocks. Time reference clocks are often referred to as GNSS clocks, since they commonly use the reference signals transmitted by the global navigation satellite system (GNSS). Each DSS device performs specific functions in the scope of the protection and control system, interacting through general-purpose and purpose-built, time-critical application services. The time-critical services handle the transfer of metering, protection, and control signals among relays and between relays and merging units, as well as time distribution from GNSS clocks. Failures of any critical device or service requires prompt detection and alarm to enable corrective actions to maintain the reliability of the system.

The international standard IEC 61508 provides guidance for the use of electrical, electronic, and programmable electronic devices in protection and safety systems [2]. It labels failures that adversely affect a protection or safety system as dangerous, and those that are monitored and create alarms as dangerous detectable failures. The standard also shows the improvement to availability and system safety provided by automatic fault detection and self-alarm implementations within a device. Failures that jeopardize the safety of equipment or people, but are not monitored, are labeled dangerous undetectable and remain as hidden failures within the system.

Appropriately designed devices that are part of a DSS calculate, measure, and report an extensive set of monitoring data. While they can be individually accessed, these data gain more meaning and value when collected in a central monitoring system that can provide system-level visibility. In this context, a comprehensive monitoring solution that collects and displays information from all participant devices of a DSS becomes a crucial component within the systems. This solution enables monitoring the performance of each component over time and facilitates troubleshooting during system contingencies. Much the same way that DSS devices perform a self-test, this DSS monitor essentially performs system-wide self-test, alarm, and automated corrective action.

Such a monitoring system is especially important in redundant applications. Due to a misunderstanding in the relation between duplication, redundancy, and monitoring, DSS designs overly prioritize the redundant aspects, treating monitoring capabilities as a secondary function. Meanwhile, studies of reliability distributions show that redundancy is only

effective if the components are constantly supervised, making redundancy a costly and ineffective design choice when applied alone. The misunderstanding around these concepts can lead to design choices where DSS-based applications remain unaware of degraded operating conditions. Redundancy can hide failures of unmonitored components, resulting in an inaccurate sense of availability. IEC TR 61850-90-12 [3] addresses this concern in item 5.10.5, stating that monitoring is necessary for both components of a redundant scheme.

This paper describes a comprehensive monitoring solution applied to a DSS for a 138 kV substation. It provides a detailed description of all the monitoring points related to the operation of devices and services. Further, it explores the concepts of redundancy and monitoring, illustrating how they are thoughtfully considered in the monitoring solution to ensure reliability. It presents examples of monitoring screens that display all the relevant information described for both devices and services. The primary purpose is to raise awareness about the importance of comprehensive monitoring within devices and, more importantly, the importance of a monitoring system, providing a practical reference for implementation.

II. Station Bus and Process Bus as per IEC 61850

The IEC 61850 series establishes the data model and a set of communication protocols that, combined, allow the integration and interoperability of IEDs involved in the protection and control of power systems. The standard specifies the basic requirements for communications networks within a substation, dividing it in two segments [4]: the station bus and the process bus.

The station bus provides connectivity between protection, control, and metering IEDs, that under the standard's definition constitute the Bay Level. The deployment of a station bus involves two concepts:

1. Replace the SCADA interface of Remote Terminal Units and associated field wiring by engineering access and SCADA communications directly to the relay and controllers using layer 3 network addressable Ethernet methods.
2. Replace the conventional hardwiring between IEDs in a control house, used to transfer protection and control signals among devices, with a communications network that typically carries both layer 2 multicast and layer 3 Ethernet traffic.

Layer 2 traffic comprises time-critical applications, such as the transfer of trip or block signals. For these applications, the standard defines GOOSE [5] as the digital message transport mechanism. The multicast component of the Precision Time Protocol (PTP) [6] is another example of layer 2 application carried over the station bus and performs the distribution of time-synchronization signals among the connected devices.

In turn, layer 3 traffic applies to connection-oriented, non-time-critical applications, such as the exchange of control and supervision information between a SCADA system and Bay Level devices. For such applications, the IEC 61850 series defines the MMS protocol [5]. MMS uses TCP to monitor message delivery and request republication of undelivered Ethernet packets.

Station bus also carries protocols that are outside the scope of IEC 61850 series, such as the SNMP [8], DNP3 [7], and other protocols unrelated to supervisory applications. Engineering workstations and databases for event report are also connected to the station bus to provide settings management and centralize the collection of event reports. The top part of Fig. 1 shows the station bus along with the associated devices and commonly used protocols.

The lower portion of Fig. 1 shows the process bus with the commonly associated devices and services. The process bus provides connectivity between the Bay Level and the Process Level with the use of IEDs known as merging units (MUs). MUs are strategically installed close to the primary equipment and provide a means for the protection and control IEDs to interact with the electrical system. They are responsible for digitizing analog signals from potential transformers and current transformers into a stream of messages representing currents and voltages according to the definitions of the Sampled Values (SV) protocol.

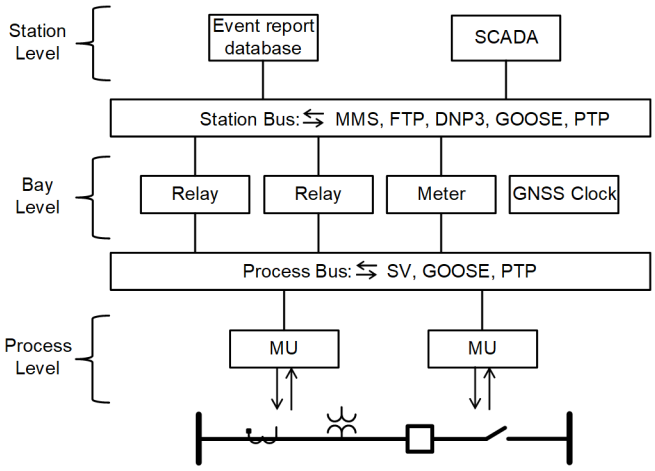


Fig. 1. Architecture of substation automation system, as per IEC 61850.

MUs can also digitize status information from circuit breakers, disconnect switches, power transformers, and other primary equipment and publish it as IEC 61850 GOOSE messages or convert GOOSE messages into electrical signals. Other MUs perform local protection and automation logic and are referred to as intelligent MUs (IMUs).

When required, the process bus also carries layer 2 PTP messages, ensuring that Process Level and Bay Level devices operate in the same time reference. Since the connectionless messages of GOOSE, SV, and PTP are published to unknown subscribers and receive no acknowledgement, the applications at source and destination need to monitor communications closely and adapt to the risk of undelivered messages. Because of the time-critical nature of these protocols, process bus presents stricter requirements for quality of service compared to station bus. Consequently, the monitoring requirements and mechanisms differ between the two network segments.

III. Fundamentals of Reliability

Before the start of deployment efforts for a comprehensive monitoring system, it is necessary to have a clear understanding of the concepts of redundancy and availability and how they relate with the overall reliability of a DSS. This understanding allows system designs to identify gap areas and even avoid worrying scenarios created by the improper use of redundancy.

A. Redundancy Principles

Redundancy is defined as the existence of more than one means for performing a given function [9]. It is a technique that increases the availability of a system by allowing it to withstand component failures. Designs of DSS can follow two distinct redundancy principles [3]: the standby redundancy and the workby redundancy, also called active redundancy. Several terminologies designate the redundant components of a protection and control system. Examples are the terms primary, dual primary, alternate, backup, Main 1 and Main 2, among others.

In standby redundancy, the backup unit remains inactive and begins operation upon detection of a failure in the primary. The activation of the backup unit can be automatic based on self-detected or manual failures. Non-critical sectors in the electrical grid often apply this type of redundancy, where the primary and backup units share the same model and the same configuration to streamline design and the replacement process when one of the units fails.

Standby redundancy is not restricted to physical units, though. In network communications, it consists in rerouting traffic to an alternate path when a primary link or switch fails. The spanning tree algorithm (STA) based on the Rapid Spanning Tree Protocol (RSTP) [12] presents an example of the standby redundancy in this context. Standby redundancy then relates to recovery rather than duplication mechanisms.

In turn, active redundancy consists in all components being continuously active and inserted into a system. Critical sectors of the power system can use the concept of active redundancy in duplication of components to eliminate downtime. Remedial action schemes (RAS) that control large geographic regions of interconnecting transmission, generation, and loads can combine the concept of active redundancy with security mechanisms and triplicate components, implementing a voting two-out-of-three scheme to issue control operations [13]. These design options relate to the concept of a monitoring system as the effectiveness of increasing components is directly related to the ability to monitor the performance over time, as discussed in the next sections.

In the context of network communications, the principle of active redundancy translates into duplication of messages and deployment of individual communication paths, in concurrent operation to deliver the duplicates to a destination device. The Parallel Redundancy Protocol (PRP) [14] is an example of a design that uses this principle. In a PRP system, the end devices are connected to two independent LANs, LAN A and LAN B. The end device handles the duplicates by forwarding the first received message to the application level while dropping the respective message of the pair received at a later instant. In doing so, PRP networks provide zero recovery time for single failures, contributing to the availability of critical applications, such as the transport of SV messages in a process bus.

