Applying Digital Secondary Systems to Optimize Power System Reliability

John Bettler, *Commonwealth Edison*
David Dolezilek, David Bowen, Shawn Westervelt, and Josh LaBlanc, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—In digital secondary systems (DSSs), programmable electronic devices are being deployed among primary equipment. Locating devices in the yard reduces traditional control circuitry copper wiring and replaces it with fiber-optic cables to communicate information to relays in the control building. Though all must meet safety, electromagnetic immunity, and environmental standards, various electronic devices allow differing levels of digitization, analog-to-digital conversion (ADC), and digitalization, replacing traditional protection and control with digital processes and communications. Electronic devices are described by the IEEE Working Group K15 based on their capabilities, such as the:**

- **Merging unit (MU)—performs ADC via hardwired connections to instrument transformers and publishes digitized protection signals.**
- **Remote input/output (I/O), process interface unit, and process interface device—perform ADC via hardwired connections to field sensors, publishes digitized binary protection signals, subscribes to digitized signals from other devices, and performs digital to hardwired output terminals to actuate digital or analog field controls.**
- **Intelligent MU (IMU)—performs ADC; publishes and subscribes to digitized communications; performs and actuates field controls; and performs digitalization of protection, automation monitoring, and control functions.**

With the integration of large quantities of inverter-based generation sources, such as wind, solar, and battery storage, power system reliability requirements are ever increasing to the electric power system. To improve power system reliability, power system protection and control system designs must isolate faulted segments at faster speeds and with better selectivity. Monitoring systems must proactively detect failing equipment before the failing equipment generates a fault or is a contributing element to a larger than necessary operation.

This paper analyzes the design of DSSs and the impacts a design has on the reliability and performance of an electric power system. The design of various DSS applications will be reviewed, including point-to-point architecture and IEC 61850-9-2-compliant applications using MU, remote I/O, and IMU electronic devices.

I. Introduction

The digitization of power system primary equipment includes the analog-to-digital conversion (ADC) of power system values, status, and alarms to use as data sources for logic within digital devices. Digitization also includes ADC to create analog signals to actuate and operate the primary system. Together, these devices create a digital secondary system (DSS) that operates the primary system. Intelligent protection devices mounted at the primary equipment perform ADC on input signals, execute digital protection and automation logic, and then create output signals. Rather than performing all necessary data collection, protection and automation logic, and signal output within one device, the tasks are often shared by several digital devices that share digitized power system and protection signals via the process bus (PB), which is named so because it is designed for transferring process-level signals among devices to operate the process; PB protocols are publish and subscribe machine-to-machine (M2M) protocols. Many of these devices also have the capability of performing process logic and recording information relating to their health and behavior as well as that of the primary equipment. Therefore, these devices also support station bus (SB) connections to accept settings and commands and send information, including engineering data, equipment reports, and fault event records.

First principles of the understanding and controlling process level functions rarely change and, based on the focus of the utility, require the careful selection of materials, equipment, systems, and features. It is essential to maximize safety, reliability, quality, and performance while managing the lowest acceptable life cycle cost and risk of failure. Because of the ongoing development of innovative technologies, these first principles of physical phenomena and processes remain constant, but the best-known methods to design, deploy, and manage control and protection systems change frequently. DSS harmonizes protection and control with more complete information about the health and behavior of the primary and secondary systems and provides mechanisms for the information to be used by other parts of the business. The digitization of secondary systems allows utilities to anticipate and use this information.

IEC 61850 standardizes several modern and popular PB protocols, so that regardless of what other protocols and features digital devices support, these few can be interoperable among devices from numerous product lines and multiple suppliers.

IEC 61850 defines the primary system as a "common term for all power system equipment and switchgear" and the secondary system as "the interaction set of all components and systems in the substation for operation, protection, monitoring, of the primary system. In case of full application of numerical technology, the secondary system is synonymous with the substation automation system" [1]. Large-scale protection and control upgrades and new construction provide opportunities to use digital technologies close to the primary equipment and, thus, use fiber cables to replace long lengths of copper wires. As recent as the 1990s, DSS digital communications standardization was limited to protocols standardized by the supplier, IEC 60870-5-101, and the related distributed network protocol (DNP3) that are standards limited to communications associated with electric power system telecommunications, teleprotection, and telecontrol. These proprietary protocols standardized by suppliers and committee standards allowed compatibility among suppliers; at that time, the committee-based ones relied on moving anonymous data referenced by memory locating, indexing, and manually defining data and information exchanged using serial telecontrol channel interfaces between data-terminating equipment and data communications equipment.

Packetized Ethernet is the method adopted by IEC 61850 to define client-server, human-to-machine (H2M), machine-to-machine (M2M), and peer-to-peer (P2P) protocols. Applications rely on the use of IEEE 802.1p priority, IEEE 802.1Q virtual local-area network (VLAN), and software-defined segregation methods. To enable interoperability among suppliers, IEC 61850 assures backward and forward compatibility, solution flexibility, and durability by enforcing that the defined methods coexist with other methods not defined by IEC 61850, including hardwiring field contacts, nonproprietary (DNP3), and proprietary Mirrored Bits communications. IEEE 802.1 Ethernet defines generic connections where messages are published into the Ether [2], without device hardware flow control, where Ethernet switches use "best-effort" buffer, store, and forward methods to send them toward their destination(s). Because the standard enforces technical coexistence, other methods that have evolved over the past 20 years including Modbus, DNP3, Mirrored Bits communications, IEEE 1588 precision time protocol, and IEC 62439 parallel redundancy protocol remain interoperable with IEC 61850.

The definition and standardization of power system digitization of the primary system process level based on IEC 61850 methods began in the late 1990s within Working Group 12 of the IEC Technical Committee 57. At the time, it was expected that power system primary equipment would be developed that was capable of direct digitization, including current transformers (CTs) and voltage transformers. These nonconventional instrument transformers (NCIT) were initially expected to publish digital messages containing raw Sampled Values (SV) of currents and voltages over direct cable to relays. Though digital relays installed in the yard were in use as early as 1997, production-quality NCITs were not produced as expected. To maintain momentum with the IEC 61850 PB as well as SB activities, the standards body chose to pivot and adopt the existing industry practice of placing nonprotection-capable digital devices near the primary equipment to perform the ADC, publish messages based on input signals, and accept messages to create output signals. PB protocols to transfer digitized temperatures; other substation analogs; and Mirrored Bits communications transferring status, alarms, and processed analog values were already in use at this time. These merging units (MUs) became the model for PB devices to transfer processed analogs, slow-changing analog samples, status, alarms, controls, and interlocks. The IEC 61850 SV Protocol, defined in Part 9-1, became a feature of MUs as an alternative to NCITs via unidirectional serial P2P links, as illustrated in Fig. 1.

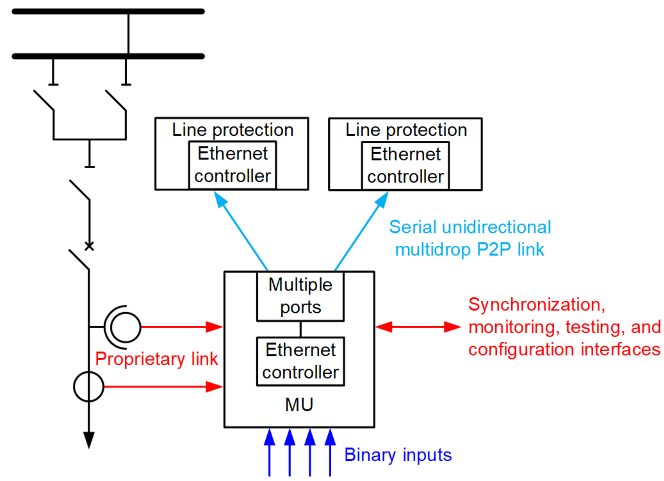

Fig. 1. Illustration of IEC 61850-9-1 MU with unidirectional serial P2P links [3].

As can be seen in Fig. 1, the IEC 61850 use of MU includes proprietary interfaces and/or digital links with the primary system binary and analog information, SB interface for engineering and configuration, and multiple unidirectional serial P2P links to other DSS devices. Years later, IEC 61850-9-2 defined it using the Open Systems Interconnection (OSI) stack for PB and SB protocols within MUs. Years after that change, IEC 61869 was starting to enhance the definition of analog and digital secondary signals for measuring, protecting, and controlling purposes. It defines allowable errors both for analog and digital secondary signals, considers bandwidth, and defines accuracy requirements for harmonics and anti-aliasing filters. Based on these enhancements, several NCITs exist in the market today and over time will eventually have service records to verify their reliability.

II. System Architecture (Installation)

As mentioned, different concepts of system architecture to support signal digitization have evolved in the absence of NCITs. To date, the most popular and inexpensive method to improve digitization is the placement of the primary system protective relays in the substation control yard. However, very few protective relays were designed to withstand the environments presented in the substation yard. Those that are designed and tested to accommodate these environments have been proven to provide the simplest and most reliable option.

Another concept is to separate substation yard digitization from protection and control processing. In this application, a digitization device or function within a digital device, called an MU, is placed in the substation yard to interface with the primary equipment to perform ADC signal digitization and publish the results in digital messages. Some MU devices also receive digital messages from other MUs to expand their local database by collecting and aggregating data from other MUs. They also receive messages from intelligent electronic devices (IEDs) to perform control actions, including tripping the breaker and interlocking. One or more subscribers receive MU publications containing digitized signals and implement apparatus protection and control schemes on these signals. As needed, they transmit messages to the MU with an operating output signal. These MUs are available with or without intelligence to perform local logic and with or without auxiliary proprietary communications interfaces. An MU with intelligence logic is referred to as an intelligent MU (IMU), and those that do only ADC or ADC and digital-to-analog conversion to create digital and analog signals to actuate and operate primary equipment without local logic are called MUs [4]. The yard digitization concept has ushered in an era of manufacturers producing MUs for the yard so that IEDs remain protected in the control building, IMUs in the yard performing all protection and control, or combinations of the two.

The capabilities of substation electronic devices have been ever increasing, as have the industry data requirements of DSSs. With increased interest in DSSs, now more than ever, it is important to review the impacts of DSS design decisions on the power system performance. When making design decisions, the design engineer should not only understand immediate impacts of decisions but also the consequences to the power system and end users of events caused by the DSS while prioritizing the future requirements of the grid, such as heavy inverter-based resources (IBR) penetration.

Over the past decade, the industry has seen a significant increase in substation electronic device data demands both to support the growth in asset health monitoring capabilities and the increasing penetration of IBR. This demand is only expected to grow in the future. It is important to design a DSS in such a way that it does not restrict future power system development and performance capabilities.

Rather than try to mount digital devices within primary system cabinets, many designers use panels mounted in the yard near the primary equipment. This method allows technicians to work on the DSS equipment separate from the primary equipment. Also, end users find that an IMU with an operator display and control buttons is ideal to understand the health and behavior of the new DSS design. In this way, they can understand and control the power system from the DSS devices during commissioning, troubleshooting, and service actions. IMU and relay front panels that enable safe and efficient adoption of new technologies include:

- A front-panel display to control and view precise time and communications as well as the status of disconnects and breakers [and] user-selectable mimic screens [5].
- Front-panel LEDs [that] indicate custom alarms and provide fast and simple information to assist with rapid digital communications and/or power restoration [5].
- Programmable operator pushbuttons with front-panel customization.

Reliability and simplicity are mutually inclusive. To maximize reliability, a design must be as simple as it can be. Per Blackburn [6], "A protective relay system should be kept as simple and straightforward as possible while still accomplishing its intended goals." It is imperative that protective relay DSS designs are as simple as possible, but no simpler. A relay, or an IMU acting as a relay, in the yard is the simplest protective system and often does not require any change to the existing protection design or tools.

When opting for more complexity, operators should use IMUs and relays to support the necessary and sufficient status and diagnostics to service PB and SB communications and improve reliability. Specific to PB communications, this includes supervision of new metrics in the yard devices, such as:

- Ethernet channel, Ethernet frame transmit and receive, and Parallel Redundancy Protocol (PRP) monitoring.
- Generic Object-Oriented Substation Event (GOOSE) and SV publication monitoring.
- GOOSE and Precision Time Protocol (PTP) subscription monitoring.
- Time master and management supervision.

MUs are required in most SV applications due to the lack of development and installation of NCITs. NCITs are capable of publishing digital signals directly from an Ethernet port without the need for an MU. The lack of primary equipment that includes NCITs and other digitization capabilities has left end users with many choices and challenges in the placement of MUs in the substation yard.

Implementing an SV system involves the separation of functions that have been traditionally performed in a single IED into multiple locations. Most commonly, users may think of the separation of the ADC being relocated from the control house out into the yard to be closer to the primary equipment. This addresses the goal of reducing the amount of copper used in a typical installation but does not alone address the question of how much intelligence is required in the MU needed to achieve this function. The relocation of protective relays into distributed kiosk locations around the yard is a proven method of addressing both questions and should be an option included in the evaluation process for any DSS design.

