Cost and Performance Comparison of Numerous In-Service Process Bus Merging Unit Solutions Based on IEC 61850

David Dolezilek, Paulo Lima, Geraldo Rocha, Augusto Rufino, and William Fernandes
Schweitzer Engineering Laboratories, Inc.

Presented at the
FISE IEEE/CIGRE Conference
Medellín, Colombia
December 4–6, 2019

Originally presented at the
10th Annual Protection, Automation and Control World Conference, June 2019

Cost and Performance Comparison of Numerous In-Service Process Bus Merging Unit Solutions Based on IEC 61850

David Dolezilek, Paulo Lima, Geraldo Rocha, Augusto Rufino, and William Fernandes,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—In this paper, we make a comparative analysis of the performance, resiliency, and security of several in-service digital secondary system architectures based on the IEC 61850 communications standard. We summarize the recent work done by several technical standards development organizations to further define process bus components. Working Group K15 of the IEEE Power System Relaying Committee on Centralized Substation Protection and Control has defined the terms *merging unit, remote input/output module, process interface unit/device,* and *intelligent merging unit*. IEC 61869-9:2016 has added two new conformance classes of merging units, bringing the total to four. These are consistent with the switchgear controller defined by IEC 62271-3:2006. Multiple in-service process bus DSS designs, based on these descriptions, are considered as extensions to the same typical station bus system.**

Next, using numerous international standards, we create necessary and sufficient design criteria for installation, performance, and availability. Using these acceptance criteria , we evaluate numerous process bus merging unit designs and use measured and observed information from in-service systems to compare speed, cost, and reliability.

I. Introduction

This paper is an expansion of [1] and provides a comparative analysis of the various communications network topologies and process instrumentation and control devices. The analysis includes the reliability of various systems in terms of unavailability. The cost and complexity of each solution is also evaluated along with the level of expertise required by maintenance teams to detect failures and restore system operation. Performance is evaluated based on the speed of detection and reaction to a power system fault.

Transmission, distribution, and industrial engineers have applied digital communications, including the IEC 61850 communications standard, in power substation energy control systems (ECSs) to reduce the large volume of cables in traditional installations. An installation is considered traditional if the interconnections are made through low-level analog signals via copper wires between equipment in the yard and protection and control intelligent electronic devices (IEDs) in the control house. It is also considered traditional if the IEDs for transfer tripping and latching are connected by electric cables.

Station bus communications are human-to-machine (H2M) connections and protocols that transmit and receive system information and send operator commands to networked IEDs. These communications perform information exchange, including exchange for supervisory control and data acquisition (SCADA), monitoring, metering, and engineering access.

Process bus communications are machine-to-machine (M2M) connections and protocols that exchange input/output (I/O) process information between IEDs and process instrumentation and control devices, including data acquisition devices, instrument transformers, and controllers.

M2M information exchange for interlocking, automation, and protection among IEDs is deployed on the station bus or process bus or both. M2M information exchange for interlocking, automation, and protection between IEDs and process instrumentation and control devices is considered process bus communications. M2M time distribution is deployed on the station bus or process bus or both.

Numerous protocols are in use in modern ECS networks for process bus communications and copper reduction strategies, including IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and IEC-61850-9-2 Sampled Values (SV) messaging, IEC 61158 EtherCAT, IEEE C37.118.2-2011 Synchrophasor Protocol, Precision Time Protocol (PTP), and MIRRORED BITS communications [2]. ECS process bus communications need to be reliable, fast, cost-effective, cybersecure, and designed for a 25-year service life.

The IEC 61850 standard establishes three major forms of data exchange:

- H2M client-server Manufacturing Message Specification (MMS) protocol for supervision and control applications.
- M2M publisher-subscriber GOOSE messaging for interrupt-driven fast messaging of status and processed analog values.
- M2M publisher-subscriber SV messaging for fast periodic messaging of raw sampled analog values of current and voltage signals.

In designing an ECS protection system, engineers must devise a solution that is economically feasible and satisfies the performance requirements for protection: speed, safety, reliability, selectivity, and sensitivity appropriate to the criticality and characteristics of each application.