It should be noted that RSTP and PRP can coexist in the same network design, even though they follow different redundancy principles. DSS often combines them in leveraging their unique characteristics. In this combination, PRP provides "bumpless" message delivery to applications for message loss due to single failures in a communications network. In turn, RSTP manages the redundant links in each LAN A and LAN B. This paper focuses the analysis on redundant network schemes based on the application of PRP protocol, since the impacts of PRP and its interplay with monitoring capacity must be thoroughly understood to grant not just network availability but also to increase the reliability of a system.

B. Availability During System Events

The setup in Fig. 2 can be used to demonstrate how network redundancy contributes to increase the availability of DSS. The setup uses a hardware-in-the-loop test that generates power system faults and interfaces with link break devices in order to time the instant of power system events with induced network failures.

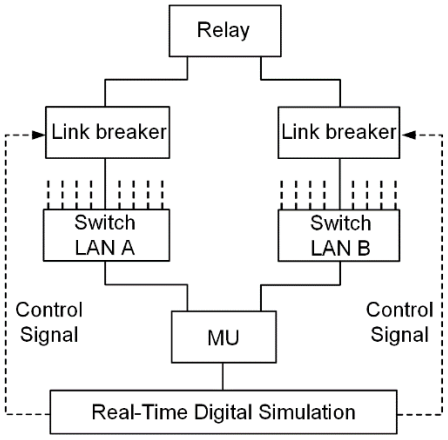


Fig. 2. Validation setup for network redundancy in a DSS protection system.

Fig. 3 shows the event report generated from the simulation. Fault inception occurs at 18:04:42.183, followed by a link break in the interface with LAN A 7 milliseconds later. The relay promptly detects the network event and deasserts binary variable LINK5A, correctly indicating that the failure is present in that LAN. The network event does not affect operation of the SV-based, communications-assisted protection system, and the relay correctly trips via Zone 1 phase distance element based on SV data received on the remaining interface. In sequence, the relay enters the autoreclose logic, and, during the open-interval timing, the test equipment reestablishes the link with LAN A and breaks the link with LAN B. Lastly, when the open-interval timer expires, the relay issues the reclose command, followed by the test equipment restoring the link with LAN B.

The event report shows a specific scenario in which the instant of a disturbance in the power system coincides with consecutive failures in a process bus. This is a valid possibility, considering that transients in the electrical grid can distress components of the protection system and drive them to failure. In this context, Fig. 3 shows how network communications use the principle of active redundancy to preserve the services required by DSS under high-demanding scenarios. The event report shows that the protection application is available during the entire event, since the redundant networks keep the continuous delivery of SV messages to the subscriber relay, even when experiencing consecutive communications failures.

From another standpoint, however, the same redundancy renders the protection application unaware of failures in the communications network. Even though the binary variables LINK5A and LINK5B provide valuable information about the relay's link statuses, they expectedly do not cover all possible scenarios of network failures. For instance, if a non-adjacent switch or link fails, it would not interfere with the link statuses in the relay and the binary variables would remain asserted. The event report shows the binary variables with the primary intent to identify the instant when the network failure begins, rather than to elaborate on a simplistic monitoring solution based only on the information from these two variables.

To better understand the concerns, suppose that in the event report from Fig. 3 the link break device does not reestablish one of the broken paths, characterizing a permanent failure. For subsequent failures, the network would degrade the system to a non-redundant one that relies on singular rather than duplicate messages.

In most cases, redundant network schemes transferring duplicate messages tolerate a single failure. However, DSS designs can make the wrong assumptions regarding what to expect when the system reaches the degraded operation. Due to a misunderstanding about the concepts of redundancy and the extension of its coverage, designs treat the absence of alarms as an expected behavior and use it as a validation of the system, when in reality this is a confirmation that it is hiding failures in plain sight [15]. Adding to this challenge, redundancy protocols implement supervision mechanisms that are not as effective as the handling of duplicates, which is the main purpose that they were designed for.

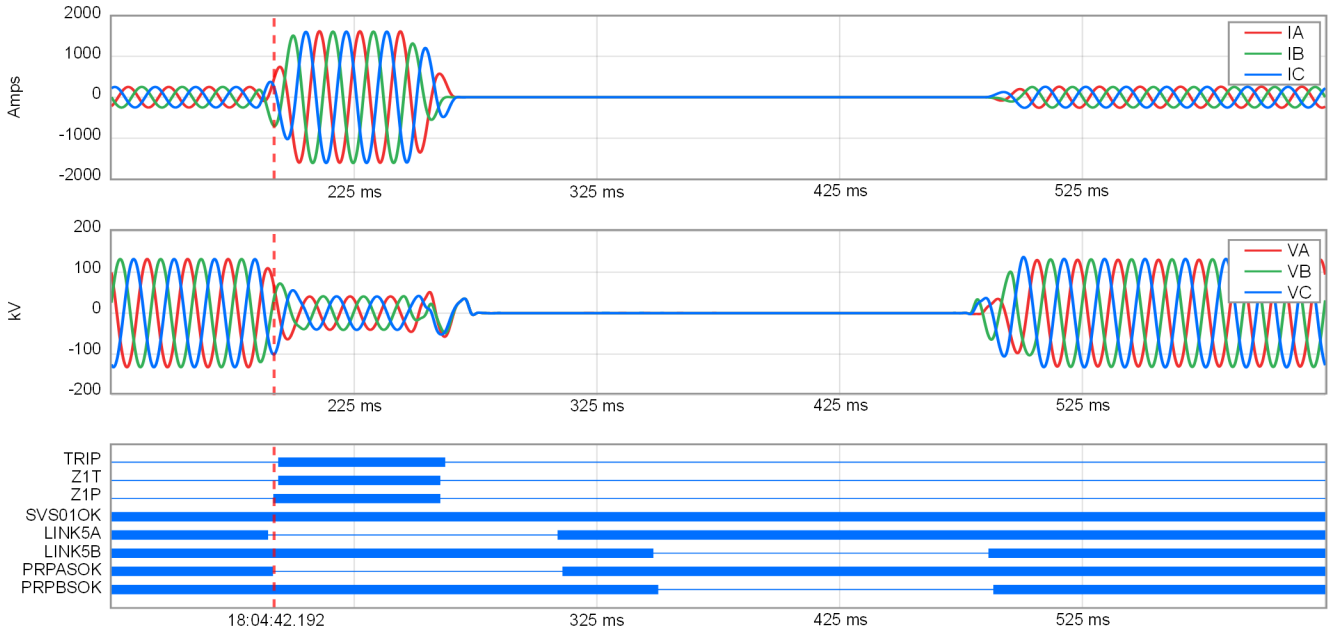


Fig. 3. Protection availability for process bus failure in a PRP network.

C. *Reliability, Redundancy, and Repair*

Reliability is a probabilistic measure that declines over time as the aging of components increases their likelihood of failure. The theory of reliability engineering defines equations that yield different reliability distributions, such as the Exponential [10] and the Weibull [11] distributions. Fig. 4 shows a reliability distributions graph adapted from IEC TR 61850-90-12 [3] covering three types of systems. The dashed blue line presents the reliability from a non-redundant system (one-out-of-one or 1oo1), the dotted yellow line presents the reliability of redundant but unrepaired system (one-out-of-two or 1oo2, no repair), while the solid orange line presents the reliability from a redundant and repaired system (1oo2, with repair). Reliability distributions represent time in multiples of the mean time to failure (MTTF), which is the reciprocal of the failure rate λ.

Rather to analyze the individual shapes from each curve, we focus on a comparative analysis. The dotted yellow line shows that the increase in reliability granted by a redundant but unrepaired system is only significant during the initial stages of its lifespan. After this period, its reliability begins to diminish. To illustrate, when MTTF equals 1, the reliability presented by the redundant but unrepaired system is only 1.5 times greater than the one of a non-redundant system, even though it involves twice as much equipment. The reliability difference between the dashed blue and dotted yellow lines gets smaller further in time, to a point where there is minor difference if the system is redundant or not. Fig. 4 shows that a redundant but unrepaired system is an ineffective design that, over time, tends to behave just as a non-redundant one.

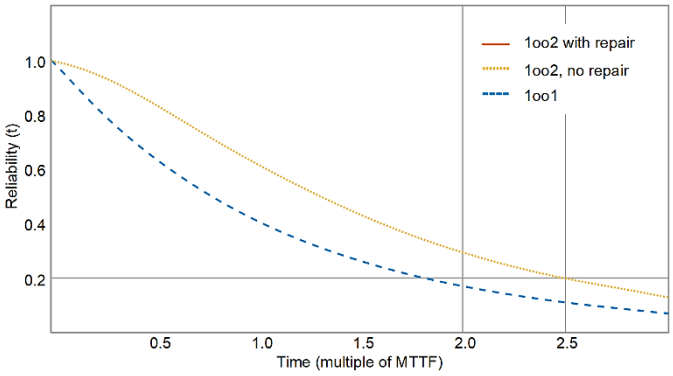


Fig. 4. Reliability over time for three types of systems.