Often, the first choice of location for an MU is in high-voltage breaker cabinets. The utilization of the cabinet that will require power and be in proximity of the signals requiring digitization is understandably a desirable location for an MU. Traditionally, the manufacturers of these cabinets have not provided the space required for the installation of the MU and associated wiring and isolating devices. Adapting a standard cabinet or enclosure design can add significant cost and increase lead times, having adverse effects on projects. Consulting with the manufacturer of both the primary equipment and the MU is required to ensure that the correct MU for the application is selected, affecting the design, factory acceptance testing, delivery, and necessary installation of the primary equipment.

Add-on cabinets or kiosks are alternatives to locating MUs in the primary equipment cabinets. This has the advantage of not requiring any changes to standard primary equipment designs. The additional cabinets can be located close to the primary equipment to provide the copper savings while allowing flexibility in design choices to locate or co-locate the MUs so that multiple MUs are combined into a single location that could be more desirable for commissioning and maintenance activities. The wide variety of applications across the industry makes offering standard kiosk designs challenging; however, utility designs that have consistencies allow utilities to take advantage of standard kiosk designs across their organization.

MU feature requirements can play a large role in determining the size and location of the kiosk. IMUs can include displays, pushbuttons, targets, and multiple Ethernet ports for SB, PB, and engineering access protocols. Simple MUs may only have a single Ethernet port and no displays or LEDs. The functionality of the MU will play a large role in determining a suitable installation location.

Commissioning and maintenance activities require personnel and test equipment to have safe and efficient access to the MU. The single biggest disadvantage of implementing a DSS is that previously all of these activities were typically completed within the confines of a control house. This protects both personnel and equipment from the elements and proximity to energized electrical apparatus. In some instances, work jurisdictions are determined by the apparatus the equipment is located in. For instance, high-voltage circuit breakers may have previously been the responsibility of a high-voltage substation electrician to maintain. Adding the MU to the enclosure could now result in multiple professional disciplines being required to have access to the asset. This can mean having additional safety training requirements and new boundaries for work jurisdiction that a utility must plan for. Using a distributed approach for kiosks that include multiple MUs, network apparatus, and required test switches can align with a utility's traditional method while providing the benefits of a DSS, allowing for safer and more efficient work locations.

Drawing from previous experience and best-known methods gives designers an advantage in the decision-making process when deploying systems. Evaluating the performance of SV systems, as demonstrated in [7], ensures designers are making informed decisions. In this paper, there are two key takeaways related to the type and location of the MU. Reviewing the destructive nature of the fault shown in Fig. 2 is a reminder of the inherent dangers in a high-voltage yard and the serious discussion that needs to take place when deciding where to locate devices in the yard. This fault occurred near a transition from a 138 kV underground cable to an overhead line. The explosion of the oil-filled pothead caused debris and oil to be sent into the surrounding area, which would be a very dangerous situation if personnel were required to be performing maintenance or work on an MU in the area.

Fig. 2. Damaged overhead-to-underground transition [7].

The paper also discusses errant measurements that were recorded by an SV relay when compared to the same currents measured by a conventional relay and CT during the fault. The MU did not have recording capabilities, leaving only the oscillography shown in Fig. 3 and Fig. 4 for the protection engineer to determine where the problem occurred. The MU was connected to a CT that measured line current, which is identified as CT 3, as discussed in [7]. The conventional wired 21-2 relay shown in the green trace reports an A-phase current that does not exactly match the 87B23-79DTL SV relay shown in the red trace. "The disagreement occurs near the peak values of current. It is suspected that the MU at CT 3 did not precisely report the CT 3 current above 50 A secondary. The voltage signals seen in each relay align very closely" [7]. Fig. 4 shows raw current signals consumed by an SV relay, as compared to raw signals produced by a conventionally wired relay for the same event. Therefore, the waveform deformities are assumed to be produced by the SV MU. This illustrates the value of MUs with recording capabilities to enable waveform comparison to better identify the source of the waveform discrepancies. The discussion in the paper illustrates the value of using IMUs with recording capabilities similar to that of protection relays to assist in event analysis and troubleshooting.

A 1.5 ms delay is also introduced into the filtered waveforms in Fig. 3. However, in the unfiltered report, no delay is introduced. “The SV relay automatically compensates for the 1.5-millisecond channel delay for analog quantities when generating the unfiltered event report. This can be thought of as shifting the analog signals 1.5 milliseconds to the left along the x-axis. This allows for direct comparison between the analog signals from conventional relays and from SV relays when doing event analysis” [7].

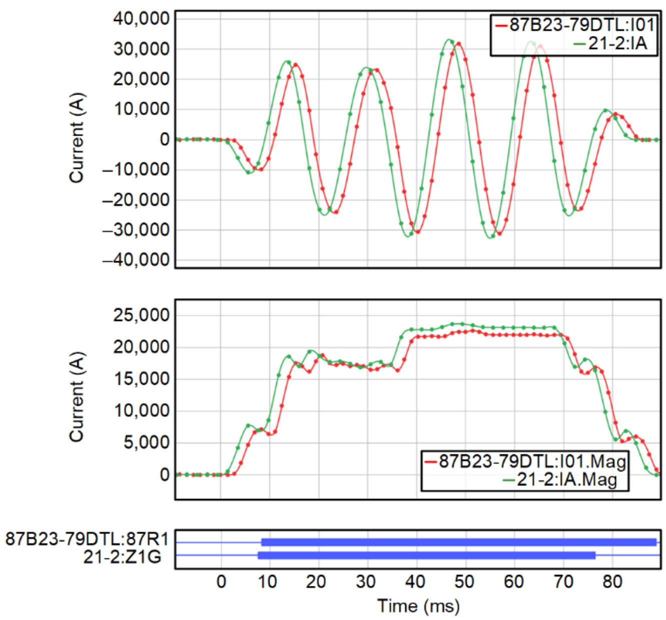

Fig. 3. 21-2 and 87B23-79DTL filtered A-phase current [7].

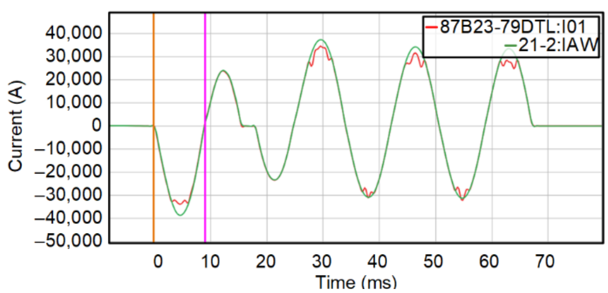

Fig. 4. 21-2 and 87B23-79DTL raw A-phase current [7].

Finally, the cost of the system being considered should be economically viable for the benefits it is providing. The system cost should not only include the system equipment costs but also the overall cost of ownership. The cost of the solution should also be economically viable when compared against other available solutions.

III. Cost Analysis

A. *Design Method*

To understand the true cost difference of the various field installation methods, an engineering, procurement, and construction (EPC) firm was contracted to create bids for each method. These bids represented the true price difference for an EPC to do the work, including design and field installation. For this scenario, DSS protection and control for a single green field substation bay was analyzed. The design did not include the primary or secondary equipment but rather material and labor costs to design and install the DSS wiring. Therefore, the costs of procuring and mounting the digital relays and MUs were not part of this installation method cost comparison. A substation field drawing with distances relevant to the analysis is shown in Fig. 5. Design considerations include:

- Engineering labor and materials to design and document DSS installation for a single bay in an open air substation, including field wiring drawings and device wiring termination drawings.
- Labor and materials to terminate DSS wiring to CTs, potential transformers (PTs), circuit breakers (CBs), and switchgear (SW).
- Labor and materials to install field wiring for various distances.
- Civil work labor and materials to build trenches.

Using this evaluation method, the wiring cost of nontraditional fiber from the control house to the yard with kiosks housing digital equipment is the same for relays in the yard kiosk and for MUs and IMUs in the yard kiosks. Both are then contrasted with traditional wiring from the control house to the primary equipment in the field. Material and labor prices in this example represent the true cost as of December 2020 in South America, and since then, copper prices have risen dramatically worldwide. Though prices change over time and across different locations, the difference in cost is relevant and proportional to any project.

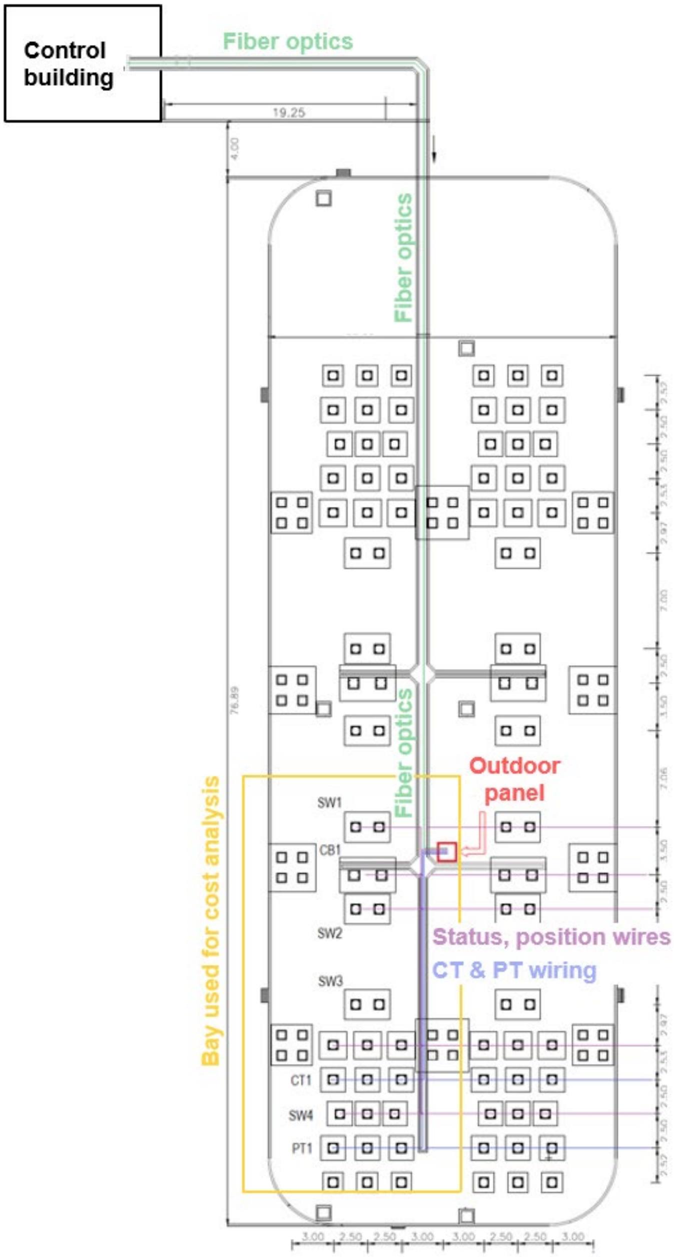

Fig. 5. Substation field drawings with distances relevant to the design analysis.

B. *Wiring Considerations*

The EPC firm created a complete cost breakdown for the wiring installation of the various methods. The primary equipment (CTs, PTs, CBs, and SW) signal requirements for sensing, monitoring, control, and actuation were used to determine the number of wires and, therefore, number of multiconductor (multiwire) cables to install as well as the recommended wire gauge for each. The location of the primary equipment was used to determine the length required for each cable between the primary equipment located in the yard and the control house. When using kiosks in the yard, the lengths of wire reduced to the distance from the primary equipment to the kiosk cut terminations remain the same. Then, fiber-optic cables are priced from the kiosk to the control house. Wiring considerations include the:

- Connections to primary equipment.
- Number of conductors required, use of multiconductor cables, and multiconductor American wire gauge (AWG).
- Lengths of wire between primary equipment and termination at the field kiosk or control house.

Table I shows traditional installation method cable multiconductor requirements and lengths to sense and send signals for each piece of primary equipment. The length multiplied by the cost per linear meter value provides the cost for each cable. Table II shows nontraditional installation method cable multiconductor requirements and lengths as well as the costs for fiber-optic cables and auxiliary power out to the kiosk to energize the digital devices.

Comparing the tables reveals that the installation of digital devices in the yard with short copper wiring to the primary equipment plus fiber-optic cables to the control house results in a cable installation price 66 percent lower than that of traditional installation wiring. Cost savings are based simply on significant reduction in the multiconductor wire cable lengths and addition of fiber cables. As illustrated in the wiring cost section, the wiring termination labor at either end of the copper wiring remains the same.