Reference [3] compares three protection and control system designs:

- A scheme with traditional wiring.
- An I/O MU located in the substation yard with a serial fiber-optic link to the IED in the control house.
- An I/O MU located in the substation yard with an Ethernet fiber-optic link to the IED in the control house.

II. Internationally Standardized Process I/O Devices

Recent work done by several technical standards development organizations provides standard definitions for process bus components based on their capabilities.

Working Group K15 of the IEEE Power System Relaying Committee on Centralized Substation Protection and Control defines process bus components as follows [4]:

- Centralized protection and control (CPC): “A system comprised of a high-performance computing platform capable of providing protection, control, monitoring, communication and asset management functions by collecting the data those functions require using high-speed, time synchronized measurements within a substation.”
- Merging unit (MU): “Interface unit that accepts multiple analog CT/VT [current transformer/voltage transformer] and binary inputs and produces multiple time synchronized serial unidirectional multi-drop digital point-to-point outputs to provide data communication.” IEEE considers an MU to be an analog input device that transmits raw analog signals to a logic processor in a separate IED via a local-area network (LAN) rather than an internal data bus in the same IED.
- Remote I/O module (RIO): “[The module] is intended to be the status and control interface for primary system equipment such as circuit breakers, transformers, and isolators.” RIOs based on IEC 61850 communications support GOOSE exchange of Boolean equipment signals and optionally support MMS.
- Process interface unit/device (PIU/PID): “[This unit] combines an MU and a RIO into one device.” PIU/PIDs publish raw analog values and Boolean equipment status signals and subscribe to control signals for equipment operation.
- Intelligent MU (IMU): “The IMU … adds RMS-based [root-mean-square-based] (simple to derive from sampled values) overcurrent and overvoltage backup protection functions in a PIU/PID to prevent damage to the related primary equipment in the event of total communication failure between the IMU and CPC during abnormal system conditions.”

IEC 61869-9:2016 describes four conformance classes of MUs. IEC 61869 is a standard for instrument transformers with a digital interface compliant with IEC 61850. It is also backward-compatible with the UCA International Users Group’s “Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2” [5]. The IEC defines the conformance classes as follows [6]:

- Class a: “The minimal set of services required to transmit MU data using sampled values (M2M SV).”
- Class b: “Class a capabilities plus the minimal set of services required to support GOOSE messages (M2M SV plus M2M GOOSE).”
- Class c: “Class b capabilities plus the implementation of the IEC 61850 series’ information model self-descriptive capabilities (M2M SV plus M2M GOOSE plus H2M data models and self-description).”
- Class d: “Class c capabilities plus services for file transfer and either one or more of un-buffered reporting and buffered reporting, or logging (M2M SV plus M2M GOOSE plus H2M data models and self-description plus H2M MMS for monitoring and control).”

IEC 62271-3 describes digital interfaces based on IEC 61850 for switchgear and control gear. The IEC defines the classes as follows [7]:

- Class a: “Minimal services to operate switchgear – simple GOOSE only device.”
- Class b: “Services to support IEC 61850 information model (logical nodes) with self-description.”
- Class c: “All services applicable for a specific LN [logical node]; configuration, file transfer, logging.”

III. Signal Exchange, Device, and LAN Acceptance Criteria Based on International Standards

Using the performance and availability criteria from the appropriate international standards, we evaluate and then measure and observe the numerous process bus MU designs. We use information from in-service systems to compare speed, cost, and reliability.

The necessary list of international standards to define message delivery performance and quality and device quality criteria includes:

- IEC 61850-3 – Communication Networks and Systems in Substations – Part 3: General Requirements.
- IEC/TR 61850-90-4 – Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines.
- IEEE 1646-2004 – IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.
- IEEE 525-2016 – IEEE Guide for the Design and Installation of Cable Systems in Substations.
- IEC 60834-1:1999 –Teleprotection Equipment of Power Systems – Performance and Testing – Part 1: Command Systems.
- NERC PRC-005-2 – Protection System Maintenance.
- IEEE C37.2 – IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations.