In contrast, the solid orange line in Fig. 4 exhibits stable behavior, with reliability values near the ideal during the entire time. This is expected since repair mechanisms allow systems to revert to a state close to initial condition. From a comparison between the three lines, Fig. 4 shows that redundancy is only effective when combined with repair, which in turn is intrinsically related to monitoring capabilities. Additional information that could also be part of the graph is a line representing a single system with monitoring and repair (1oo1 with repair), which would be between the dotted yellow (1oo2, no repair) and the solid orange (1oo2 with repair), illustrating that it has superior reliability.

Despite the significance of using redundancy in combination with monitoring solutions, the design of a DSS can place a disproportional emphasis on redundancy at the expense of monitoring. This approach is due to the capacity of readily validating redundant schemes, causing failures in different parts of the communications network and verifying the absence of alarms. As stated above, the lack of alarms is an indication that the duplicates operate correctly, but also that the system is oblivious to its failures. In fact, one cannot state that the focus is on availability, because availability implies that a component is ready to operate when it is requested to. But since there is no visibility, it is impossible to ascertain whether it is available or not.

Reliability, on the other hand, is a more complete metric to evaluate a system, considering not just the capacity to withstand localized failures, but also how components perform over time. Reliability is a result of the design choices, which in the case of DSS, must combine redundancy and monitoring in the right proportions.

IV. Monitoring at the Application Level

Section III demonstrates the implications of improper monitoring in redundant systems with the example of a link failure. While the example offers a straightforward explanation, DSS can experience numerous types of failures beyond the physical layer. For example, consider a subscriber relay sporadically receiving corrupted or out-of-sequence SV messages on one of the LANs from a PRP network. It can be a result of a problem in the publishing MU or in the process bus network. Irrespective of the root source, the redundancy protocol would keep discarding the SV streams from the faulty LAN and the system would not generate any alarm so that the error could be repaired.

Redundancy protocols can provide some level of network monitoring. The PRP protocol defines the supervision frames, layer 2 messages that each participating device publishes to advertise itself in the network. If the subscribing device does not receive a supervision frame withing a time-out interval, it declares a communication failure to its pair. This functionality, however, should not be used as the sole monitoring mechanism for a communications network, especially on process bus applications. The limitation relates to the supervision interval. While a PRP device publishes supervision frames in the range of seconds, SV messages occur in the microsecond range, and GOOSE messages occur in the range of milliseconds for event messages that generate fast publications. The PRP supervision frames then provide a snapshot of the network operation only in a given instant and would not flag problems in the proposed example of transient failures in an SV stream. The supervision frames are messages that are not used by the protection applications and so only prove that those frames passed through the network to the subscriber.

To provide better coverage for critical protocol applications, it is necessary to implement the monitoring mechanism at the application layer, creating dedicated monitoring for each LAN. The implementation in the SV subscriber relay from the event report in Fig. 3 applies this solution, monitoring the SV stream

from LAN A with binary variable PRPASOK and SV stream from LAN B with PRPBSOK. The overall SV supervision that considers messages from either of the two LANs is present in the binary variable SVS1OK, where 1 refers to the first SV subscription. Similarly, the relay's implementation enables individual monitoring for GOOSE messages, indicating the status of the GOOSE application in LAN A with binary variable PRPAGOK and from LAN B with PRPBGOK.

Focusing the analysis on the SV protocol, the digital section in the event report from Fig. 3 shows that PRPASOK and PRPBSOK deassert when the respective LINK5A and LINK5B deassert. In contrast, the overall supervision SVS1OK remains asserted during the entire event. Supervision frames from PRP would not flag it, neither would the overall supervision for application-level protocols. Redundancy protocols such as PRP certainly can bring more resilience to a communications network, but the design should employ them in a way that does not hide intermittent failures for operational and maintenance teams.

In addition to the binary indications specific for each LAN, individual monitoring allows the generation of statistical data to evaluate the performance of an application over time. Further sections detail the specifics for different protocols. Based on both binary indications and statistical data, a properly designed monitoring system should be capable of answering the following questions:

1. Are messages arriving on both networks?
2. Is the availability of both networks being monitored?
3. Is the performance of both networks measured and qualified?
4. Are statistical data from both networks being stored?

V. Concept of the Monitoring System

A complete monitoring system collects information from all participating devices involved in the protection and control functions. In DSS, this encompasses protective relays, bay controllers, MUs, gateways, Ethernet switches, and GNSS clocks. It can also include equipment from WANs when they transport critical services such as line current differential (ANSI 87L) or the IEEE C37.118 synchrophasors protocol. This paper focuses on the devices involved in protection and control schemes confined to one substation, excluding the monitoring data and the integration with WAN equipment such as routers and multiplexers. Still, the solution can extend to include these devices when applicable, as they implement similar protocols as the ones verified in DSS devices.

Fig. 5 shows the conceptual idea of the monitoring system. Protection and control devices usually implement a variety of protocols that allow the integration with a monitoring platform, such as the MMS, DNP3, and SNMP. This paper focuses on the development of the monitoring system on the MMS and SNMP protocols. It describes the organizational data model from which these protocols gather a set of standardized information, highlighting applicable additional information available through the use of protocol extensions defined in the standards. The intent is to provide an interoperable solution subset that, at the same time, does not constrain the application when there is monitoring data that has not yet been standardized.

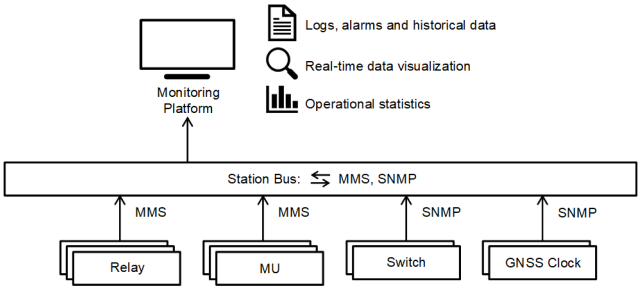


Fig. 5. Concept of the monitoring platform.

The devices and system monitor physical signals as well as application services. Physical signals include operating temperatures, link status alarms, and port activity counters. Application services include real-time machine-to-machine communications, time synchronization, and logical redundant links. With such data actively collected and stored, the monitoring platform provides real-time indication of alarms, logs, and historical data, as well as operational statistics, allowing not only the determination of the operating condition of the system in a specific instant but also its behavior over time.

The use of MMS as the client-server protocol to collect monitoring information from devices in the DSS leverages models associated with SV and GOOSE protocols used for protection and control functions, as the IEC 61850 suite of protocols share the same data object-oriented database and data model. The MMS protocol is essential to configure and monitor both protective relays and MUs using IEC 61850 methods. In turn, the SNMP protocol is commonly used for monitoring communications and timekeeping devices, such as GNSS clocks and Ethernet switches.

Whenever possible, the monitoring platform should rely on information provided by end devices, given that they are the direct participants in the protection and control system and the subscribers of the critical control services. They are the most reliable sources, providing not only protocol information, but also the result of interactions with their internal algorithms. Comparatively, the approach of mirroring messages in Ethernet switches and forwarding them to a protocol analyzer is restricted for the monitoring of network traffic, which is not sufficient for a complete monitoring application. Besides, due to possible component failures, there is no guarantee that the traffic received in the protocol analyzer is the same as what is delivered and processed on an end device.

Once the integration between the monitoring platform and all the DSS devices is completed, the next task is to present the information through human-machine interface screens in an intelligible way, organizing the large volume of data in a way that enables operation and maintenance teams to easily identify adverse conditions and to promptly respond with targeted actions to correct them. Section IX describes examples of such screens.

VI. Integrating Process Devices to Station Bus

While Section V shows logical connections from the process bus devices into the station bus, there is typically a requirement to physically segregate the networks. This segregation ensures that traffic from one network does not degrade performance from the other, which is especially useful in preventing the high-bandwidth traffic of multicast SV messages from process bus interference in the applications running on station bus. In this context, the monitoring platform that is connected to the station bus needs to have access to devices connected to both networks. This section discusses the design options available in providing such access.

A. MUs With Dedicated Interfaces

In the case when the implementation of process bus devices supports independent interfaces for each network segment, it is possible to connect the respective interface directly to the station bus, as shown in Fig. 6. This concept brings simplicity and the physical and visual segregation of the two networks is convenient for operational and maintenance teams. In addition to the monitoring capacity, it allows process bus devices to support other services present in the station bus, such as engineering access, retrieval of event reports, and integration with SCADA system. Fig. 6 shows the MMS protocol between the dedicated interfaces of the MUs and the connection to the station bus to provide these services. Besides the reporting, the protocol also supports file transfer capabilities.