TABLE I
WIRING EQUIPMENT COST FOR TRADITIONAL SUBSTATION

Primary equipment	Cable description	Multiconductor wire type	Cable quantity	Total cable length (m)	Cable price	Total price
CB	Control signals (digital status)	8x12	2	84.845	$7.56	$1,284
	Trip circuit (compressor motor)	4x12	3	84.845	$3.78	$963
	Power supply	2x12	1	84.845	$1.98	$168
SW1, SW2, SW3, SW4	Control signals (digital status)	8x12	2	84.845	$7.56	$1,283 x 4
	Trip circuit motor	4x12	1	84.845	$3.78	$321 x 4
	Power supply	2x12	1	84.845	$1.98	$168 x 4
PT	Analog measurements	4x12	2	103.345	$3.78	$782
	Miniature circuit breaker (MCB) position	2x12	2	103.345	$1.98	$409
CT	Line, transformer, and coupling measurements	4x10	9	98.345	$5.28	$4,669
					Total:	**$15,363**

TABLE II
WIRING EQUIPMENT COST FOR DIGITAL DEVICE-IN-THE-YARD INSTALLATION

Primary equipment	Cable description	Multiconductor wire type	Cable quantity	Total cable length (m)	Cable price	Total price
CB	Control signals (digital status)	8x12	2	7.75	$7.56	$117
	Trip circuit (compressor motor)	4x12	2	7.75	$3.78	$59
	Power supply	2x12	1	84.845	$1.98	$168
SW1, SW2, SW3, SW4	Control signals (digital status)	8x12	2	7.75	$7.56	$117 x 4
	Trip circuit motor	4x12	1	84.845	$3.78	$321 x 4
	Power supply	2x12	1	84.845	$1.98	$168 x 4
PT	Analog measurements	4x12	2	26.25	$3.78	$199
	MCB position	2x12	2	26.25	$1.98	$104
CT	Line, transformer, and coupling measurements	4x10	9	21.25	$5.28	$1,010
Fiber and digital	Jacketed cable	4 cores	2	77.095	$5.72	$882
	Power supply	2x12	1	84.845	$1.98	$168
					Total:	**$5,131**

C. *Civil Works and Construction Considerations*

Though distances do not change for either design, cable types and quantities reveal the size of the cable trenches required for associated trenches. The trench design chosen has concrete floor and walls as well as a concrete lid flush with the substation yard gravel. Recognizing that there is significantly less volume of fiber-optic cables for the digital device-in-the-yard installation than multiconductor cables for traditional wiring, the trenches required for the digital solution are much smaller. Pricing based on the amount of concrete and rebar required illustrates the cost difference between the two options.

The information necessary for determining the cost per meter of various types of trenches include the:

- Labor to design each trench type.
- Ability to consolidate cabling into a single larger trench.
- Digital device in the field kiosk requiring a shortened wiring trench to the primary equipment and a fiber-optic trench to the control house.
- Labor and materials to excavate, set forms, transport, and dispose of fill.
- Labor and materials to set reinforcing steel (floor, walls, and lid) and pour trench concrete (floor, walls, and lid), priced as dollars per cubic meter of concrete and dollars per kilogram of steel.

The EPC firm had established prices (as illustrated in Table III) for several trench sizes based on their experience. Each trench type has associated requirements for the size of excavation, concrete pour, and slab area. This information is used to determine the space in the yard, volume of excavation, and amount of concrete and steel necessary for each type. The requirements for the digital device-in-the-yard kiosk were so dramatically reduced that it is possible to use a new and smaller trench design labeled Type 6 in Table III.

TABLE III
TRENCH TYPE AND DIMENSIONS IN METERS

Type	Trench width	Duct width	Duct height	Concrete floor/wall thickness	Concrete lid thickness
1	0.225	0.2	0.3	0.15	0.04
2	0.415	0.4	0.3	0.15	0.056
3	0.675	0.6	0.4	0.15	0.072
4	0.675	0.6	0.6	0.15	0.072
5	1.045	0.8	0.6	0.15	0.088
6	0.415	0.4	0.4	0.15	0.056

For comparison, the fixed costs used to price the different options for ductwork within underground trenches are illustrated in Table IV. Based on those costs, the pricing for ductwork necessary to complete the traditional wiring scheme for the substation configuration being evaluated is illustrated in Table V, and the pricing for digital devices in the yard is illustrated in Table VI. The installation of digital devices in the yard results in a trenching price 33 percent lower than that of traditional wiring.

TABLE IV
FIXED COSTS FOR DUCT TRENCHING AND CONSTRUCTION

Item	Unit	Price per unit
Excavation	m^3	$9
Transport and disposal of fill	m^3	$104
Concrete for floor	m^3	$215
Concrete for walls	m^3	$215
Concrete lid	m^3	$311
Reinforcing steel in floor	kg	$1
Reinforcing steel in walls	kg	$1
Concrete delivery	m^3	$170

TABLE V
PRICE FOR DUCTING REQUIRED FOR TRADITIONAL INSTALLATION

Duct type	Duct length (m)	Price
1	5.12	$294
2	20.1	$1,420
3	12.53	$1,154
4	63.23	$6,864
	Total:	**$9,732**

TABLE VI
PRICE FOR DUCTING REQUIRED FOR
DIGITAL DEVICE-IN-THE-YARD INSTALLATION

Duct type	Duct length (m)	Price
1	5.12	$294
2	20.1	$1,420
6	12.53	$855
6	63.23	$3,952
	Total:	**$6,521**

D. *Cable Termination and Wiring Considerations*

Though total distances of cabling remain the same for both designs, cable types and quantities do change and, therefore, the effort to terminate and test the cables is different. For this substation, when digital devices are installed in the field, fiber connections convey the signals to and from the digital devices in the control building. When the digital devices in the yard are MUs, the fiber conveys PB communications, and when the digital devices in the yard are relays, the fiber conveys SB communications. This eliminates the entire task of wiring and testing copper connections to a marshalling cabinet in the control building in the traditional installation method. The evaluation of the effort for the two methods, as illustrated in Table VII and Table VIII, considered labor effort of a person as a full-time equivalent technician terminating multiconductor wiring at the primary equipment and digital equipment, including the:

- Activity cost as effort in person-days.
- Number of technicians.
- Number of days.

With less multiconductor termination and testing, the installation of digital equipment in the yard results in a cable installation, termination, and testing price 29 percent lower than that of traditional wiring.

TABLE VII
PRICES FOR INSTALLING, TERMINATING, AND TESTING
COPPER WIRING FOR TRADITIONAL INSTALLATION

Activity	Number of persons	Number of days	Effort in person-days
Pulling cables to the primary equipment from the control house marshalling cabinet	4	7	28
Pulling cables from the control house marshalling cabinet to the digital device	4	7	28
Wiring termination and testing at the primary equipment	2	8	16
Wiring termination and testing in the control house marshalling cabinet	2	3	6
Wiring termination and testing at the digital equipment	2	6	12
		Total:	**90**

TABLE VIII
PRICES FOR INSTALLING, TERMINATING, AND TESTING
COPPER WIRING FOR DIGITAL DEVICE IN THE YARD

Activity	Number of persons	Number of days	Effort in person-days
Pulling cables to the primary equipment from the field kiosk	4	7	28
Pulling cables from the field kiosk to the control house digital device	4	1	4
Wiring termination and testing at the primary equipment	2	8	16
Wiring termination and testing at the digital device in the kiosk	2	6	12
Cable termination and testing between the digital device in the field kiosk and in the control house (fiber)	2	2	4
		Total:	**64**

E. Control House and Kiosk Construction Considerations

The spaces for the battery system, operator, and technician workspaces and bathrooms are left to the discretion of the end user. With many of the protection and control panels moved into kiosks in the field for the digital device-in-the-yard installation, the required control house dimensions are much smaller. Smaller control buildings require less labor and material, and permitting is often simpler, less bureaucratic, and less expensive. In this example, the reduction in cost of the control house is not offset by the added cost of labor to install kiosks in the yard. For this end user, the kiosks are roughly 10 percent more expensive than the six walled cabinets that are typically used in the control house. Therefore, changing them from inside the control building to mounting them as kiosks outside does not represent a large cost difference. The labor to mount and test the digital devices and accessories is the same within a kiosk cabinet and control house cabinet. The cost savings due to the smaller control building will be significant and unique per end user; however, end users that place MUs in the yard and relays in the control building will have twice as many panels and a similar-sized control house. It is expected that based on moving the cabinets with relays to the yard, the control building can be reduced by 25 or 50 percent in size and cost. One typical floor plan change shown in Fig. 6 illustrates a 25 percent reduction in control building size and expense.

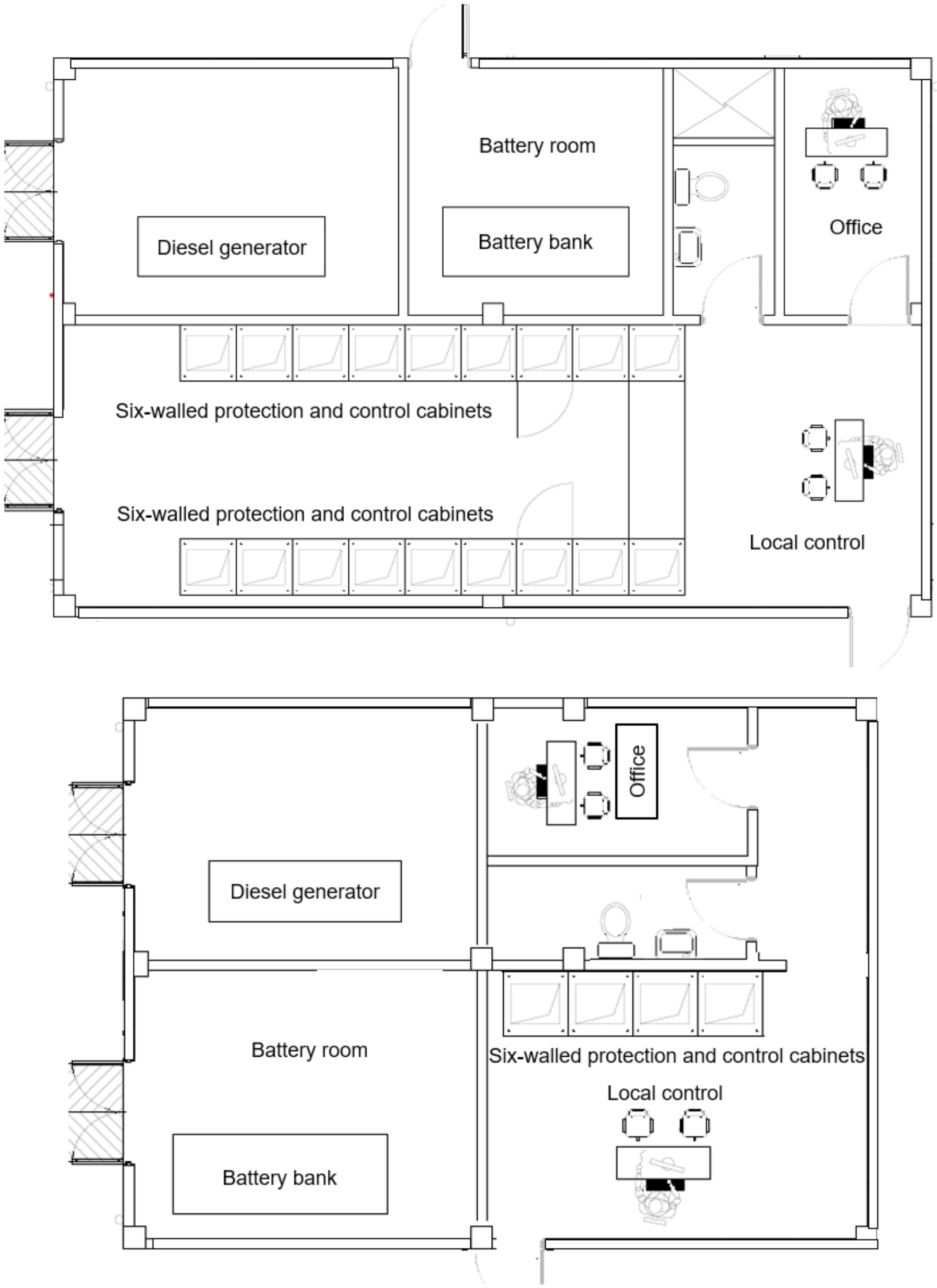

Fig. 6. Example reduction in floor plan of smaller control building.

Prices for the external cabinet are illustrated in Table IX for reference.

TABLE IX
PRICES FOR FIELD KIOSKS TO ACCOMMODATE
TWO 5U 19″ RACK IEDS PLUS ACCESSORIES

Component	Quantity	Price
External cabinet 800 x 800 x 1,600 mm	1	$2,642.55
Lot (e.g., terminal blocks, rails, fiber patch panel, test switches)	1	$2,096.22
	Total:	**$4,738.77**

Finally, Table X illustrates the possible cost savings as a result of moving the protection and control panels into the yard and replacing a majority of the copper wiring with fiber-optic cables.

TABLE X
PRICE COMPARISON FOR TRADITIONAL WIRING AND INSTALLATION OF THE DIGITAL DEVICE IN THE YARD

Activity	Traditional solution	Digital device in the yard	Cost reduction of digital devices in the yard
Civil works construction material and labor	$9,732	$6,521	33%
Control house size	1	0.75	25%
Copper and fiber material	$15,363	$5,131	66%
Copper and fiber labor	90 person-days	64 person-days	25%

Without factoring the change in size of the control house, the device-in-the-yard approach is 50 percent less expensive than the traditional approach when considering the:

- Reduction in design and drafting hours for a simpler design.
- Reduction in required materials, including cables, trenches, and ducts.
- Reduction in labor and time for trenches and ducts.
- Reduction in labor and time for installation and wiring tests.