- IEEE C37.236-2013 – IEEE Guide for Power System Protective Relay Applications Over Digital Communication Channels.
- IEC/TR 61850-90-1 – Communication Networks and Systems for Power Utility Automation – Part 90-1: Use of IEC 61850 for the Communication Between Substations.
- IEC 60870-4, Telecontrol Equipment and Systems – Part 4: Performance Requirements.
- IEEE 802.1 – Standard for Local and Metropolitan Area Networks.
- IEC 15802 Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks.
- IEEE 1613-2003 – IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations.

In accordance with these standards, the ECS must be designed to perform protection signal exchange that meets the following criteria:

- Have a signal exchange success rate greater than 99.99 percent.
- Achieve an expected signal transfer time between devices of less than 3 ms.
- Achieve an expected signal transit via LAN of less than 1 ms.
- Have a maximum data delivery time between devices within a substation of less than 0.25 cycles.
- Have a maximum data delivery time between devices external to a substation of less than 8–12 ms, as illustrated in Table I, from IEEE 1646-2004 [8].

The LAN must be designed in accordance with these signal exchange and performance criteria to avoid failure. However, the design must also anticipate failure and have built-in resilience that meets the following criteria:

- Boolean protection logic with fewer than 4 dropped GOOSE packets and momentary outages shorter than 16 ms.
- Analog protection calculations with fewer than 4 dropped SV packets and momentary outages shorter than 433 µs.
- Failover within each device that occurs within one logic-processing interval.

LAN faults must be detected and isolated, and a dual-primary data path must be made available that is fast enough to deliver the protection signal. Therefore, a momentary outage is defined for each signal exchange. Longer sustained outages may prevent the communications-assisted protection from operating.

It must be recognized that communications will eventually fail and the design must have built-in resilience to compensate.

IV. In-Service Process Bus Application Scenarios

This paper uses analysis methods first illustrated in [3] to compare designs for replacing traditional copper wiring with Ethernet communications. The Ethernet communications replace analog CT and VT signals and Boolean equipment status and control signals with digital communications via MUs and IMUs. Communications channel design choices include shared-bandwidth switched Ethernet networks and point-to-point links. In this paper, we consider reliability, cost, and ease of diagnostics to evaluate the solutions.

TABLE I
SUBSTATION LINE PROTECTION AND CONTROL COMMUNICATIONS PERFORMANCE REQUIREMENTS

Data/Application	Critical Class	Priority Class	Rate	Maximum Delivery Time
Breaker tripping and breaker failure initiate	High	High	On demand	0.25 cycles*
Backup breaker tripping (after breaker failure time-out)	High	High	On demand	8 to 12 ms
Breaker reclosure, including voltage-supervised and multiple	Medium	Normal	On demand	8 ms
Control of transfer trip for Send/Receive	High	High	On demand	0.25 cycles
Keying for permissive schemes	High	High	On demand	8 ms
Send/Receive trip command	High	High	On demand	2 to 8 ms
Initiate lockout function (not in mechanical lockout)	High	High	On demand	16 ms
Motor-operated disconnect	Medium	Normal	On demand	16 ms
Indicator control (On, Off, Blink, etc.)	Medium	Normal	On demand	1 s
Testing of trip and block channels	Medium	Low	On demand	1 s

* Actual breaker operation may take 1.5 to 8 cycles.

In Section VI, an example application with a one-line diagram is used to aid analysis. The IED types used for this comparison are MU1, MU2, PCM3, PCM4, and PCM5. They are defined as follows.

MU1 is a process bus publisher device with an I/O interface to the process-level Boolean equipment status, control, and analog signals from CTs and VTs. It has internal logic processing for protection and automation. This device is an IEEE IMU and IEC 61869-9 Class d MU with M2M SV, M2M GOOSE, H2M data models and self-description, and H2M MMS for monitoring and control. The device also supports protocols for process bus publications, including IEEE C37.118.2-2011, PTP, and MIRRORED BITS communications.

MU2 is a process bus publisher device with an I/O interface to the process-level Boolean equipment status, control, and analog signals from CTs and VTs. This device is an IEEE PIU/PID that publishes raw analog values and Boolean equipment status signals and subscribes to control signals for equipment operation based on IEC 61158 EtherCAT.