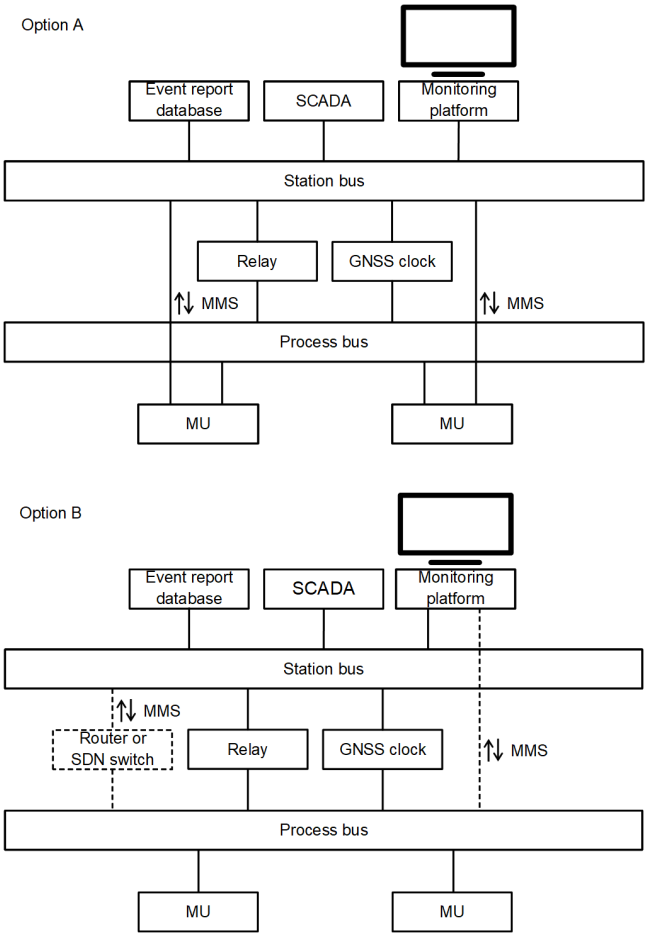


Fig. 6. Concept of the monitoring platform.

As considerations for this option, the immediate impact relates to the increase in fiber and network connections. While cables with multiple fiber strands contribute to mitigate the increase in fiber optics costs, the duplication of endpoints can increase the number of switches in the station bus. Additionally, process bus devices that do not implement a dedicated interface to station bus, such as process bus switches, present obstacles for the integration with the monitoring system.

B. MUs With Merged Interfaces

Two other options are available when the devices connected to the process bus can combine traffic from the two networks in a single communication interface or when the implementation only supports a single Ethernet interface. Fig. 6 depicts these options, identifying them as dashed lines to convey the idea that they are two independent design choices.

In one option, the monitoring platform accesses the process bus through a controlled connection between the two networks. The intermediate device implements filtering capabilities in a way that allows only monitoring, management traffic, and other intended services to pass through. IEC TR 61850-90-4 [16] describes layer 3 Ethernet routers for this task. Switches based on the concept of software-defined networking developed for operational technology environments (OT SDN) are also used in this application, with the advantage of implementing enhanced filtering capabilities [17].

This option allows reach through access from the station bus towards any process bus device, including MUs and Ethernet switches. It also reduces the number of connection endpoints, alleviating the need for additional fiber-optic cables and station bus switches. Such reductions in the number of connections and devices should be weighed against the need for additional equipment in the system and the possible challenges for maintenance and operational teams resulted from merging the network traffics in the same interface.

The second option in this scenario consists of establishing a direct link between the monitoring platform and the process bus. In doing so, it eliminates the need of an intermediate device, reduces the count of connection endpoints and fiber-optic cables, and keeps station bus traffic isolated from the process bus.

VII. IEC 61850 Monitoring Data

IEC 61850 employs specific data structures called logical nodes (LNs) to model devices and functions within the power system. In turn, the LNs are composed of a set of data objects (DOs). Fig. 7, adapted from IEC TR 61850-90-4, shows the implementation of the IEC 61850 data model in an IED with a 5-port Ethernet interface. In the figure, Ports 1 and 2 are dedicated to process bus, Ports 3 and 4 are dedicated to station bus, and Port 5 is dedicated to engineering access. If so desired, upon configuration, the interfaces can operate with process bus and station bus traffic merged in Ports 1 and 2, supporting integration options described in Section VI , when it is applied to MUs.

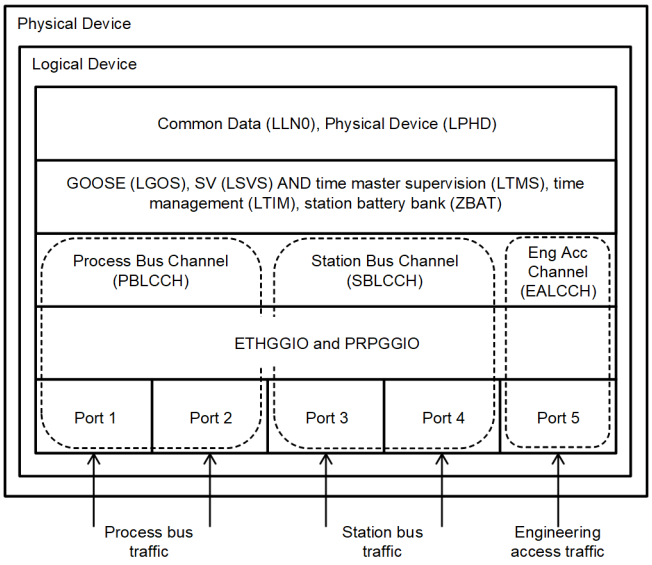


Fig. 7. Organization of the IEC 61850 data model in an IED.

It should be noted that while IEC 61850-7-4 [18] defines the LN classes and the associated mandatory and optional data objects, it allows the implementation of additional points as extension data objects as well as additional LNs based on the methods defined in the standard. Several data objects mentioned in the next sections are extensions to the standard's specific LN definitions, as well as innovative LNs such as ETHGGIO and PRPGGIO illustrated in Fig. 7. The following subsections provide a general description for each LN listed in Fig. 7. For the complete list of DOs they implement, refer to the monitoring screens examples in Section IX.

A. Physical Link

In the lower part of Fig. 7, LN ETHGGIO maps the physical link data from each of the communication interfaces, providing information about network traffic and the operation of small form-factor pluggable (SFP) modules connected to them. For instance, this LN maps binary data of link status, the activity of each port (whether it is in operation or in standby). It also maps analog data in the form of counters for number of received and transmitted packets, receive and transmit optical power (in dBm) for SFPs, and their operating temperature (in °C). This information is useful to troubleshoot communications failures, as when changes due to weather or accumulation of dust weakens fiber-optic signals in an interface. LN ETHGGIO also models a data object to reset statistics, useful during momentary assessments or after troubleshooting.

To map this type of data, LN ETHGGIO uses the generic IO (GGIO) class with a descriptive prefix to convey that it is related to the Ethernet interfaces. IEC 61850-7-4 defines the LN class LPCP to map a subset of this information. The GGIO class provides support to interoperable use of the LNs and is essential when used with the intent to uniquely and completely name and model data to be interoperable, while standards task work on the development of specific LNs.

B. Channel Link

LCCH is the next class of LN shown in Fig. 7. This LN models physical communication channels. It is different from LN ETHGGIO because it is not bound to a specific interface. The organization model from Fig. 7 uses one instance of the LN for each channel: PBLCCH models the process bus, SBLCCH models the station bus, and EALCCH models the engineering access channel. Its data objects contain information about the status of primary and backup channels, statistical data about the number of received and transmitted frames per channel, and their respective error rates.

Being one of the first LNs in the organization model from Fig. 7 to supervise logical data, it is well suited to monitor the individual applications of critical protocols. Hence, this LN implements specific data objects to supervise GOOSE and SV protocols operating in duplication in a PRP network. In this way, it provides complete visibility for the applications on each LAN and, alongside the application-level monitoring described in Section IV, prevents redundancy from hiding failures in the system.

C. GOOSE and SV Subscriptions

Higher in the organization model from Fig. 7 are the LNs related to application functions, such as GOOSE and SV subscriptions. For each subscribed GOOSE message there is an LN LGOS with information about subscription status, specific field values from incoming messages, expected values based on device configuration, and statistical data. The LN also contains error codes in the form of enumerated data that convey information about mismatching values in configured revision numbers, corrupted, out-of-sequence, or missed messages.

Similarly, for each subscribed SV message there is an LSVS LN. The two LNs have common data objects, resulting from the similarities between the protocols they map. LN LSVS implements specific data objects for the SV protocol, encompassing the synchronization state of a MU, the number of interpolated messages, enumerations regarding decoding errors, mismatched time references between streams, and excessive delays, among others. Similarly to the subscriptions, one could collect data related to the publication of GOOSE and SV messages, displaying the characteristics of the publications.

The detailed monitoring points from these two LNs assist in directing troubleshooting analysis and, as previously described, the statistical data generated for each subscription enables monitoring of their applications. At the same time, these LNs are unaware whether the received messages are unique or duplicates because the duplicates are discarded before the messages reach the applications. Supervision of each individual network is not within the scope LN LGOS and LN LSVS, necessitating a combination with other data for a complete analysis when in a redundant scheme.