IV. COMMUNICATIONS INTERFACE AND NETWORKING IMPACTS

Ethernet was first commercially introduced in 1980 and is a technology used to interconnect devices to facilitate device-to-device communications. Ethernet devices place data into packets and send them across links where the packet is passed to the device intended. As Ethernet applications have evolved and become implemented for critical communications, it is critically important to understand network details and engineer the network for reliable and deterministic performance under all conditions.

It is important to note that Ethernet is not a multiplexed communications technology. At any given moment, a single data frame can exist on a given network link. This requires managing the packet payload and the gaps between the packets. Several techniques are implemented to successfully switch and prioritize traffic on the network. Traffic management controls, like VLANs and switching queues, are used in network equipment to ensure critical traffic receives segmentation and higher priority on the network. As the amount of critical traffic increases, so does the amount of traffic receiving priority on the network. This results in network congestion and, in extreme cases, significant delays in lower priority data being received.

Priority queues are implemented in switches to receive, buffer, and send traffic out of ports based on network performance requirements and configured packet priority. Some switches implement strict priority queuing, where higher priority packets are passed first and then packets with lesser configured priority, or a weighted round robin approach, where a larger portion of higher priority traffic is sent relative to lower priority traffic. In this approach, a weighted portion of all priority traffic is released from the switch buffer.

VLAN tags and frame priorities that provide Class of Service are essential technologies used to prioritize frames and segregate them onto appropriate network segments. These technologies allow engineering of the message data flow and become increasingly important as networks grow in traffic diversity, complexity, and size. A VLAN is used in operational technology (OT) communications to create virtualized connections used to separate and isolate frame ingress and egress at the data link layer. Even though cabling and physical equipment infrastructure are physically shared with other VLANs, logical LANs use data flow rules to transfer frames to their intended destinations. Each VLAN within a network identifies a group of ports that messages will be sent to, known as a broadcast domain. Ethernet frames in one VLAN are prevented from being transmitted onto another VLAN, but network ports can participate in more than one VLAN. The application of VLAN tags occurs at the device or network switch and follows a standard format defined by IEEE 802.1Q within the Ethernet header, as illustrated in Fig. 7.

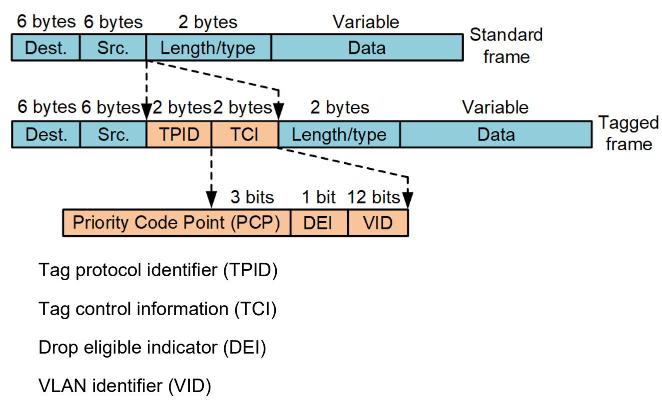

Fig. 7. Tagged Ethernet header showing the 4-byte VLAN tag structure.

Ethernet switches use VLANs to aggregate traffic between switches into groups called trunks. The trunks of Ethernet traffic create a path between switching centers or network nodes by joining data paths on the network edge onto the main trunk line like the branches of a tree, as illustrated in Fig. 8. When protocols like Manufacturing Message Specification (MMS), Telnet, or others are transmitted from the source device without a VLAN tag, these IP-based messages are referred to as untagged traffic. A VLAN tag is added to the message at the ingress port of an Ethernet switch. A VLAN made from the application of port-based VLAN tags is called a PVLAN [8]. This is used to identify the application and broadcast domain, as illustrated in Fig. 8. This method of traffic segmentation provides a powerful security mechanism. Users and IEDs connected to ports configured with one PVLAN cannot reach other ports with other PVLANs with IP protocols, as illustrated in Fig. 8. This is how businesses seamlessly segregate computers and servers, even when the end devices are not capable of managing the application of VLAN tags. An example is how one department or function is isolated to VLAN 2, preventing access from other network devices. These PVLAN tags exist only within the Ethernet network switch and determine which local ports the frame can be sent to. The PVLAN tags are removed from the Ethernet frame when it exits a switch port. The process is repeated if the Ethernet frame reaches another switch port. When the Ethernet frame reaches an IED, it will process the frame, unaware that the PVLAN mechanism was used in the data path.

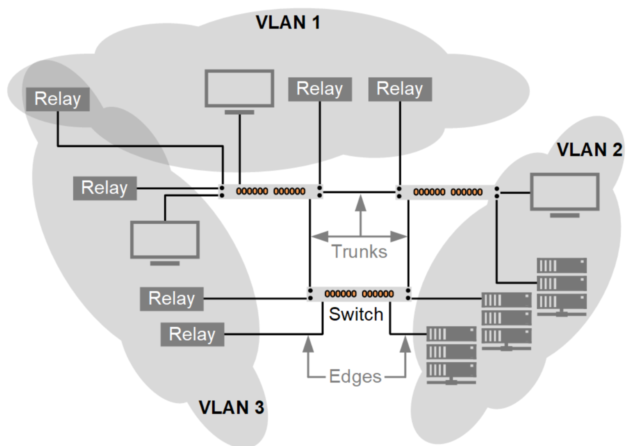

Fig. 8. PVLAN segregated network.

As shown in Fig. 7, the IEEE 802.1Q four-byte extension (tag) added to the Ethernet frame header is used during network data flow to distinguish traffic destined for one VLAN from traffic for another VLAN. The 12-bit field VID allows 4,094 different VLANs to exist on a single network. Traffic in a VLAN-enabled network include[s] both VLAN tagged and untagged traffic. Between trunk ports that interconnect switches, all frames are tagged. In edge ports that connect IEDs and PCs to the network, frames may be untagged or tagged. GOOSE and SV frames published by IEC 61850 IEDs are examples of tagged frames. These IED-applied VLAN tags are not well understood or expected by IT professionals. IT professionals commonly use port-applied or PVLAN tags.

A substation application may have mission-critical protection traffic (such as a command to trip a breaker) coexisting with supervisory control and data acquisition (SCADA) or device maintenance traffic (such as event oscillography retrieval). The differing delivery time requires that these messages separate traffic into priority queues within switches and IEDs. The priority queuing mechanism uses a 3-bit quality of service field. Fig. 7 shows the actual position of this field.

Successfully implementing a VLAN-enabled network requires managed Ethernet switches to ensure that traffic from one VLAN does not cross the boundary to another VLAN. Users must configure managed switches to specify which VLANs exist, their assignments to physical Ethernet ports, and whether the traffic is tagged or untagged.

Substation IEDs have evolved so they now include additional processing and memory to manage IEEE 802.1p message prioritization and IEEE 802.1Q VLANs. IEDs use this to segregate traffic and improve data flow quality in addition to other message navigation methods for multicast messages. OT Ethernet uses the same VID defined in IEEE 802.1Q to segregate traffic among substation network devices to improve data flow quality. To avoid confusion about when the same Ethernet identifier is being used for different purposes, OT VLAN tags are sometimes referred to as QVLAN tags to identify when they are used to improve data flow quality in an OT network versus trunking in an IT network. Substation networks and devices use VLAN segregation and priority, and OT switches perform fast queue handling to transfer some messages with better speed than others. This is done by queue management that processes higher priority messages ahead of lower priority messages when there is not enough bandwidth to quickly process all frames. However, there is no guarantee of speed or delivery, and latency will be added when any message queue in the data path becomes saturated.

Unfortunately, multiple uses of the IEEE 802.1Q VID for different but related segregation purposes cause confusion. QVLAN, PVLAN, and VLAN all refer to the same VID field in the Ethernet frame shown in Fig. 7. A QVLAN is a logically separate Ethernet network (based on QVLAN tags) that shares cabling and physical equipment infrastructure with other VLANs. These messages have multiple destinations, but network settings prevent them from going to all destinations. Similar to using a VID as a PVLAN, each VID used as a QVLAN on a network has its own broadcast domain, meaning that Ethernet frames from one QVLAN will not be transmitted onto another QVLAN, as illustrated in Fig. 9. In this illustration, physical connections are shown with black arrows, and virtual data flow is illustrated by VLAN 20, 30, and 40.

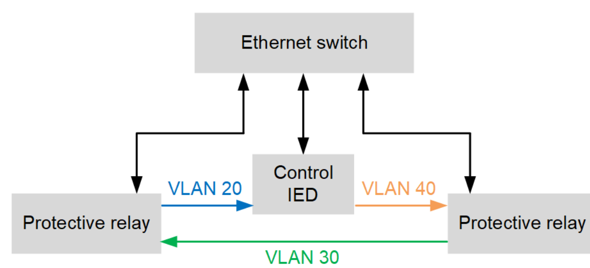

Fig. 9. QVLAN segregated network.

If more than one message is given the same QVLAN, the broadcast domains overlap, as shown as a single VLAN in Fig. 10. This will cause congestion and saturation, which will lead to increased message latency when network queues are overly utilized.

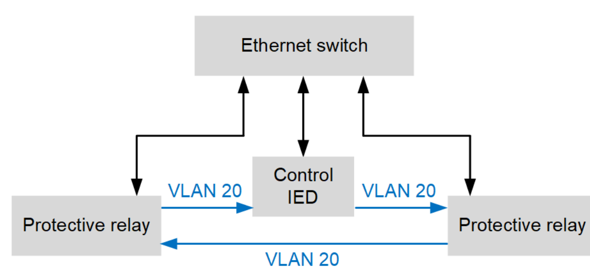

Fig. 10. QVLAN network without segregation.

The number of priority queues varies among switches, with a minimum of two needed for IEEE 802.1p support. A queuing strategy is usually configurable, with strict priority as one of the options. Strict priority means that the switch forwards all higher priority traffic before processing other messages.

When complete, the Ethernet network will support delivery of lower priority tagged and untagged traffic.

Each IED will participate in many unique broadcast domains via QVLANS. Each IED should participate in the same PVLAN for IP messages supporting SCADA, synchrophasors, event collection, and engineering access. They will also simultaneously participate in one or more QVLANs to send and receive high-speed GOOSE messages.

Substation networks can be configured without the correct use of VLANs, but network congestion and reconfiguration will cause problems in message delivery when network queues are overly utilized. It is very difficult to add VLANs to an in-service system due to the interruption of in-service traffic. Therefore, to prevent downtime, it is advised to engineer and design traffic segmentation and VLANs from the beginning with traffic management in mind. The additional burden of learning about and configuring managed switches does present a new but essential requirement. However, as critical intersubstation and intrasubstation protection schemes using MUs are designed, VLANs and priorities are recognized to be essential for ensuring timely and secure data traffic.

Best-known methods for configuring mission-critical Layer 2 SV messages match those documented for GOOSE multicast Ethernet messages based on IEC and IEEE standards, including the following information from [9]:

- Assign each GOOSE message a unique VLAN based on IEEE 802.1Q, referred to as a QVLAN. [When this is not possible, carefully group alike GOOSE messages into a single VLAN.]
- Assign each GOOSE message a unique multicast media access control (MAC) address.
- Assign each GOOSE message a unique application identifier (app ID).
- Assign a [short but] descriptive GOOSE identifier (GOOSE ID) rather than generic IDs in the IED to improve documentation and troubleshooting.
- Label GOOSE message payload contents with [short] descriptive names, rather than generic names, in the IED to improve documentation and troubleshooting.
- Carefully design payload size and contents to facilitate appropriate GOOSE application processing [(GAP)]—mind the GAP.
- Carefully choose IEDs that process incoming GOOSE messages appropriately fast for protection-class applications—mind the GAP.
- Do not publish multicast messages on the network without QVLAN tags.
- Disable all unused [device] communications ports.
- Monitor GOOSE message attributes to derive the quality of the message [reception at each subscriber].
- Use the GOOSE attributes of sequence number and state number to determine if all wanted messages reach the receiver.
- Monitor, record, and alarm failed GOOSE message receptions.
- Provide GOOSE reports with configuration, status information, and statistics pertaining to GOOSE messages being published and subscribed to by the IED.
- Record and alarm failed quality of GOOSE messages for use in local and remote applications.
- Display status of GOOSE subscriptions and alert operators of failure.
- Configure each switch port to block the ingress of unwanted and allow wanted multicast messages via VLAN and MAC filtering. This reduces the multicast traffic through the network to only that which is required.
- Configure each switch port to block the egress of unwanted and [only] allow wanted multicast messages via VLAN and MAC filtering. This prevents unwanted messages from reaching the IEDs.
- Use switches designed for rugged environments and Layer 2 multicast among…IEDs in a fixed address network.
- Do not allow dynamic [IED data model and reporting] reconfiguration; this leads to [systems different than commissioned].
- Use switches that provide real-time status of traffic behavior and network configuration [9].