PCM3 is a process bus subscriber protection, control, and monitoring device with internal logic processing for protection and automation and no I/O interface to the process level. This device receives Boolean equipment status, control, and analog signals from CTs and VTs via digital messaging. This device is an IEEE CPC with M2M SV plus M2M GOOSE. The device also supports protocols for process bus publications, including IEC 61850 GOOSE, IEEE C37.118.2-2011, PTP, and MIRRORED BITS communications. It supports data models and self-description plus H2M station bus protocols, including MMS, Telnet, File Transfer Protocol (FTP), Distributed Network Protocol (DNP3) LAN/wide-area network (WAN), IEEE C37.118.2-2011, PTP, and Simple Network Time Protocol (SNTP).

PCM4 is a process bus subscriber protection, control, and monitoring device with internal logic processing for protection and automation and no I/O interface to the process level. This device is an IEEE CPC that receives Boolean equipment status, control, and analog signals from CTs and VTs via IEC 61158 EtherCAT. It also supports protocols for process bus publications, including IEC 61850 GOOSE, IEEE C37.118.2-2011, PTP, and MIRRORED BITS communications. It supports data models and self-description plus H2M station bus protocols, including MMS, Telnet, FTP, DNP3 LAN/WAN, IEEE C37.118.2-2011, PTP, and SNTP.

PCM5 is a process bus subscriber protection, control, and monitoring device with internal logic processing for protection and automation and also has an I/O interface to the process level and receives Boolean equipment status and control via digital messaging. It is both an IEEE CPC and an IMU with M2M GOOSE. The device also supports protocols for process bus publications, including IEC 61850 GOOSE, IEEE C37.118.2-2011, PTP, and MIRRORED BITS communications. The device supports data models and self-description plus H2M station bus protocols, including MMS, Telnet, FTP, DNP3 LAN/WAN, IEEE C37.118.2-2011, PTP, and SNTP.

We will consider the following solutions:

- Scenario A—MU1 is in the yard sending information to PCM3 in the control house with communications based on networked or point-to-point Ethernet connections. PCM3 has station bus connections in the control house.
- Scenario B—MU2 is in the yard sending information to PCM4 in the control house with communications based on point-to-point Ethernet connections. PCM4 has station bus connections in the control house.
- Scenario C—PCM5 is in the yard without an MU for local protection logic. It also serves as an IEC 61869-9 Class d MU for other station devices. It is communicating process bus and station bus information over networked or point-to-point Ethernet connections to devices in the control house.

V. Reliability Analysis Using Device Rate of Failure and Unavailability

In this section, we evaluate the unavailability of the protection system, taking into account the mean time between failures (MTBF) and mean time to repair (MTTR) of equipment and devices involved. To simplify the comparative analysis, we disregard common points of failure. For the economic analysis, we consider the cost of equipment involved, such as switches, MUs, cables, and fiber as well as the design costs and level of expertise required to perform diagnostics on the system already in operation. As a summary, we present the comparison between solutions in a table, including unavailability, costs, and level of difficulty for maintenance and diagnostics.

A system consists of several components, for which reliability can be expressed in more than one way. A common measure is the probability that a device will become unavailable to perform functions vital to system operation. If the unavailability of system components is known, a fault tree analysis allows us to predict the unavailability of any system.

The failure rate of a device is the number of failures expected over a period of time. It is common to express these data as the MTBF.

Availability and unavailability are usually expressed as probabilities [9]. For all equipment used in the analysis, the failure rates are based on field data or, where field data are lacking, equipment that has the same level of complexity and is exposed to the same operating conditions.

Given the MTBF and the time needed to detect and repair the problem, unavailability can be calculated as shown in (1).

$$q \cong \lambda \bullet \mathrm{MTTR} = \frac{\mathrm{MTTR}}{\mathrm{MTBF}} \tag{1}$$

where:

q = unavailability.

λ = constant failure rate.

$\mathrm{MTBF} = \dfrac{1}{\lambda}$.

Each failure leads to an MTTR period where the equipment is unavailable. The system is unavailable for a fraction of the MTBF. Therefore, system unavailability is equal to $\frac{\text{MTTR}}{\text{MTBF}}$ [9] [10] [11] [12].