Specifically, for PRP designs, the LN PRPGGIO indicates the status of the SV and GOOSE protocols on each LAN. These points are not part of the channel link supervision modeled in LN LCCH because a redundant channel link can support other types of redundancy, such as the standby redundancy with the STA/RSTP or failover implementation [19]. In this way,

problems in GOOSE and SV protocols in a PRP network are first flagged by status indications from LN PRPGGIO, with LN LCCH being involved in the further analysis for detailed information of each communication channel.

D. Time Synchronization

The monitoring of time synchronization involves two LNs, namely LN LTMS and LN LTIM. The first supervises the quality of synchronization by reporting a master clock's attributes, mapping information regarding its accuracy, identity, protocol used, and whether it is locked to a global time reference or operating in a holdover state. Beyond modeling specific information about a master clock, LN LTMS assists the correlation of system-wide events, since it is common for time synchronization to affect multiple devices, especially in a DSS [20].

Meanwhile, LN LTIM is used for monitoring time settings in an IED. For instance, this LN informs the current settings for UTC offset and for daylight saving time. Although the MMS protocol does not apply compensation factors in reporting timestamps, the information from LN LTIM is still valuable to ensure an IED is applying them to local functions, such as in timestamping Sequence of Events and Event Reports.

E. Battery Bank

The capacity to monitor the performance of the station dc voltage from a battery bank is also crucial for the purposes of a monitoring system, since the most demanding scenario for a battery bank happens during a fault in the power system. Protective relays and MUs can monitor the dc voltage levels and generate alarms when the measured values fall outside preconfigured limits.

The measurement and alarms regarding the performance of the battery bank are mapped to LN ZBAT. This LN conveys metering data for the station dc voltage and alarms for operating values within warnings or failure zones. It can also map information about ac ripple levels to supervise charging cycles and alarm indications for complete or partial ground faults when the battery system is centered around the chassis ground.

F. Physical Device

All the LNs described above reside within an IED, which is monitored through the LN LPHD. This LN maps information about an IED's operating state (whether it is enabled or disabled), hardware and firmware versions, serial number, and internal temperature.

Although the common LN LLN0 does not directly relate to physical data, IEC 61850 literature frequently cites it alongside LN LPHD, since both reside in the upper level of the hierarchy of LNs. This LN monitors and controls the mode of operation of LNs. As an example, LN LLN0 includes DOs that represent the control authority of a device, its simulation state, its operation mode (on, test, blocked, test/blocked, and off), and when those DOs are changed.

VIII. Specific Features for MUs

Among all the devices in a DSS, the MUs, or relays in the yard, operate under the most challenging conditions. Placed in the substation yard, devices experience significant variations of temperature, humidity, and other environmental factors. To illustrate the scenario, Fig. 8 shows the internal temperature changes for a 24-hour period measured by two different IEDs in a substation in the Southeast region of Brazil. The solid orange line corresponds to the temperature measurements taken by a relay installed in the substation yard (representative of an IMU), while the dashed blue line corresponds to the measurements taken by a protective relay installed in the control house.

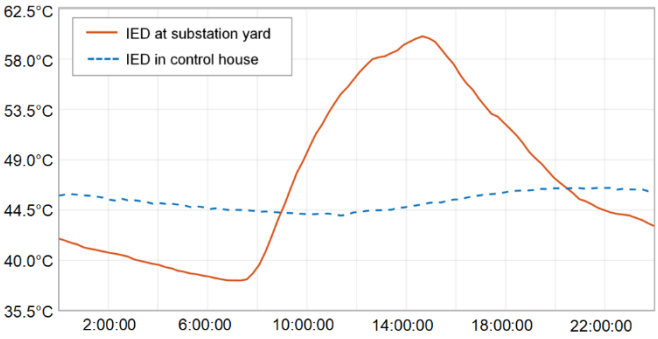


Fig. 8. Temperature variations for a relay and an MU.

Fig. 8 shows small temperature changes for the relay, stable at approximately 45°C. This is expected since it is installed a conditioned environment. The IED installed in the substation yard, however, experiences significant changes, with the solid orange line reaching the minimum of 38°C and, a few hours later, the maximum of 60°C. The changes in temperature justify the importance of thoroughly monitoring MUs. Fig. 8 reiterates the relevance of a robust, proven, and mature-MU hardware design, maintaining operation through decades while withstanding high-demanding environmental conditions.

The monitoring capability is one of the essential features for MUs when they are part of a DSS. Yet, MUs involved in non-critical applications might not require the same level of implementation. Considering this scenario, the IEC 61869-9 standard defines four conformance classes for MUs. The conformance classes are as follows [21]:

- Class A: the minimal set of services necessary to transmit MU data using SVs.
- Class B: includes Class A capabilities plus the minimal set of services necessary to support GOOSE messages.
- Class C: includes Class B capabilities plus the support for IEC 61850 series' information model self-descriptive capabilities.
- Class D: Includes Class C capabilities plus services for file transfer and either one or more of unbuffered and buffered reporting.

According to the definitions, a device that simply converts analog data and publishes it in the form of SV streams classifies as a Class A MU. However, this class lacks the necessary services for integration with a monitoring system. The same holds true for Classes B and C. Class B implements GOOSE in addition to SV, which is a protection and control service rather than a supervision protocol. Meanwhile, Class C implements

the IEC 61850 data model on top of the capabilities from Class B, which helps in the exchange of descriptive messages but is not sufficient for integration.

Though a Class C MU may include local monitoring DOs, only a Class D MU implements the necessary features for the integration with the monitoring system, combining features of all other MU classes with the implementation of buffered or unbuffered reports. In addition, Class D MUs implement file transfer services, allowing for read and write operations used in settings management and in the retrieval of event reports.

IX. Monitoring Screens

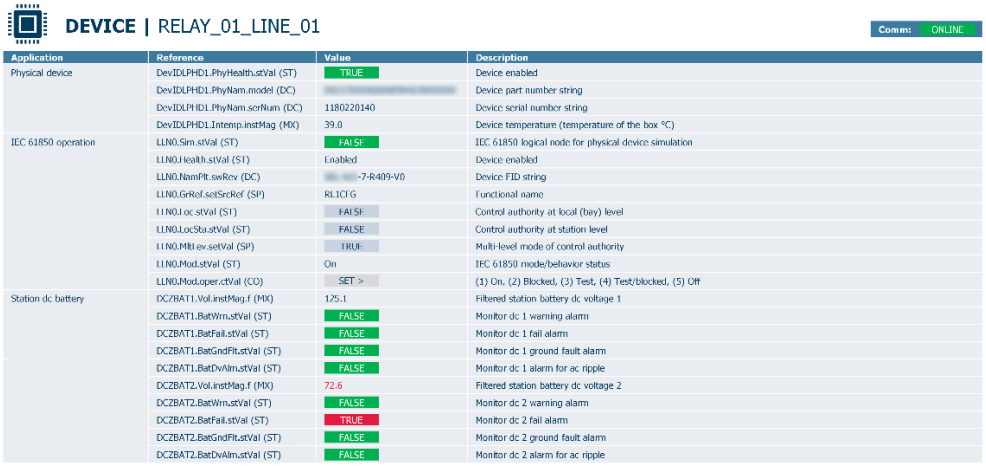
This section presents illustrative examples of how screens in a monitoring platform can be configured to display the collected data points mentioned above. While it is impractical to cover all possible operational and troubleshooting scenarios, the examples provide the fundamental concept of arranging relatively large volumes of data in a way that enables intuitive operation and facilitates the identification of alarming conditions.

A. Physical Device

Fig. 9 shows the monitoring screen related to the physical and operational data of a protective relay, with all parameters related to the physical data and IEC 61850 operation modes in normal conditions. On the other hand, the example indicates an alarm based on the station dc voltage from one of the redundant battery banks. The reduced value of for the dc measurement is below the low-fail threshold limit, configured to 80 percent of the 125 Vdc nominal operating voltage. In this example, the battery system is centered around chassis ground and the alarming condition is caused by the positive terminal partially shorted to the chassis ground. In this condition, the system also asserts the ground fault alarm.

B. GOOSE and SV Matrices

In addition to the monitoring of individual devices, it is possible to display the status of the critical communications between them in the form of matrices. Fig. 10 shows an example of a GOOSE matrix for a DSS composed of MUs and different types of protective relays. In the example, each device publishes one GOOSE message destined for protection and another for control functions. The matrix shows the status of each subscription and provides a visual and comprehensive indication of the operating conditions of the system. In the example, the transformer Relay 04 indicates a failed subscription to the protection GOOSE messages published by MU 05. The same concept of monitoring screen applies to other multicast services, such as the exchange of SV messages between MUs and subscriber relays.