Recent technology advances introduced additional best-known methods. OT software-defined network (SDN) Ethernet networks are simpler because they behave as configured based on pre-engineered data flow, and they use fast, static lookup table instructions to mitigate faults rather than dynamic spanning tree decisions. OT SDN develops and maintains data flow diagrams for all Ethernet network traffic.

For SV, applications require pre-engineered OT SDN for fast network fault resolution within 100 µs to ensure consistent message data flow of SV messages every 208 µs or faster, supporting 4.8 kHz publishing rates.

When adequate network technology is not available, duplication methods can be used to enable data flow of one path while the second path failed [10]. Care must be taken to monitor failures within PRP and high-availability seamless redundancy (HSR) designs to initiate corrective action [11].

If a port cannot be disabled, all unused switch communications ports should be placed into unique, dedicated VLANs preventing access to other ports or devices. Other best practices to develop and maintain the network port allocation include:

- Develop and maintain documentation of the Layer 1 physical connections for the network devices.
- Develop and maintain documentation of the Layer 2 MAC address network architecture. This would include traffic segmentation and management based on Layer 2 information.

- Develop and maintain documentation of the Layer 3 IP address network architecture and any Layer 3 routing.
- Audit and record network performance packet latency information in normal and contingent network topologies. For Spanning Tree Algorithm (STA) networks that use the Rapid Spanning Tree Protocol (RSTP), OT SDN, and unmanaged networks, network performance must meet designed network estimates and ensure all network topologies converge within the required time.

In addition to these message and network design methods, one approach to ensure network-based devices can reliably transfer data is to create physically segregated networks based on criticality or data application. With physical segmentation, security controls following defense-in-depth security principles are easier to apply. The application of the Purdue model and segmentation of traffic is clearer with physical isolation of network traffic. With physical segmentation, traffic management and port-based access controls to enable and disable access are easier to create and implement.

The IEC 61850 standard provides for discrete classification of networks into PB, restricted to only time-sensitive critical communications, and SB that is either restricted to low-priority, less time-demanding protocols only or applied with both low-priority and time-sensitive critical communications on the same bus. Still, another option is to have both merged onto a single bus.

In OT networks, communications protocols have evolved significantly with each new protocol being developed in response to different performance requirements of the protocol purpose. When considering SCADA protocols, DNP3 was developed and released in 1993 to promote device interoperability using a nonproprietary protocol. Additionally, DNP3 was an evolution to protocols like Modbus that did not provide source time stamps with state changes. In IEC 61850, MMS was adopted to create a standard way for all manufacturer devices to exchange low-criticality SCADA information with accompanying time-stamp and state-change information. These SCADA protocols are designed to withstand variations in network performance and support sending accurate time-stamped state-change information from the end device. This method of the source applying the time-stamp information ensures that accurate point-assertion times are retained during varying delays in network performance.

Traditional non-IEC 61850, critical, P2P communications have leveraged lightweight high-speed protocols like Mirrored Bits communications. This protocol is designed to send 8 bits between two devices with a focus on speed and reliability. While this protocol works well between two devices with a limited data set, it is not a protocol that allows for one-to-many or many-to-many communications. For this reason, IEC 61850 GOOSE was developed to provide rapid reporting of events without the need for bidirectional communications or acknowledgment that a device has received the message. This protocol lends itself to multicast critical messaging to a group of peers on a given network. A consideration for GOOSE is the management of time-stamp information. The standard allows for time and quality information to be included in the GOOSE data set. There is no guarantee that the time and quality information inside the GOOSE packet will be used by the receiving device. With the absence of source applied and used time stamps, a time stamp applied at the receiving device will add network performance delays to the assertion time.

The protocols mentioned each require tradeoffs in how frequently the data are sent, where the time stamp is applied, or how many devices can participate in a communications session. These tradeoffs are made anytime a value is communicated over a protocol. The underlying decision is made based on where the time stamp is applied for changes of state; if devices do it differently, the Sequential Events Recorder (SER) recorded by the different devices will not have the same accuracy and precision. Further, in connectionless protocols like GOOSE, network engineering is required to ensure messages are sent with minimal network delay and a high degree of reliability.

Locating an IMU that is directly wired to the field primary equipment contact points enables the IMU to internally create, store, and report SERs, events and other records essential to analyzing the behavior of the power system. By performing this action locally, the IMU associates state changes to the monitored points with a high degree of precision. This information logged to a Sequence of Events (SOE) file is available for auditing during event analysis.

The communications services required in an MU or IMU will affect both the protocols and types of communications ports that are required. An IMU may have PTP, GOOSE, SV, MMS, and engineering access protocols to configure device reports and retrieve all SOE, oscillography, or other generated reports. This could include a single interface or multiple pairs of interfaces, depending on the network architecture chosen. Compared with a simple MU that may have a single port and protocol, the location and size requirements can change dramatically. Thorough evaluation of the current and future application requirements is required to understand the impacts of communications interfaces on MUs.

V. Power System Impacts

When designing DSSs, power system performance should be prioritized. Power system protection has a direct impact on the overall power system performance, meaning any decisions made in the design of DSSs will also have either a direct or indirect impact on system performance. As electric grids become more reliant on generation assets requiring inverters to connect onto the electrical power grid, the performance of power system protection equipment will become more important. Systems with higher inverter-based generation penetration generally have faster tripping requirements to maintain power system reliability and stability. In some situations, if the IBR penetration is high enough, modern fault detection techniques may also be required.

A. *Reliability*

The predicted unavailability of a protection and control system will have a direct impact on the reliability of a power system. A rudimentary approach to predict the unavailability of each design under consideration is to consider the reliability of devices, based on their failure rate, the quantity being used, and time to detect and repair a failure in the future and return the application to service. Using a simple representation, the predicted unavailability of a system is represented as the mean time to repair (MTTR) the system divided by the mean time between failures (MTBF) of the system per (1).

$$\text{Unavailability} = \frac{\text{MTTR}}{\text{MTBF}} \tag{1}$$

MTTR includes the mean time to detect (MTTD) the failure and then return it to service. The industry average to repair or replace a digital device is 48 hours with adequate spares and technical support. For digital devices with fault detection and alarm, the notification will be nearly immediate. Device failures that are not monitored will be discovered during a power system fault or during routine maintenance testing. The MTTD of monitored faults is considered zero, and that for nonmonitored faults, which can happen at any time after one test and before the next, is considered to be half of the maintenance period. MTBF is a metric used to represent quality of a given device population as the inverse of the failure rate. For the sake of this discussion, all electronic devices are assumed to have an equivalent MTTR and MTBF. The MTTR and MTBF of a device or system changes depending on different factors, such as the availability of device self-diagnostics, maintenance intervals, spare stock, and supply chain constraints. These factors are important to consider when comparing one device type against another, such as comparing the unavailability of a traditional copper cable against the unavailability of communications-based signals. The self-diagnostic capabilities of both the traditional copper and communications-based signals should be considered. Communications-based applications have inherently available message reception monitoring capabilities. Control cable applications also have self-diagnostic capabilities through applications, such as trip coil monitors and CT and PT monitoring functions. For a more comprehensive analysis of DSS reliability, refer to [12] and [13].

The topologies compared in this paper differ in many regards, including the physical data path for PB communications. The fault tree analysis of a relay versus an MU installed in the yard and the associated PB communications via switched network communications versus direct connections were done based on industry MTBF values and the standard 48-hour MTTR [14].

Contrasting these PB solutions' risk of a fault while in service illustrates the differences between the scenarios and separates the MU and PB communications topology from the relay and applications discussed next. The unavailability of Scenario A, via fault tree analysis, including optical interfaces, power supplies, an MU, an Ethernet switch, and a GPS clock is illustrated in Fig. 11.

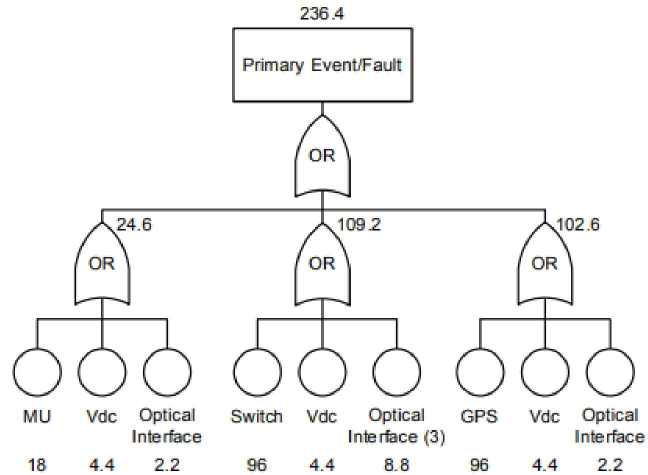

Fig. 11. Fault tree for an MU communicating over a PB fiber Ethernet network (the multiplier for all unavailabilities is 10^{-6}) [14].

The unavailability of Scenario B, via fault tree analysis, including a single optical interface, power supply, and MU, is illustrated in Fig. 12.

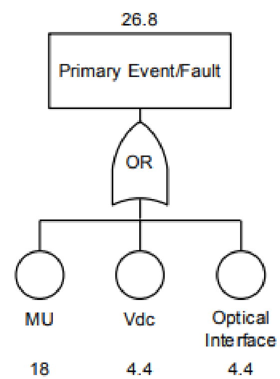

Fig. 12. Fault tree for an MU communicating over a PB direct fiber connection (the multiplier for all unavailability is 10^{-6}) [14].

The unavailability of Scenario C of the relay in the yard is not relevant because no PB communications are required, as illustrated in Fig. 13.

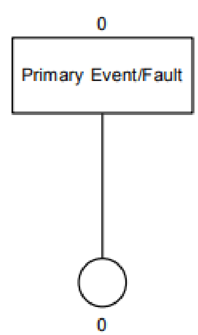

Fig. 13. Fault tree for PB communications of a field-installed relay (the multiplier for all unavailabilities is 10^{-6}) [14].

This PB fault tree and associated zero unavailability represents the predicted unavailability of the nonexistent PB communications and not the rest of the system. The non-zero unavailability values of the other scenarios illustrate the added risk that a component will fail, based on the type and quantity of additional components. For PB communications alone, the risk of having a failure in service with the Scenario B direct connection is about 27 times greater than the relay in the yard. The risk of having a failure in service with scenario-switched Ethernet is about 236 times greater than the relay in the yard.

The addition of equipment in DSSs creates an overall protection system reliant on more electronic devices to correctly function as compared to that of a conventionally wired system. In such applications, the availability of a system can be expected to reduce in inverse proportion to the number of additional devices in the system. For example, consider a dual-breaker application with SV MUs applied at each breaker for digitization, as shown in Fig. 14. In this application, four devices must correctly function for the overall primary protection system to perform appropriately. The primary protection system includes a high-accuracy clock, subscriber, and two MUs. One can therefore expect the predicted availability of such a system, as related to electronic devices, to decrease by as much as one-fourth as compared against a conventionally wired system.

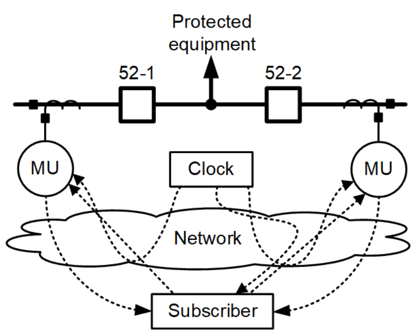

Fig. 14. SV MU application example.

A system with relays applied in the substation yard with only protection interconnecting functions digitized is shown in Fig. 15. In this application, only one electronic device is required to operate correctly to give an appropriate response from the primary protection function, assuming tripping is routed directly to the neighbor breaker. If tripping is routed through the neighbor electronic relay, then two electronic devices are required to give correct protection system performance. In both of these cases, the availability of the protection system can be expected to improve when compared to the system in Fig. 14, simply due to the reduction of electronic equipment. In the case of only one electronic device required to provide appropriate operation, one can expect the same performance, as compared to a conventionally wired system applied in a control house environment. In the case where two electronic devices are required to appropriately operate, an availability reduction of one-half, as compared against a conventionally wired system, can be expected.

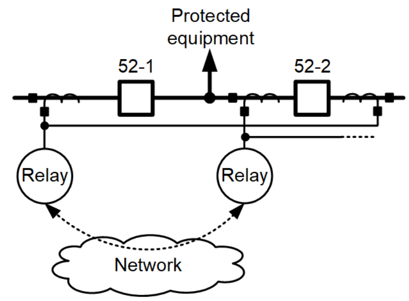

Fig. 15. Relay-in-the-yard application example.

In both examples discussed previously, the network impacts on the overall DSS reliability are not considered. The network will consist of network switches, which can be expected to further decrease the overall system reliability considerably, especially with the application of improper networking architecture and knowledge. For further discussion on networking complexities, refer to [15].