For each IED with automatic internal failure detection, we use a detect and repair time of 48 hours, or MTTR = 48 hours. For devices that do not have self-diagnosis, we will describe how MTTR is obtained. Average unavailability is adequate for comparative analyses [3].

A. Ethernet Switch

Several switch manufacturers provide devices with high reliability. For one of these switches, the manufacturer indicates an MTBF of 500,000 hours. Unavailability is shown in (2).

$$q = \frac{48 \text{ hours}}{500{,}000 \text{ hours}} = 96 \bullet 10^{-6} \tag{2}$$

B. IED Ethernet Interface

Data based on a manufacturer's experience shows a 2,500-year MTBF for the Ethernet interface of IEDs designed for substation environments. Unavailability is shown in (3).

$$q = \frac{48 \text{ hours}}{2{,}500 \text{ years} \bullet 365 \text{ days} \bullet 24 \text{ hours}} = 2 \bullet 10^{-6} \tag{3}$$

C. Electrical Cable Connection

Reference [13] states that manufacturer statistics show a 5,000-year MTBF for electrical cable connections, assuming functional tests have been performed as well as the aging of a new facility. Reference [14] states that connections in terminal strips have an MTBF of 4,400 years or more.

It is common practice in power companies to not have an automatic fault detection system for wiring, so the average time to detect these faults is half the periodic maintenance time. For this paper, a two-year test interval was considered. Unavailability for the electrical cable connections is shown in (4).

$$q = \frac{1 \text{ year}}{5{,}000 \text{ years}} = 200 \bullet 10^{-6} \tag{4}$$

D. Power Cable Connection for IEDs and Analog Signals

The connection of cables for power and other analog signals is considered with the same MTBF as electrical cables for I/O, but since there is monitoring, it is considered to have an MTTR of 48 hours. The unavailability for the electrical cable connections for powering the IEDs is shown in (5). This same unavailability can be considered for the current and voltage analog signals.

$$q = \frac{48 \text{ hours}}{5{,}000 \text{ years} \bullet 365 \text{ days} \bullet 24 \text{ hours}} = 1.1 \bullet 10^{-6} \tag{5}$$

E. Monitored Fiber-Optic Connection

In the absence of field data, we considered the failure rate of a fiber-optic connection equal to the failure rate of an electrical cable connection—a conservative estimate. Since the fiber connection has self-monitoring, an MTTR of 48 hours is assumed. Unavailability for the fiber connections is shown in (6).

$$q = \frac{48 \text{ hours}}{5{,}000 \text{ years} \bullet 365 \text{ days} \bullet 24 \text{ hours}} = 1.1 \bullet 10^{-6} \tag{6}$$

F. Merging Unit

MUs are relatively new devices and there is no historical data for failure rates measured from field experience. One manufacturer has a 300-year MTBF for protection and control IEDs. Considering that MUs have the same level of complexity, have very similar hardware, and are manufactured for installation in the same environment as protection and control IEDs and that some MUs even incorporate protection functions, this paper considers the MTBF of an MU equal to the MTBF of a protective relay. Unavailability for an MU is shown in (7).

$$q = \frac{48 \text{ hours}}{300 \text{ years} \bullet 365 \text{ days} \bullet 24 \text{ hours}} = 18 \bullet 10^{-6} \tag{7}$$

G. Global Positioning System (GPS)

Data based on a manufacturer's experience shows a 500,000-hour MTBF for GPS equipment designed for substation environments. Unavailability is shown in (8).

$$q = \frac{48 \text{ hours}}{500{,}000 \text{ hours}} = 96 \bullet 10^{-6} \tag{8}$$

A summary of results is shown in Table II.