Application	Reference	Value	Description
Physical device	DevIDLPHD1.PhyHealth.stVal (ST)	TRUE	Device enabled
	DevIDLPHD1.PhyNam.model (DC)	[redacted]	Device part number string
	DevIDLPHD1.PhyNam.serNum (DC)	1180220140	Device serial number string
	DevIDLPHD1.Intemp.instMag (MX)	39.0	Device temperature (temperature of the box °C)
IEC 61850 operation	LLN0.Sim.stVal (ST)	FALSE	IEC 61850 logical node for physical device simulation
	LLN0.Health.stVal (ST)	Enabled	Device enabled
	LLN0.NamPlt.swRev (DC)	[redacted]-7-R409-V0	Device FID string
	LLN0.GrRef.setSrcRef (SP)	RL1CTG	Functional name
	LLN0.Loc.stVal (ST)	FALSE	Control authority at local (bay) level
	LLN0.LocSta.stVal (ST)	FALSE	Control authority at station level
	LLN0.MltLev.setVal (SP)	TRUE	Multi-level mode of control authority
	LLN0.Mod.stVal (ST)	On	IEC 61850 mode/behavior status
	LLN0.Mod.oper.ctVal (CO)	SET >	(1) On, (2) Blocked, (3) Test, (4) Test/blocked, (5) Off
Station dc battery	DCZBAT1.Vol.instMag.f (MX)	125.1	Filtered station battery dc voltage 1
	DCZBAT1.BatWrn.stVal (ST)	FALSE	Monitor dc 1 warning alarm
	DCZBAT1.BatFail.stVal (ST)	FALSE	Monitor dc 1 fail alarm
	DCZBAT1.BatGndFlt.stVal (ST)	FALSE	Monitor dc 1 ground fault alarm
	DCZBAT1.BatDvAlm.stVal (ST)	FALSE	Monitor dc 1 alarm for ac ripple
	DCZBAT2.Vol.instMag.f (MX)	72.6	Filtered station battery dc voltage 2
	DCZBAT2.BatWrn.stVal (ST)	FALSE	Monitor dc 2 warning alarm
	DCZBAT2.BatFail.stVal (ST)	TRUE	Monitor dc 2 fail alarm
	DCZBAT2.BatGndFlt.stVal (ST)	FALSE	Monitor dc 2 ground fault alarm
	DCZBAT2.BatDvAlm.stVal (ST)	FALSE	Monitor dc 2 alarm for ac ripple

Fig. 9. Device monitoring screen.

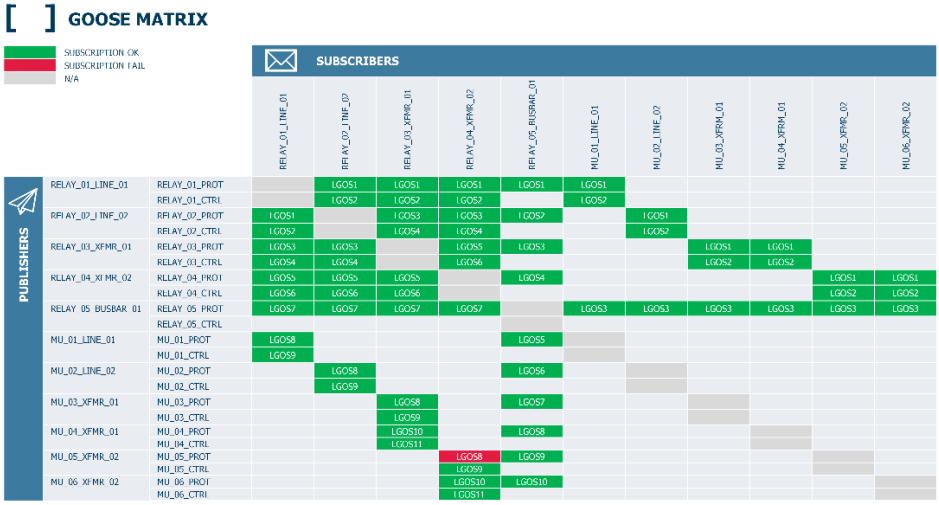


Fig. 10. GOOSE matrix monitoring screen.

C. *GOOSE Subscription*

From the GOOSE matrix example, the monitoring platform can be configured to direct the user to a screen with further details for the specific subscription. Fig. 11 shows an example of a GOOSE subscription screen considering the scenario mentioned above. The data show a failed reception status with an error code of corrupted message, which is an indication that the content inside the data set of the received GOOSE messages does not meet the subscriber's configuration. While the failed condition persists, the statistics of cumulative and maximum continuous inactive time keep increasing and can be cleared once the problem is solved.

GOOSE SUBSCRIPTION | RELAY_04_XFMR_02 (MU05CFG/LLN0.MU05_GOO_PB) — Comm: ONLINE

Application	Reference	Value	Description
Message information	LGOS5.GoCBRef.setSrcRef (SP)	MU05CFG/LLN0.MU05_GOO_PB	Control block reference
	LGOS5.DatSet.setSrcRef (SP)	MU05CFG/LLN0.GOO_PB	Dataset reference
	LGOS5.GoID.setVal (SP)	MU05CFG	GOOSE identification
	LGOS5.Addr.setVal (SP)	01-0C-CD-01-00-10	Multicast MAC address
	LGOS5.VlanID.setVal (SP)	100	VLAN identification
	LGOS5.VlanPri.setVal (SP)	4	VLAN priority
	LGOS5.AppID.setVal (SP)	4112	Configured APPID
Reception status	LGOS5.St.stVal (ST)	FALSE	Reception status
	LGOS5.ErrSt.stVal (ST)	MSG CORRUPTED	Reception error code
	LGOS5.SimSt.stVal (ST)	FALSE	Processed simulation message
	LGOS5.LastStNum.stVal (ST)	1608	Last state number (StNum) received
	LGOS5.LastSqNum.stVal (ST)	55932	Last sequence number (SqNum) received
	LGOS5.ConfRevNum.stVal (ST)	1	Expected ConfRef
	LGOS5.RxConfRevNum.stVal (ST)	1	Received ConfRef
	LGOS5.NdsCom.stVal (ST)	FALSE	Needs commissioning
Subscription statistics	LGOS5.TotDwnTm.instMag.f (MX)	3998.795	Cumulative inactivity time (s)
	LGOS5.MaxDwnTm.instMag.f (MX)	2520.615	Maximum continuous inactivity time (s)
	LGOS5.OosCnt.stVal (ST)	1	Number of messages received out of sequence (OOS)
	LGOS5.TalCnt.stVal (ST)	1	Number of "time to live" violations detected
	LGOS5.DecErrCnt.stVal (ST)	0	Number of messages with decoding failures
	LGOS5.BufOvflCnt.stVal (ST)	0	Number of messages lost because of buffer overflow
	LGOS5.MsgLosCnt.stVal (ST)	22	Estimated maximum number of messages lost due to messages received out of sequence
	LGOS5.MaxMsgLos.stVal (ST)	22	Estimated total number of messages lost due to messages received out of sequence
	LGOS5.RsStat.t (ST)	2023-07-10-16:53:27.820700	Last reset of stats
	LGOS5.RsStat.Oper.ctlVal (CO)	RESET >	Reset reception statistics (command)

Fig. 11. GOOSE subscription screen.