One solution to eliminate the concern regarding the networking architecture on the system reliability is the utilization of P2P architecture, as seen in Fig. 16. In this architecture, data are streamed via direct connections from yard-applied MUs to control house-applied subscribers without the introduction of a network switch. This technology is easy to apply with little to no substation networking knowledge. This dramatically reduces the risks of misoperation as the result of a networking error and thus greatly improves system reliability.

When comparing the availability of a system with regard to electronic device count, this system will have improved performance over an SV MU application. In this architecture, data are synchronized using a port ping-pong technique; therefore, a high-accuracy clock is not critical to the performance of the protection system. This means the example protection system is reliant on correct operation of three electronic devices instead of four from the SV MU example. Thus, this system would have approximately one-third the reliability of a conventional system.

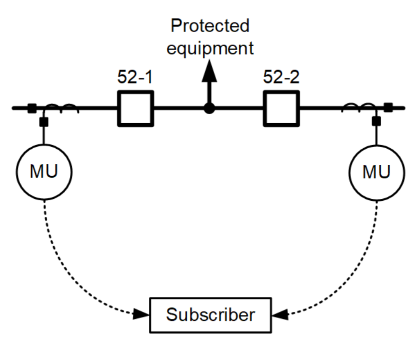

Fig. 16. P2P architecture application example.

The addition of parallel signal paths can increase the overall system reliability but cannot increase the reliability beyond that of a conventionally applied protection system. An example of this is the application of multiple MUs at each breaker in Fig. 14. An equally sized resistor circuit can be used as an analogy to compare the performance of a system by parallel combinations. One can imagine this electronic device combination as a current measurement from the combination of four equally sized resistors in series, as shown in Fig. 17. If an additional MU is placed at Breaker 52-1, the circuit becomes that of Fig. 18. This improves the availability of the overall system, similar to how a parallel resistor combination reduces the overall resistance of a circuit, thus increasing the measured total current. Though, it could never increase the overall availability of the system beyond that of a singular electronic device, similar again to how a single paralleled resistor in a series combination circuit could not reduce the circuit resistance beyond that of a singular resistance, assuming all resistances equal. The only way to improve availability beyond a singular system is applying two or more complete systems in parallel.

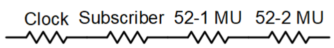

Fig. 17. Availability circuit representation of Fig. 14.

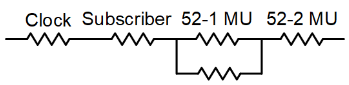

Fig. 18. Availability circuit representation with addition of MU.

As is evident in the relay-in-the-yard example, applying protective relays in the substation yard near the system apparatus will result in an improved system reliability, as compared to SV systems with protection applied in a subscribing unit. The reliability savings are due to the reduction in electronic device count. One method to retain some reliability in an SV solution is to apply intelligence in the MU, per [13]. Applying intelligence within the MU and hosting some localized protection back into the MU will increase the system reliability, though not to the point of a conventionally applied protection system.

B. Complexity

The complexity of a system also has an impact on the performance of the system. The more complex a system is, the more likely a human error is to cause an undesired operation. It is a good practice as a design engineer to make a system only as complex as needed to accomplish the overall intended goal.

Substation yard-installed protective relaying also results in a signal reduction in protection schemes. Fig. 19, Fig. 20, and Fig. 21 provide examples of the signals required of a typical protection system for various DSSs. Solid lines in these figures represent control wired signals, and dashed lines represent signals shared across the substation PB or SB. The figures provide example signals used to fully protect the bay-tapped equipment and include signals required for the breaker failure protection of Breaker 52-1. Signals would be replicated in neighboring bay sections. When inspecting these application examples, users may notice that the relay-in-the-yard example in Fig. 21 requires the smallest number of signals shared across the substation PB or SB. The application examples requiring MUs, whether they are intelligent or not, require network paths for the same number of discrete signals. Based on these observations, it can be argued that relay-in-the-yard applications provide the least complex solution with respect to the number of routed signals required while maintaining the same functionality.

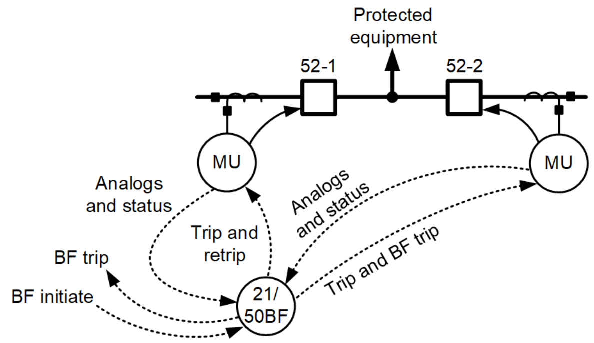

Fig. 19. Example of signal requirements in an SV application with simple MUs.

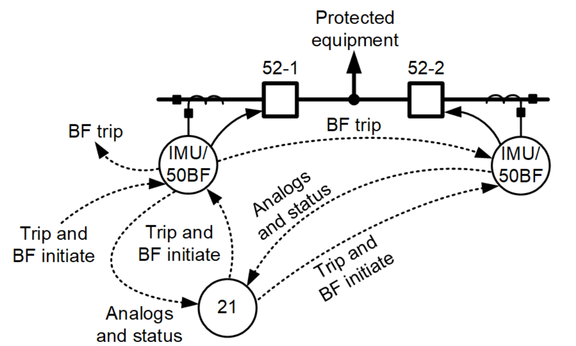

Fig. 20. Example of signal requirements in an SV application with IMUs.

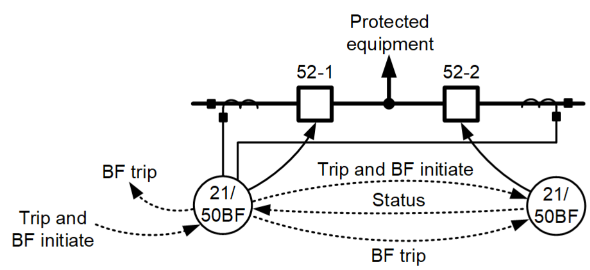

Fig. 21. Example of signal requirements in a relay-in-the-yard application.

When comparing the design of the relay-in-the-yard example application provided in Fig. 21, it is easy to discern that this system provides the simplest DSS solution when compared against those of Fig. 19 and Fig. 20. This system results in the smallest amount of signal routing, and all routed signals would be identically mapped from device to device in a completed substation application. When comparing Fig. 19 to Fig. 20, what is not as obvious is an added complexity involved in the simple MU application example provided in Fig. 19, as compared to the IMU application example provided in Fig. 20. When comparing the trip signals in the two application examples, users notice this signal is shared with one other signal in each application. Furthermore, one observation from the IMU application example is that the shared signal is always the breaker failure initiate signal, regardless of the breaker the trip signal is routed. In Fig. 19, however, the shared signal differs depending on the breaker the trip signal is routed through. This adds a complexity to the system and, more importantly, is a complexity that can very easily be overlooked in application implementation. One solution to eliminate this complexity is to separate the trip signal with the other shared signals in Fig. 19; however, doing so increases the routed signal count in the application example and would result in lower reliability.

P2P architecture, shown in Fig. 16, can also significantly reduce the application complexity due to the elimination of networking equipment as well and the elimination of high-accuracy satellite-synchronized clocks. The utilization of P2P architecture greatly simplifies an overall DSS design, because it is configured very similarly to a conventionally wired system with only an extension of the device digitization. One big expense with a networked DSS is the budget required to train employees on those systems. This expense is greatly minimized and negligible in P2P architecture applications because of its close similarities to conventionally wired systems.

C. Experience With Installing Digital Devices in the Yard

The Chongqing CEPREI Industrial Technology Research Institute in China studied the impact of outdoor installations on MUs in hundreds of substations. This study illustrated the negative impacts on digital devices that were installed in the yard, were fairly new to the market, and did not have a proven track record of field installation [16]. Reference [16] explains the challenges to the PB based on unavailability of system components, which include:

- High-field failure rate.
- Unexpected maintenance and repair.
- Large economic losses.
- Serious accidents.

[The] analysis of the products and suppliers reveals the possible reasons for the poor reliability, which include:

- Insufficient reliability design and review.
- Material defects.
- Assembly process problems.
- Absence of reliability acceptance test [16].

From these results, it can be seen that it is necessary to require the same design and type tests and manufacturing processes for MUs and IMUs as for protective relays. "IEC 61869-13 defines the required type tests, insulation, electromagnetic compatibility (EMC), and safety requirements for [stand alone merging unit (SAMU)] devices" [17]. "Recognizing the fact that new devices are typically mounted in the immediate vicinity of the high-voltage breakers, IEC TC 38 based their recommendations for the standard on the wealth of information available from substation yard based relay installations" [17]. These end users conclude that new SAMU devices are exposed to similar conditions and must meet or exceed the general capabilities defined in the IEC 60255 series of standards. SAMU EMC requirements defined in IEC 61869-13 match IEC 60255-26 with safety requirements based on [18].

In contrast, Elektro Eletricidade e Serviços S.A., a large electric distribution utility in Brazil, designed a digital emergency control system in which the feeder, bay control, and transformer relays are installed directly in the yard and communicate using IEC 61850 GOOSE messages for the protection and control schemes, including breaker failure and bus protection, interbay interlocking, event report triggers, and automatic transfer between high-voltage lines [19]. The adoption of IEC 61850 made it possible to build a decentralized automation system (distributed over several IEDs) and dramatically reduce copper while updating brownfield stations. By placing relays in the yard near the primary equipment, the modernization team was able to avoid the expense of testing and terminating existing wiring contacts as well as eliminate most of the long runs of copper wiring. By using metrics for availability and resiliency found in IEC 61508, the supplier and customer team engineered a design to create a digital system predicted to be more reliable than the traditional one that it replaced. For example, the project to date includes several hundred relays, with over 65 percent of the feeder relays installed in the yard while, due to the potential corrosion of seaside locations, the others were installed in control buildings. The system in-service metrics include a reduction in maintenance interventions, and based on the meticulous record-keeping of the engineering team and supplier quality division, it is known that the relays and satellite-synchronized clocks in the yard experienced the same high availability as those in the control building. It is important to note that for SV applications, though clocks may be robust enough to survive in the yard, multiple distributed time sources are more complicated than a single, or redundant, centralized time source. The innovative use of GOOSE reception disturbance alarms converts failures that, when unmonitored, are classified in IEC 61508 as "dangerous undetected failures" into "dangerous detected failures," which are then alarmed and corrected [20]. Other metrics include a significant reduction in the interruption of power delivery to [end users] because of the quick restoration of the system after a disturbance. Situations [in the past that] needed two to three hours to be identified, analyzed, and released for re-energization are now re-energized almost immediately because of the robust automation schemes implemented. The success of these outdoor installations has not only led to modernization of many more Elektro stations, but also served as a roadmap for other utilities to safely do the same. The relay supplier has designed and tested the clocks, STA and OT SDN Ethernet switches, relays, and MUs to the same high standards with the same manufacturing standards for mission-critical electronic devices. MUs based on the same proven relay platform have a large installed base from which end users have become confident in reliability and availability.

Reference [21] describes insulation-level and electrical clearance recommendations for the use in air-insulated electrical power substations. Although miniaturization of relays and MUs is often done, if it is unnecessary, it can be avoided. "Printed circuit boards [(PCBs)] that conduct high voltages can be victimized by an electrostatic discharge between exposed metal if that metal is too close together. This discharge can potentially cause damage to the board and its components, and [PCB] designers need to observe proper spacing between metal conductors on the board. Conductor spacing on a circuit board, like that of the substation itself, is measured using creepage, the distance between two conductors on the surface of the board or along the surface of the insulating material, and clearance, the line-of-sight distance between two conductors through the air"

[21]. Like air-insulated substations, air-insulated DSS devices benefit from appropriate component spacing.

Programmable electronic devices withstand greater temperature ranges and have a prolonged service life when designed to be large enough to support appropriate spacing between parts and components to satisfy safety, electromagnetic, EMC, and environmental standards.

D. Speed

The speed of protection is critically important to power system performance. The speed of fault detection and isolation has a direct impact on power system stability and power quality. The faster a fault is detected and isolated, the less likely the power system is to reach its critical clear time and maintain stability and the better the power quality. Therefore, when we analyze a DSS performance, the speed of detection and isolation is very important in the analysis.