TABLE II
APPROXIMATE AVAILABILITY OF SYSTEM COMPONENTS

Component	**Unavailability ($1 \bullet 10^{-6}$)**	**Availability (%)**	**Stationary Time Equivalent (minutes)**
Ethernet switch	96	99.99040	50.46
IED Ethernet interface	2	99.99978	1.15
Electrical cable connection	200	99.98000	105.15
Power cable connection for IEDs and analog signals	1.1	99.99989	0.58
Monitored fiber-optic connection	1.1	99.99989	0.58
MU	18	99.99817	9.60
GPS	96	99.99040	50.46

VI. EXPECTED UNAVAILABILITY OF DIGITIZATION SOLUTIONS

This section includes descriptions and block diagrams for each solution as well as the expected unavailability based on fault tree analysis.

We use fault tree analysis to compare several solutions, so the focus will be given to the differences between them. That is, everything that is common between the solutions does not influence this analysis and is disregarded in the evaluations.

A. Scenario A—MU1 in Ethernet Network

Fig. 1 shows the block diagram and Fig. 2 shows the fault tree for Scenario A. In the example, MU1 is installed in a junction box in the substation yard and receives digital and analog signals electrically.

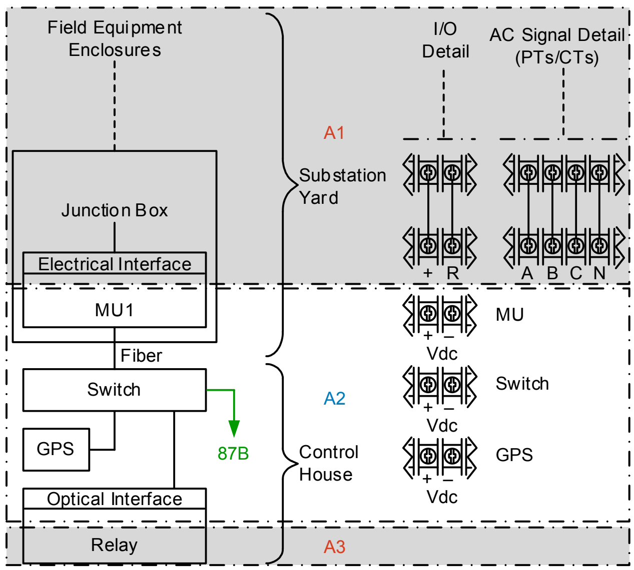

Fig. 1. Block diagram for Scenario A—MU1 in an Ethernet network.

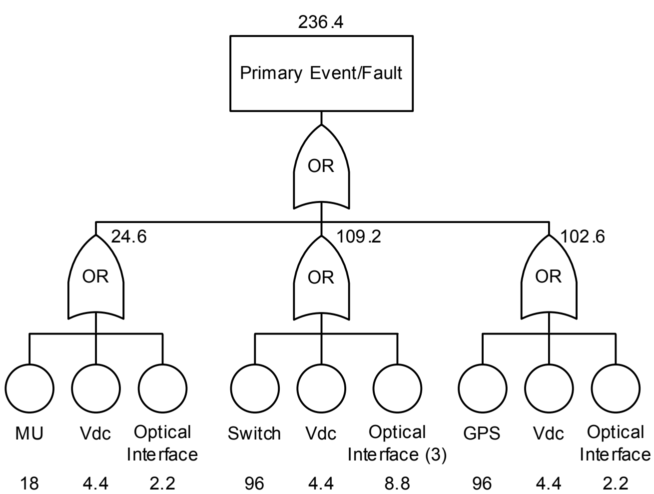

Fig. 2. Fault tree for MU in an Ethernet network (the multiplier for all unavailability is 10^{-6}).

In Fig. 1, the shaded areas (A1 and A3) represent what is common to all solutions and therefore is disregarded in this analysis. The white area (A2) represents the specific characteristics of MU1 in an Ethernet network scenario; they are:

- MU1: hardware and power cable pair with four connections and optical interface for connection to the switch.
- Ethernet switch: switch hardware, MU switch power cables with four connections and optical interfaces for connection to the MU, GPS, and IED. It is considered an optical interface, which is the connection to the IED.
- GPS: GPS hardware, a pair of cables for GPS power with four connections, and an optical interface for connection to the switch.

The fault tree for this solution is shown in Fig. 2. The loss of any analog or digital signal is the primary event, so failures related to MUs, switches, and GPS must be added through an OR logic gate.

The unavailability shown in Fig. 2 is related only to the association of components present in A2.