PROCESS BUS | RELAY_01_LINE_01 — Comm: ONLINE

Application	Reference	Value	Description
Process bus statistics	PBLCCH1.NetMode.setVal (SP)	PRP	Port 5 network operating mode setting
	PBLCCH1.BusModP.setVal (SP)	Independent	Port 5 bus operating mode setting
	PBLCCH1.NetPorP.setVal (SP)	A	Port 5 primary network port setting
	PBLCCH1.ChLiv.stVal (ST)	TRUE	Status of primary channel
	PBLCCH1.RedChLiv.stVal (ST)	FALSE	Status of redundant channel
	PBLCCH1.RxCnt.actVal (ST)	0	Number of non-SV, non-GOOSE frames received on the primary channel
	PBLCCH1.RedRxCnt.actVal (ST)	0	Number of non-SV, non-GOOSE frames received on the redundant channel
	PBLCCH1.RxCntGo.actVal (ST)	3563149	Number of GOOSE frames received on the primary channel
	PBLCCH1.RedRxCntGo.actVal (ST)	3562420	Number of GOOSE frames received on the redundant channel
	PBLCCH1.RxCntSv.actVal (ST)	2803676774	Number of SV frames received on the primary channel
	PBLCCH1.RedRxCntSv.actVal (ST)	2803257532	Number of SV frames received on the redundant channel
	PBLCCH1.TxCnt.actVal (ST)	5350582	Number of frames transmitted on both channels
	PBLCCH1.FerCh.stVal (ST)	0	Number of non-SV, non-GOOSE PRP frames missed on the primary channel over the last 1000 processed PRP frames
	PBLCCH1.RedFerCh.stVal (ST)	0	Number of non-SV, non-GOOSE PRP frames missed on the redundant channel over the last 1000 processed PRP frames
	PBLCCH1.FerChGo.stVal (ST)	0	Number of GOOSE PRP frames missed on the primary channel over the last 1000 processed PRP frames
	PBLCCH1.RedFerChGo.stVal (ST)	166	Number of GOOSE PRP frames missed on the redundant channel over the last 1000 processed PRP frames
	PBLCCH1.FerChSv.stVal (ST)	0	Number of SV PRP frames missed on the primary channel over the last second
	PBLCCH1.RedFerChSv.stVal (ST)	10602	Number of SV PRP frames missed on the redundant channel over the last second
	PBLCCH1.RsStat.stVal (ST)	2023-7-11-13:17:31.6002	Status of statistics reset
	PBLCCH1.RsStat.Oper.ctlVal (CO)	RESET >	Reset Ethernet card statistics
Parallel Redundancy Protocol	PRPGGIO1.Ind01 (ST)	TRUE	PRP port 5A GOOSE status
	PRPGGIO1.Ind05 (ST)	TRUE	PRP port 5A SV status
	PRPGGIO1.Ind02 (ST)	FALSE	PRP port 5B GOOSE status
	PRPGGIO1.Ind06 (ST)	FALSE	PRP port 5B SV status
Interface port 5A statistics	ETHGGIO.Ind03.stVal (ST)	TRUE	Port 5B ready
	ETHGGIO.Ind04.stVal (ST)	TRUE	Link status of port 5B connection
	ETHGGIO2.CntVal02.actVal (ST)	15459	Total number of packets transmitted on port 5B
	ETHGGIO2.CntVal07.actVal (ST)	66002049	Total number of packets received on port 5B
	ETHGGIO2.CntVal12.actVal (ST)	0	Total number of packets discarded on port 5B
	ETHGGIO2.CntVal17.actVal (ST)	0	Total number of erroneous packets received on port 5B
	ETHGGIO2.AnIn02.instMag.f (MX)	-19.8	SFP transceiver receive power info (dBm) on port 5B
	ETHGGIO2.AnIn07.instMag.f (MX)	-17.0	SFP transceiver transmit power info (dBm) on port 5B
	ETHGGIO2.AnIn12.instMag.f (MX)	44.2	SFP transceiver temperature info (°C) on port 5B
	ETHGGIO2.SPCSO01.Oper.ctlVal (CO)	RESET >	Reset Ethernet card statistics
Interface port 5B statistics	ETHGGIO.Ind03.stVal (ST)	FALSE	Port 5B ready
	ETHGGIO.Ind04.stVal (ST)	FALSE	Link status of port 5B connection
	ETHGGIO2.CntVal02.actVal (ST)	15462	Total number of packets transmitted on port 5B
	ETHGGIO2.CntVal07.actVal (ST)	66002047	Total number of packets received on port 5B
	ETHGGIO2.CntVal12.actVal (ST)	2	Total number of packets discarded on port 5B
	ETHGGIO2.CntVal17.actVal (ST)	0	Total number of erroneous packets received on port 5B
	ETHGGIO2.AnIn02.instMag.f (MX)	0	SFP transceiver receive power info (dBm) on port 5B
	ETHGGIO2.AnIn07.instMag.f (MX)	0	SFP transceiver transmit power info (dBm) on port 5B
	ETHGGIO2.AnIn12.instMag.f (MX)	40.0	SFP transceiver temperature info (°C) on port 5B
	ETHGGIO2.SPCSO01.Oper.ctlVal (CO)	RESET >	Reset Ethernet card statistics

Fig. 12. Process bus monitoring screen.

D. *Process Bus and Station Bus*

Fig. 12 shows the process bus screen for Relay 01, also listed among the devices from the GOOSE matrix. The relay is operating a PRP mode, with a failed connection in the interface with LAN B. In the PRP statistics, there are alarms for the status of the LAN B (in the figure referred to as redundant channel), as well as highlighted counters indicating abnormal values for missed GOOSE and SV messages in the redundant channel. It is essential to comprehend that this degraded scenario does not generate any alarms in the GOOSE matrix from Fig. 10. As previously discussed, the duplication method ensures the continuous delivery of GOOSE messages through LAN A but inhibits the application from recognizing failures in the communications network. Because of this, it is recommended to implement one GOOSE and one SV matrix for each LAN of a PRP network, or to use different colors to provide indications of independent failures in the same matrix. In this scenario, the individual monitoring of each protocol with LN PRPGGIO allows the identification of the existing failure and the complete visibility sought after by the monitoring system.

E. *Time Synchronization*

Fig. 13 depicts the time-synchronization data related to the quality of the master clock and to the time management for a MU. All data points show normal operating condition, with the device synchronized with a time accuracy greater than 1 microsecond and traceable to the GPS time source. The last data point for LN LTMS provides an analog indication of the quality of the time synchronization by quantifying the interval between two consecutives synchronization messages. In the figure, the value of 999.9998 milliseconds between two consecutive pulses translates into a variation of 200 nanoseconds, which is within the high-accuracy limit of 1 microsecond reported.

TIME SYNC | MU_03_LINE_02 — Comm: ONLINE

Application	Reference	Value	Description
Time master supervision	LTMS.TmAcc.stVal (ST)	20 (1 us accuracy)	Number of significant bits in the second fraction
	LTMS.TmSrc.stVal (ST)	GPS	Time source used by the clock (timeSource as per IEEE-1588)
	LTMS.TmSrcTyp.stVal (ST)	3 (PTP)	Timing source type (IRIG-B, PTP, SNTP, or Unknown)
	LTMS.TmSyn.stVal (ST)	3 (GlobalAreaClock)	Timing source traceability (Global, Local, or Internal)
	LTMS.TmSynLkd.stVal (ST)	1 (External)	Clock synchronization status (external or holdover)
	LTMS.TmTosPer.instMag.f (MX)	999.9998	Duration between two consecutive points at the top of the second (ms)
Time management	LTIM.TmDT.stVal (ST)	FALSE	Indicates daylight-saving time is currently in effect at the IED location
	LTIM.TmOfsTmm.setVal (ST)	-480	Offset of local time from UTC in minutes
	LTIM.TmUseDT.setVal (ST)	FALSE	Set to True if daylight-saving time is enabled
	LTIM.TmChgDT.setTm (ST)	N/A	Local time of next change to daylight-saving time
	LTIM.TmChgST.setTm (ST)	N/A	Local time of next change to standard time

Fig. 13. Time-synchronization monitoring screen.

Application	Reference	Value	Description
Satellite status	1.3.6.1.4.1.31823.1.2488.2.3.1.4.1.4.1	0	GPS used
	1.3.6.1.4.1.31823.1.2488.2.3.1.4.1.3.1	0	GPS visible
	1.3.6.1.4.1.31823.1.2488.2.3.1.4.1.4.2	0	GLONASS used
	1.3.6.1.4.1.31823.1.2488.2.3.1.4.1.3.2	0	GLONASS visible
Time input	1.3.6.1.4.1.31823.1.2488.2.4.1.5.1.2.1	Holdover	Source 1
	1.3.6.1.4.1.31823.1.2488.2.4.1.5.1.2.2	-	Source 2
	1.3.6.1.4.1.31823.1.2488.2.4.1.5.1.3.1	< 213 ns	Quality source 1
	1.3.6.1.4.1.31823.1.2488.2.4.1.5.1.3.2	-	Quality source 2
	1.3.6.1.4.1.31823.1.2488.2.4.1.2.0	- 08:00	Local time offset
	1.3.6.1.4.1.31823.1.2488.2.4.1.3.0	Off	Daylight saving time status
Precision Time Protocol	1.3.6.1.4.1.31823.1.2488.2.6.1.1.1.1.1	00:30:A7:FF:FE:17:CB:B8	ETH1 clock identity
	1.3.6.1.4.1.31823.1.2488.2.6.1.1.1.1.2	00:30:A7:FF:FE:17:CB:B9	ETH2 clock identity
	1.3.6.1.4.1.31823.1.2488.2.6.1.1.1.1.3	00:30:A7:FF:FE:17:CB:BA	ETH3 clock identity
	1.3.6.1.4.1.31823.1.2488.2.6.1.1.1.1.4	00:30:A7:FF:FE:17:CB:BB	ETH4 clock identity
System statistics	1.3.6.1.4.1.31823.1.2488.2.7.1.1	45%	CPU usage
	1.3.6.1.4.1.31823.1.2488.2.7.1.2	21%	RAM usage
	1.3.6.1.4.1.31823.1.2488.2.7.1.3	40%	Storage capacity
	1.3.6.1.4.1.31823.1.2488.2.7.1.7	8d 4h 26m 25s	System uptime
Hardware diagnostics	1.3.6.1.4.1.31823.1.2488.2.2.1.9	52°C	Temperature
	1.3.6.1.4.1.31823.1.2488.2.2.1.1	OK	Antenna
	1.3.6.1.4.1.31823.1.2488.2.2.1.10.1.3	OK	GNSS Receiver A
	1.3.6.1.4.1.31823.1.2488.2.2.1.10.1.3	OK	GNSS Receiver B
	1.3.6.1.4.1.31823.1.2488.2.2.1.2	OK	Holdover Clock
	1.3.6.1.4.1.31823.1.2488.2.2.1.3	OK	RAM
	1.3.6.1.4.1.31823.1.2488.2.2.1.4	OK	FLASH
	1.3.6.1.4.1.31823.1.2488.2.2.1.5	OK	FPGA
	1.3.6.1.4.1.31823.1.2488.2.2.1.6	OK	Clock
	1.3.6.1.4.1.31823.1.2488.2.2.1.7	OK	Clock Battery
	1.3.6.1.4.1.31823.1.2488.2.2.1.8	OK	LCD

Fig. 14. GNSS clock monitoring screen.