In a conventionally wired system, signals move at close to the speed of light between the power system primary equipment and protective relaying. When comparing a conventionally wired system against any DSS, one can expect additional delay in the DSS. An IEC 61850-9-2-compliant system introduces two additional delays into protection operation when compared against the conventionally wired system. The first delay is in the SV stream publication, often referred to as an SV publication operational delay, which is typically a 3-sample delay, which at 4,800 Hz is 625 µs. Another operational delay of the SV is the subscription time, which is typically between 1.5 and 3 milliseconds and accommodates both the publication and network delay. This is a one-time delay and is not accumulative for each new SV publication. The next delay introduced is a GOOSE operational delay. GOOSE messaging publishes information in a burst of messages in rapid succession starting at the moment of a state change before reverting to a heartbeat message publication at a constant but slow rate. The maximum GOOSE transmission delay will be dependent on which GOOSE publication is received by the subscriber. If the first or subsequent packets are buffered or dropped, an additional delay is added to the system until the subscriber receives a message with a change of state. The design and performance of the Ethernet network will determine how many GOOSE packets are lost in scenarios, such as network reconfiguration caused by a port or cable failure. OT SDN or OT RSTP networks have very different network recovery times that vary from 10 µs to 15 ms or more. Due to the variety of network performance characteristics and design choices available for the sake of this discussion, we assume a worst-case network recovery time of less than 15 ms to satisfy an overall protection function application time of 30 ms, as shown in Table XI [22]. This recovery time is common in OT RSTP networks. GOOSE transmit delays are accumulative and added based on the number of GOOSE transmit paths in the series of a protection function. The SV operational delay and GOOSE operational delay are also accumulative with one another.

TABLE XI
TIMING OF DIGITAL MESSAGES PERFORMING PROTECTION FUNCTIONS

Signaling messages	LAN recovery time	Transfer time	Application time (digital input to digital output)
1st (t_0)	No failure	<3 ms	<14 ms
2nd (t_0 + 4 ms)	<3 ms	<8 ms	<18 ms
3rd (t_0 + 8 ms)	<7 ms	<12 ms	<22 ms
4th (t_0 + 16 ms)	<15 ms	<20 ms	<30 ms

If this discussion is applied to the application examples provided in Fig. 19, Fig. 20, and Fig. 21, comparisons can be made of the speed performance in the three applications. The worst-case delay in each application can be determined, assuming a breaker failure event and a fault located on the neighboring (left) circuit to Breaker 52-1, as compared to what is represented in the figures. Protection and processing delays are added until fault isolation is achieved. In doing so, it can be concluded that the additional operational delay included in the example SV applications (Fig. 19 and Fig. 20) is as high as 35 ms. When comparing the relay-in-the-yard application (Fig. 21), the additional operational delay is as high as 32 ms.

If the comparison analysis is performed, assuming breakers operate as desired, the additional operational delay of each system will improve. When only considering the additional operational delay, assuming the breaker operated as intended, one can expect an additional delay as high as 19 ms, which is the maximum network reconfiguration delay (16 ms) plus the SV subscription operational delay (3 ms) in the SV application. In the relay-in-the-yard application, no additional delay would be expected on top of a conventional wired system if the relay is directly tripping both breakers. If the relay utilizes GOOSE messages to trip the adjacent breaker, an additional delay as low as 4 ms and as high as 16 ms can be expected.

E. Functions Requiring High-Resolution Data

The speed at which the power system can be restored to normal operating service also impacts the performance of the power system. The quicker the system can be restored, the better the power system performance. When temporary faults occur on the power system, automatic reclosing schemes are employed to restore the system to normal after a short, programmed open period. However, if the fault was permanent, the fault must first be located and cleared by utility linemen prior to restoration. Locating permanent faults more quickly provides a tremendous cost savings to the utility and better power quality to the end user.

This is evident in the first ever purchase of a microprocessor-based relay. The purpose of the first ever microprocessor relay purchase was so the utility could locate faults on its circuits quicker. Prior to the advent of microprocessor relays, fault locating was very crude and could only be determined to be on a percentage of the line, often upwards of 60 to 80 percent of the circuit. Fault-locating techniques have improved since the first purchase of a microprocessor relay in 1984. Most notably, modern relays offer the capability of locating faults using the traveling waves generated from the fault. This technique provides fault-locating accuracies within 300 meters of the actual location, a significant improvement from phasor-based locating techniques in early generation microprocessor relays.

Traveling-wave fault locating (TWFL) is becoming very popular, and many utilities are adding TWFL into their relay panel standards. When designing a DSS, it may be important to the designer and company for the system to include TWFL techniques. TWFL techniques, however, require the sampling of power system signals with high resolution, something that would be very difficult to support using SV streams. One manufacturer requires a sampling resolution of at least 1 MHz for TWFL implementation.

An SV stream transmission has strict requirements for message size and determinism. Though the message size of an SV stream may be small in comparison to other Ethernet protocols, the rate at which the stream is published far exceeds other protocols. To avoid lost packets, the latency of the system must be far less than the publishing rate of the stream. Per [23], latency is introduced by switch port latency and transmission delays. Switch port latency delays are dependent on the network switch design, and the transmission delays are dependent on the frame size, as compared against the network port throughput. For the sake of this discussion, we will assume no delays are introduced from the switch port latency. In a proper network design, however, this delay must not be ignored. Reference [23] provides a good explanation of the limitations that signal latency plays on SV stream transmissions.

Equations (2) and (3) can be used to calculate the latency limitations using various IEC 61850-9-2 [light edition] and IEC 61869-9 publication techniques. Of most interest to this discussion is the capabilities of various techniques at analog quantity sampling rates of 1 MHz due to the sampling requirements of TWFL. If (2) and (3) are first solved, assuming the rest of the data structure meets the protection requirements of IEC 61850-9-2 LE, the maximum frame size would be 203 bytes (i.e., 1,624 bits). This data structure includes a single sample of eight analog quantities. Some variances in frame size can be observed based on the chosen SV identifier. Using (2), with a single analog quantity sample per frame and sampling rate of 1 MHz, the SV frame publication period can be found to be 1 µs. Now using (3), the minimum throughput of the network to support this publication without losing packets would be 1.63 Gbps. Again, this does not account for any switch port latency. This also assumes one data stream; however, in most dual-breaker applications, at least two data streams are required. If a subscriber is receiving two data streams, the throughput requirement would effectively double or require a 3.25 Gbps link.

$$\mathrm{T\_SV} = \frac{\mathrm{ASDU}}{\mathrm{S\_rate}} \tag{2}$$

$$\mathrm{BW} = \frac{(\mathrm{F\_S})}{(\mathrm{T\_SV})} \tag{3}$$

where:

T_SV = SV frame publication period
ASDU = number of analog quantity samples per frame
S_rate = analog quantity sampling rate
BW = minimum network port throughput
F_S = frame size in bits

Through careful inspection of (2) and (3), there are two knobs available for adjustment to control the required port throughput, assuming the sampling rate is fixed at 1 MHz. The first technique would involve adding more data samples into the same frame. The second is reducing the number of analog quantities published in the frame, which effectively reduces the frame size. Adding more samples into a frame would effectively increase the frame publication period; at the same time, it increases the frame size. The frame size, however, does not increase linearly with the increase in additional samples because frame overhead is only included once. Reducing the analog quantity count within each frame will often result in larger throughput savings. However, the best results can be achieved by applying both techniques together.

TWFL requires, at minimum, three current analog quantities. Next, one can reduce the analog quantity count to three and also increase the samples per frame to two. This will cause a frame-size reduction, resulting from the reduction of quantities, and will increase the frame publication period to 2 µs. This results in a frame size of 178 bytes (i.e., 1,424 bits). This would then reduce the minimum port throughput requirement of a single stream to 0.72 Gbps. Though still difficult, this stream is more manageable than the stream with eight analog quantities and one sample per frame. The stream is limited in that it only supports three current signals and no voltage signals and, therefore, cannot be used for many purposes other than TWFL in the time-domain realm.

A more recent transmission line innovation is the ability to detect the incipient stages of faults, such as dirty or failing insulators and vegetation encroachment. The innovation gives the ability to detect and correct the problem before it turns into a conventional transmission line fault, resulting in an outage and potential equipment failure. This function is also gaining popularity with utilities as a performance-based maintenance tool. The function requires three voltage signals along with three traveling-wave current signals and requires 1 MHz sampling rates. If the number of analog quantities is increased to six and two samples are combined per frame at the same publication rate, the bandwidth capabilities need to be no less than 1.02 Gbps, assuming a 254 byte or 2,030 bit frame. To support a dual-breaker application with two streams, a minimum bandwidth of 2.04 Gbps would be required.

All throughput requirements mentioned are quite high, especially when considering the number of 1 MHz SV streams expected inside a substation, the addition of the switch port latency, addition of other layered protocols, addition of other equipment SV streams, and limitation of relay port processing capabilities. It is therefore important to consider alternatives to TWFL application within the DSS in the substation.

One way to eliminate the concern of throughput requirements of a 1 MHz SV stream is to apply an electronic device with intelligence in the substation yard. The yard application of the TWFL function would eliminate the need for SV publication of signals. In modern day, this is done with the application of a relay in the yard. Potential future yard TWFL dual-breaker IMU applications may require very high Ethernet network data rates and message processing. A non-Ethernet direct protocol reduces bandwidth requirements, because it omits the Ethernet overhead information from each data frame. Another benefit of this connection is the use of P2P architecture, because there is only one data stream on each network connection. Similarly, a DSS with P2P architecture provides another solution to reduce signal bandwidth.

F. Future Development

Protection systems have evolved over the last 25 years since IEC 61850 first became a concept and are expected to evolve over the decades to come. With DSS integration in the electric power system, new ideas in protection concepts should be expected. To best support these new and changing ideas, intelligence should be installed in the substation yard to facilitate easy integration of advancing technologies.

One example of a new idea made easily possible with DSSs is the concept of breaker differential. This is a percentage restraint differential concept that takes advantage of the common application of applying an MU to measure and publish analog samples from CTs located on each side of a circuit breaker, as seen in Fig. 22. The main advantage of such a system is very quick fault identification and better fault sensitivity to faults within the breaker chamber.

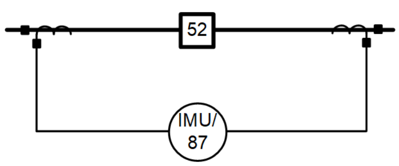

Fig. 22. Breaker differential application example.

This concept can be applied through the use of a simple MU; however, it is cheaper and easier to apply if MUs with intelligence are applied. In a simple MU application, a dedicated subscribing relay is required to support such a differential application. In this application, the differential element would also require a network to interconnect the MU to the subscribing unit. However, if an IMU is applied, the differential element can be applied within the IMU, making the element simpler to apply and operation not reliant on networking.

VI. Asset Monitoring Impacts

Since 1998, the data within a substation have evolved significantly. Low-speed, low-bandwidth serial communications have given rise to Ethernet-based communications. Rudimentary primary system monitoring at low resolution using transducers has been replaced by high-resolution information from intelligent devices. File transfers for system events and asset health are now commonplace in OT networks. Incorporating new methods in both existing and new locations presents significant challenges.

Commonly, field equipment is connected by a network of ducts and trenches of a fixed capacity to intelligent devices in a remote building. As more points are monitored and conductors are installed, it comes at the cost of future equipment. Conductors must be sized for the voltage, voltage type, current required, and distance. Something as simple as monitoring a digital contact requires a dedicated conductor to monitor contact state. It is common for design choices to be made, and points become grouped together logically to provide summary status and save on terminal block space and installed conductor count. This sacrifices a detailed system and asset monitoring.

Tradeoffs become apparent when attempting to monitor a breaker's trip circuit. When viewed as a system, trip coils are a subset within a complex system of electrical circuits and mechanical linkages required for successful operation of a breaker. The trip coil converts electrical energy to the mechanical energy required to move a linkage, causing the breaker to operate and extinguish a system fault. In high-reliability applications, multiple trip coils may be present for each pole of a breaker. Depending on the voltage level and application, a three-phase breaker can have between one and six trip coils that need to be monitored. When applied in parallel, and in normal operation, the force required to actuate the breaker is shared between the two trip coils. However, each trip coil must be capable of generating the force required to operate the tripping mechanism should a failure render one coil unable to actuate the breaker successfully. This presents significant challenges to effective monitoring of the tripping system. Maintaining and monitoring these critical circuits to ensure effectiveness is an item identified by NERC and is included in regulatory standards.

In widespread practice, a protective relay located quite some distance away completes an electrical circuit that initiates the operation of a breaker. Both the physical separation between the device or contacts initiating the tripping of the breaker, and the number of coils used, present challenges to effective monitoring. It has been a frequent practice to use rudimentary circuits and indicators to monitor these critical circuits. Fig. 23 provides one example.

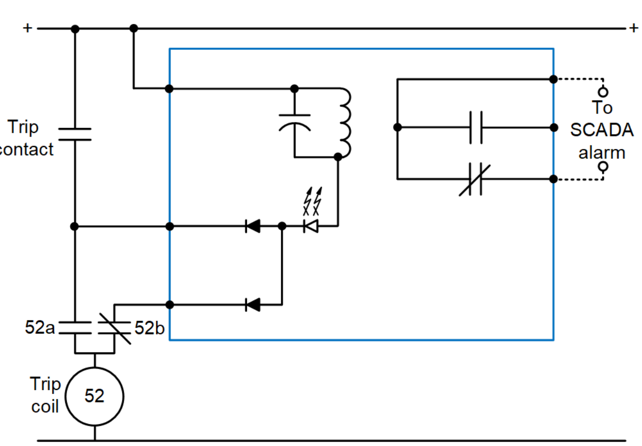

Fig. 23. Breaker trip coil continuity monitor example [24].

This circuit's implementation requires installing additional dedicated contacts, conductors, and terminal blocks to provide constant power and SCADA indication between the field assets and the control building. The information obtained provides few predictive indicators of the health of the complex tripping system beyond basic circuit continuity.

In contrast to this rudimentary approach to monitoring, the current waveshape recorded by a trip coil provides a fingerprint for the specific breaker tripping system. The magnitude of the voltage and current in addition to the current waveshape can provide predictive indicators about the tripping system holistically. Fig. 24 provides an example breaker trip coil current signature.

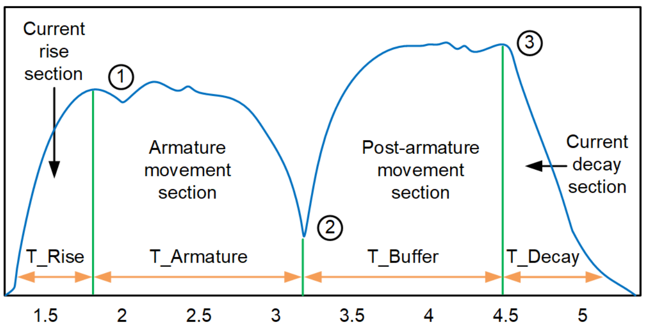

Fig. 24. Breaker trip coil current signature example [25].

The first interval, T_Rise, represents the initial current rise of the coil current upon closure of the device initiating the trip operation. Once the coil is fully energized, the circuit enters the second region, T_Armature, where current begins to drop as the armature moves through the trip coil windings, reaching a local minimum and where the armature contacts the breaker trip bar. In the third region, T_Buffer, as the trip coil begins to exert work on the breaker trip linkage, the current rises in relation to the force required to actuate the breaker. The fourth region, T_Decay, represents the current decay characterized by the specific electrical properties of the trip coil. Using this information, potential failures in both the electrical and mechanical properties of the tripping system can be identified. Mechanical linkage misalignments and indications of subtle changes in trip circuit impedance can be diagnosed by examining this waveshape. Incorporating intelligence into field-mounted MUs allows these data to be easily captured and recorded. High-resolution data make information like this possible and more informative; therefore, downsampling to satisfy PB protocols may degrade the performance of these intelligent monitoring features.

The monitoring of the asset cabinet and ambient temperatures allows for the correlation between weather and system performance. Next-generation trip system monitoring is sensitive enough to detect changes in trip coil ambient temperatures. With the digitization of cabinet temperatures, changes in recorded waveshapes can easily be correlated to variations in temperature. This is a key indicator to discern between weather-related changes or indicators of future system failure.

Once an IMU is installed in field equipment, additional detailed asset monitoring becomes a small incremental change. For the breaker asset example, it becomes much easier to expand detailed trip coil monitoring to include breaker gas pressure and tank heater operation.

The power system uses SF_6 gas for its pressure stability across a wide temperature range and as an insulator in many breaker applications. To prevent liquification at low temperatures, tank heaters are installed. If the gas pressure reaches a level too low, the breaker will be blocked from operation or will proactively open. To monitor gas volume, discrete thresholds are set for minimum gas pressure with a status point used for indication to SCADA. With an IMU located in or near the field equipment, the SF_6 gas pressure can be digitized and measured as an analog quantity. By digitizing ambient temperature and breaker tank heater current draw, a detailed model can be constructed to diagnose changes in both breaker gas pressure and tank heater operation. These digitized analog quantities can be included in event records and sent to an operations center or asset monitoring system. Once a central system has this detailed digitized information, it becomes trivial to use forecast weather temperature as a predictive function of gas pressure and tank heater operation. Now, predictions can be made for asset maintenance, allowing field crews to perform maintenance efficiently and proactively.

VII. Conclusion

Increases in substation digitization over the past decades have greatly expanded data possibilities within the substation. DSS designs all have different performance capabilities, and all these capabilities should be well understood prior to choosing a design implementation. The design of best fit for each company might differ depending on what is important to that company. The primary goal of a DSS is to provide the best performance to the primary power system with which it is controlling at a respectable cost. Therefore, when considering a DSS, the performance of the electric power system should be prioritized. It is also important to consider the present and future needs of substation protection on control systems when evaluating DSS design. Placing IMUs or relays close to primary equipment in the yard enables modern protection and monitoring capabilities unavailable in simple MU based on IEC 61850 SV. IMUs and relays often sample power system values at a much higher frequency than required for IEC 61850 SV publication and must downsample these values to the publication period that may degrade the sample resolution. Different publication rates being discussed in IEC 61869 will still require downsampling from the state-of-the-art IMUs sample rates as they range up to MHz rates. The yard application of a relay or IMUs are recommended for enhanced protection and monitoring functions, such as:

- Asset and breaker trip coil monitoring.
- Circuit breaker differential for better sensitivity to faults within the breaker chamber and fault identification.
- Advanced grid monitoring, including traveling-wave and time-domain elements for improved power quality monitoring and protection of existing systems and IBRs.

This paper introduced key secondary system performance characteristics, such as reliability, complexity, and speed. Through an analysis, we learned as functions are installed closer to the primary system apparatus, each of the three performance characteristics see improvement. Furthermore, installing intelligence in the substation yard improves monitoring and recording capabilities on the DSS as well as of the primary power system. To support advanced features, such as TWFL or advanced trip coil monitoring, substation yard intelligence is required.

VIII. References

[1] IEC 61850-5, *Communication Networks and Systems in Substations* – Part 5: Communication Requirements for Functions and Device Models, 2003.

[2] P. Schaefer, "Why is 'Ether' in Ethernet?" *International Journal of Communication*, Vol. 7, 2013, pp. 2,010–2,026.

[3] IEC 61850-9-1, *Communication Networks And Systems In Substations* – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled Values Over Serial Unidirectional Multidrop Point To Point Link, 2003.

[4] J. Bettler, J. Silva, D. Morman, R. Abboud, D. Bowen, E. Cenzon, and D. Dolezilek, "Case Studies of IEC 61850 Process Bus Systems Using GOOSE and Sampled Values: Recent Installations and Research," proceedings of the 47th Annual Western Protective Relay Conference, virtual format, October 2020.

[5] SEL 2021 Catalog, January 2021.

[6] J. L. Blackburn, *Protective Relaying: Principles and Applications*, 3rd ed., Marcel Dekker, New York, NY, 1998, pp. 190–195.

[7] J. Bettler, R. McDaniel, and D. Bowen, "Performance of IEC 61850 Sampled Values Relays for a Real-World Fault," proceedings of the 49th Annual Western Protective Relay Conference, Spokane, WA, October 2022.

[8] K. Leggett, R. Moxley, and D. Dolezilek, "Station Device and Network Communications Performance During System Stress Conditions," proceedings of the 1st Annual Protection, Automation and Control World Conference, Dublin, Ireland, June 2010.

[9] D. Dolezilek, "Ethernet Design for Teleprotection and Automation Requires a Return to First Principles to Improve First Response," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

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

[11] A. McDonald, A. Dolezilek, and D. Dolezilek, "Hidden in Plain Sight: Anticipating and Avoiding Hidden Failures in Communications-Assisted Protection," proceedings of the 47th Annual Western Protective Relay Conference, virtual format, October 2020.

[12] A. Genz, D. Haas, and K. Zimmerman, "Test the Right Stuff: Using Data to Improve Relay Availability, Reduce Failures, and Optimize Test Intervals," proceedings of the 75th Annual Conference for Protective Relay Engineers, College Station, TX, March 2022.

[13] V. Skendzic, I. Ender, and G. Zweigle, "IEC 61850-9-2 Process Bus and Its Impact on Power System Protection and Control Reliability," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[14] D. Dolezilek, P. Lima, G. Rocha, A. Rufino, and W. Fernandes, "Cost and Performance Comparison of Numerous In-Service Process Bus Merging Unit Solutions Based on IEC 61850," proceedings of the 10th Annual Protection, Automation and Control World Conference, Glasgow, United Kingdom, June 2019.

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

[16] Z. Jia-yong, H. Sheng-zong, C. Tie-zhu, and Y. Sheng-jun, "Study of Highly Accelerated Life Test for Merging Unit of Intelligent Substation," proceedings of the 18th International Conference on Electronic Packaging Technology, Harbin, China, August 2017.

[17] V. Skendzic and D. Dolezilek, "News from the Editor – Updates and Enhancements to Process Bus IEC 61850-9-2 and Related Standards," proceedings of the 14th International Conference on Developments in Power System Protection, Belfast, United Kingdom, March 2018.

[18] IEC 60255-27, *Measuring Relays and Protection Equipment* – Part 27: Product Safety Requirements, 2013.

[19] S. Kimura, A. Rotta, R. Abboud, R. Moraes, E. Zanirato, and J. Bahia, "Applying IEC 61850 to Real Life: Modernization Project for 30 Electrical Substations," proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

[20] IEC 61508-1, *Functional Safety Of Electrical/Electronic/ Programmable Electronic Safety-Related Systems* – Part 1: General Requirements, 2010.

[21] IEEE Std 1427, *IEEE Guide for Recommended Electrical Clearances and Insulation Levels in Air Insulated Electrical Power Substations*, 2020.

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

[23] P. S. P. Junior, R. C. Bernardino, C. M. Martins, P. S. Pereira, and G. E. Lourenco, "Analyzing the Limits of Data Transmission in the Process Bus," proceedings of CIGRE Session 48, Paris, France, August 2020.

[24] *SEL-2652 Trip Coil Monitor Instruction Manual*. Available: selinc.com.

[25] S. S. Biswas, A. K. Srivastava, and D. Whitehead, "A Real-Time Data-Driven Algorithm for Health Diagnosis and Prognosis of a Circuit Breaker Trip Assembly," *IEEE Transactions on Industrial Electronics*, Vol. 62, Issue 6, June 2015, pp. 3,822–3,831.

IX. Biographies

John Bettler has a BSEE from Iowa State University of Science and Technology and an MSEE from Illinois Institute of Technology (IIT). John has worked at Commonwealth Edison Company (ComEd), a power company in the Chicago area, for 29 years. He has experience as a field engineer and protection engineer. Currently, he is the principal engineer for ComEd's relay division. His team's purview includes 4 kV and 12 kV feeders up to 765 kV transmission lines and all transmission and distribution equipment in between (e.g., transformers, buses, cap, and inductors). John's team also reviews interconnections, independent power producers, and distribution generation projects. John is also adjunct faculty at IIT and University of Wisconsin-Madison teaching power and protection classes. He is a PE in Illinois.

David Dolezilek is a principal engineer at Schweitzer Engineering Laboratories, Inc. (SEL) and has three decades of experience in electric power protection, automation, communication, and control. He develops and implements innovative solutions to intricate power system challenges and teaches numerous topics as adjunct faculty. David is a patented inventor, has authored dozens of technical papers, and continues to research first principles of mission-critical technologies. Through his work, he helped coin the term operational technology to explain the difference in performance and security requirements of Ethernet for mission-critical applications versus IT applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of UCA2, and a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a member of the IEEE, the IEEE Reliability Society, and several CIGRE working groups.

David Bowen, a Certified Technician (CTech), graduated from the Electrical Engineering Technologist program at Georgian College in Barrie, Ontario, Canada. He is currently a senior application technologist for automation products in the sales and customer service division at Schweitzer Engineering Laboratories, Inc. (SEL). David has held this position with SEL since 2008. In this role, he provides training and assistance to customers applying SEL power system protection, automation, and communication products. Before coming to SEL, he spent 17 years working in protection, control, and automation departments at utilities in the greater Toronto area. During this time, he performed system integration for protective relays in applications ranging from 230 kV utility substations and low-voltage distribution to electromechanical relays and modern digital relays. David specializes in power system automation, legacy system integration protocols, and modern IEC 61850-based systems.

Shawn Westervelt earned his BS in electrical engineering in 2012 and MS in Electrical Engineering in 2015 from Wichita State University. He was employed with Westar Energy, where he validated system fault study models. Then, he was employed with Omaha Public Power District, where his responsibilities included substation automation, SCADA, protective relaying for transmission and distribution applications, and digital fault recorder applications. In 2019, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as an application engineer. He provides training and assistance to customers applying SEL power system automation and communication products. Shawn is a registered professional engineer in the state of Nebraska. He is a member of the IEEE.

Josh LaBlanc received his BS in electrical engineering from the University of North Dakota in 2011. Upon graduating, he worked for an oil and gas pipeline company, Enbridge Energy, until 2014. In 2014, he joined the utility industry working for Minnesota Power’s relay and maintenance engineering department for 6 years. He is presently an application engineer with Schweitzer Engineering Laboratories, Inc. (SEL), where his primary roles are providing application support and training on protection-related topics in all areas of power system protection. Josh is a registered professional engineer in the state of Minnesota.

20231020 • TP7136-01