F. GNSS Clocks

Fig. 14 depicts the monitoring screen for a GNSS clock distributing time as a PTP master in the scenario when it loses satellite references and enters the holdover operation. In this state, the generation of time-synchronization pulses gradually deviates from the absolute time reference, with the drift rate dependent on the quality of the internal oscillator. The figure shows alarms for the absence of visible satellites and, consequently, the lack of a satellite lock. It maintains the remaining indications in a normal state as they are still within operational requirements for a DSS-based application where the GNSS clock participates. The normal status for the antenna indicates that the hardware receiver is healthy, and the loss of satellite lock is likely due to external factors.

G. Ethernet Switches

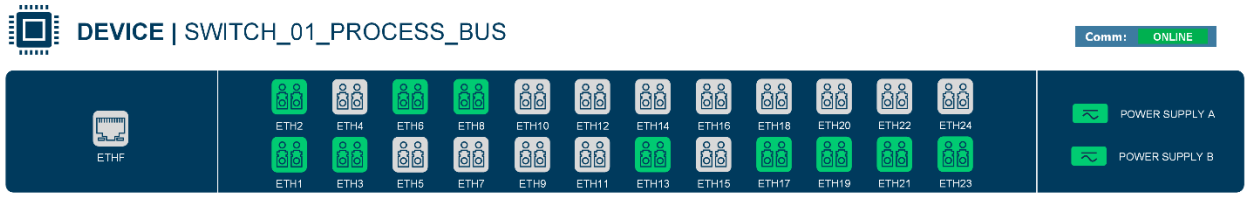
Lastly, Fig. 15 shows the monitoring screen for Ethernet switches, containing information about the operative state and the percentage of bandwidth utilization for each port. The information about the percentage utilization can help in identifying communication problems like the existence of unmanaged network loops that can quickly escalate to affect large portions of the network. The screen in Fig. 15 shows the monitoring points for an SDN switch, which can manage network loops efficiently from a centralized configuration tool. In the case of traditional Ethernet switches, the screen can also display information about STA/RSTP's operative state for each port, whether it operates in discarding, learning, or forwarding mechanisms.

X. Conclusion

In the past, protective and control devices were considered silent sentinels of the power system. Modern devices in a DSS provide important information about the performance and status of a network, and consequently, about the protection scheme, even when there are no disturbances in the power system. By collecting their information, monitoring solutions can provide system-level visibility, becoming an essential component of a DSS.

Choosing from the great amount of available data and methods to collect such information can be a challenging task. The solution described in this paper serves as a reference in this effort with contributions based on a monitoring platform for a DSS. It shows the monitoring information on a per-device level, describes how the information is modeled, and which protocols are used to collect them. It further describes how system diagnostics can help troubleshooting contingencies on a DSS.

Monitoring solutions also play a crucial role in the context of redundant schemes. In the absence of monitoring, failures in unmonitored components remain hidden, creating an inaccurate perception of availability that might only be uncovered when a second failure affects the application, or when the protection and control system is called to the action and it fails, making the redundancy ineffective. Conversely, monitoring each component of a redundant scheme enables prompt repair or, at least, enabling remedial actions while waiting for the proper fix, significantly increasing the reliability levels of the protection and control system, and, consequently, of the power system.



Application	Port	RX%	TX%
Port utilization	ETH1	10.44	0.00
	ETH2	10.44	0.00
	ETH3	10.44	0.00
	ETH4	0.00	0.00
	ETH5	0.00	0.00
	ETH6	10.44	0.00
	ETH7	0.00	0.00
	ETH8	10.44	0.00
	ETH9	0.00	0.00
	ETH10	0.00	0.00
	ETH11	0.00	0.00
	ETH12	0.00	0.00

Application	Port	RX%	TX%
Port utilization	ETH13	0.00	20.87
	ETH14	0.00	0.00
	ETH15	0.00	0.00
	ETH16	0.00	0.00
	ETH17	0.00	20.87
	ETH18	0.00	0.00
	ETH19	0.00	52.20
	ETH20	0.00	0.00
	ETH21	0.00	31.32
	ETH22	0.00	0.00
	ETH23	0.00	20.87
	ETH24	0.00	0.00

Fig. 15. Ethernet switch monitoring screen.

XI. References

[1] J. L. Blackburn and T. J. Domin, *Protective Relaying: Principles and Applications*, 4th ed., CRC Press, Boca Raton, FL, 2014.

[2] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

[3] IEC 61850-90-12, Communication networks and system for power utility automation - Part 90-12: Wide area network engineering guidelines, 2015.

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

[5] IEC 61850-8-1, Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, 2011.

[6] IEEE 1588, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 2019.

[7] RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, 2002.

[8] IEEE 1815, IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3), 2012.

[9] IEEE Std C37.100, IEEE Standard Definitions for Power Switchgear, 1992.

[10] IEEE Std 802.1w, IEEE Standard for Local and Metropolitan Area Networks - Media Access Control (MAC) Bridges - Amendment 5: Rapid Spanning Tree Protocol (RSTP), 2004.

[11] R. Schloss, S. Manson, S. Raghupathula, and T. Maier, "PacifiCorp's Jim Bridger RAS: A Dual Triple Modular Redundant Case Study," presented at the 11th Annual Western Power Delivery Automation Conference, 2009.

[12] IEC 62439-3, Industrial communication networks - High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). Geneva, 2012.

[13] A. McDonald, A. Dolezilek, and D. Dolezilek, "Hidden in Plain Sight: Anticipating and Avoiding Hidden Failures in Communications-Assisted Protection," presented at the 47th Annual Western Protective Relay Conference, 2020.

[14] V. P. Singh, *Entropy-Based Parameter Estimation in Hydrology*. Springer, 1998.

[15] W. Weibull, "A Statistical Distribution Function of Wide Applicability," *Journal of Applied Mechanics*, 18, 293—297, Stockholm, Sweden, 1951.

[16] IEC TR 61850-90-4, Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines, 2020.

[17] D. Shaffer and D. Thewlis, "Solving Performance and Cybersecurity Challenges in Substation and Industrial Networks With Software-Defined Networking," presented at the 7th Annual PAC World Americas Conference, 2020.

[18] IEC 61850-7-4, Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible LN classes and data object classes, 2010.

[19] D. Dolezilek, J. Dearien, and A. Kalra, "Design and Validation Practices for Ethernet Networks to Support Automation and Control Applications," presented at the 6th Annual Protection, Automation and Control World Conference, Glasgow, United Kingdom, 2015.

[20] B. Smyth, M. Rensburg, and M. Rajasekaran, "It's About Time—Considerations and Requirements for DSS and Line Current Differential Applications," presented at the 76th Annual Georgia Tech Protective Relaying Conference, 2023.

[21] IEC 61869-9, Instrument transformers - Part 9: Digital interface for instrument transformers, 2016.

XII. Biographies

Adilson Kotryk served as a lead engineer at Companhia Paranaense de Energia Distribuição from 2002 to 2012. During that time, he completed his specialization degree in protection of electrical power systems from Universidade Federal de Itajubá, Brazil. In the same year, he was promoted to the position of senior engineer. Additionally, he obtained a specialization degree in occupational safety from Centro Federal de Educação Tecnológica do Paraná in 2003.

Eduardo Goncalves earned his BSEE in electrical engineering from Federal University of Itajubá in 2014. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in the same year, where he has taken numerous roles as project engineer, application engineer, and SEL University instructor. He earned the specialization degree in power systems automation in 2021 from National Telecommunications Institute, in Brazil. In 2023, he transferred to Pullman, Washington, to join the research and development division where he works as a lead integration & automation engineer.

Ricardo Abboud received his BSEE degree in electrical engineering from Universidade Federal de Uberlândia, Brazil, in 1992. In 1993, he joined CPFL Energia as a protection engineer. In 2000, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as a field application engineer in Brazil, assisting customers in substation protection and automation. In 2005, he became the field engineering manager, and in 2014, he became the engineering services manager. In 2016, he transferred to the SEL headquarters in Pullman as an international technical manager. In 2019, he joined SEL University as a professor, and he is currently a fellow engineer with SEL Engineering Services, Inc. (SEL ES). He is a senior member of IEEE.

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

Paulo Lima received his BSEE in electrical engineering from Universidade Federal de Itajubá, Brazil in 2012. In 2013, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as a protection application engineer in Brazil. In 2018, he became application engineering group coordinator and has been the regional technical manager for Brazil since 2020. He has experience in application, training, integration, and testing of digital protective relays. He also provides technical writing and training associated with SEL products and SEL University.

Vinicius Ferrari earned a BSEE in electrical engineering from Centro Universitário Salesiano São Paulo in 2015, with a specialization in electrical systems automation from Instituto Nacional de Telecomunicações in 2019. He joined Schweitzer Engineering Laboratories, Inc. (SEL) the same year, contributing as an application engineer and SEL University instructor. Vinicius has expertise in industrial power system studies and substation automation.