The digital and analog signals provided for the line-gap protective relay are also available for other applications, such as differential busbar protection.

B. Scenario B—MU2 With Point-to-Point Link

Fig. 3 shows the block diagram and Fig. 4 shows the fault tree for using an MU with a point-to-point link. In the example, MU2 is installed in the junction box and receives digital and analog signals.

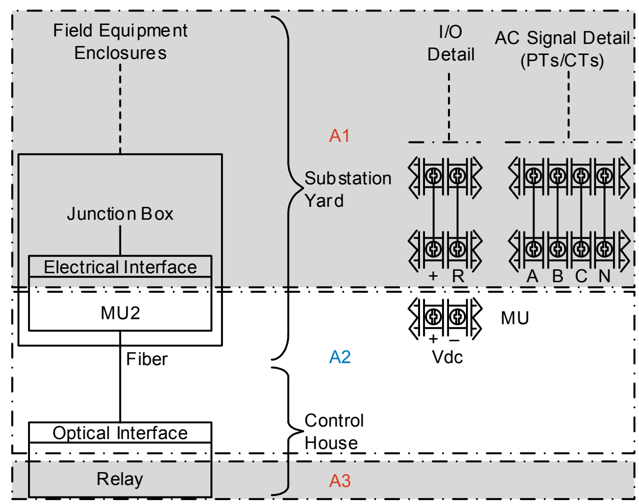

Fig. 3. Block diagram for Scenario B—MU2 with a point-to-point link.

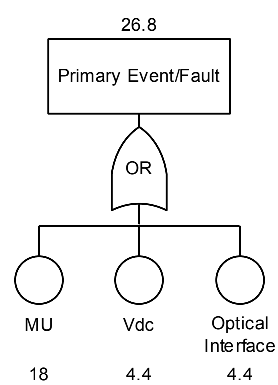

Fig. 4. Fault tree for an MU with a point-to-point link.

In Fig. 3, the white area (A2) represents the specific characteristics of MU2 with a point-to-point link scenario; they are:

- MU2: hardware, a pair of power supply cables with four connections, and an optical interface for connection to the IED.
- A relay optical interface.

The fault tree for this solution is shown in Fig. 4. The loss of any analog or digital signal is considered the main event; thus, we have to add the faults related to the MU and the optical interface of the relay.

C. *Scenario C—Field-Installed PCM5 Relay/CPC/IMU*

Fig. 5 shows the block diagram and Fig. 6 shows the fault tree for a field-installed PCM5 relay solution. In this case, the protective relay is located in the position occupied by the MU in the previous scenarios.

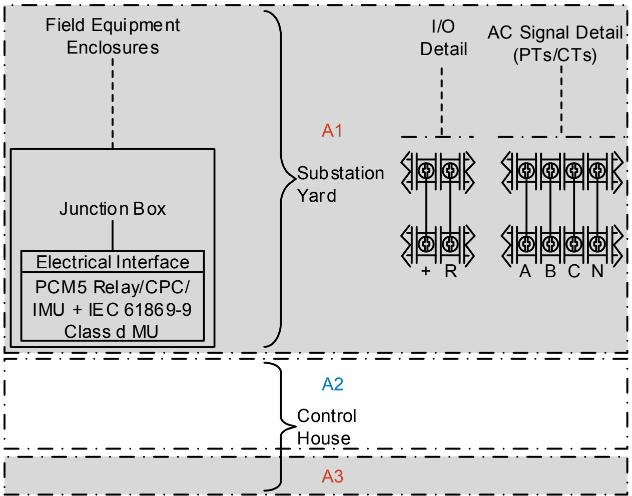

Fig. 5. Block diagram for Scenario C—field-installed PCM 5 relay/CPC/IMU.

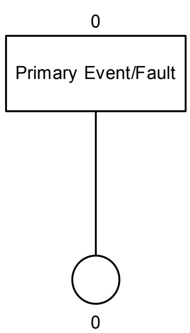

Fig. 6. Fault tree for a field-installed relay.

In Fig. 5, the white area (A2) represents the specific characteristics of the field-installed relay solution. There is no item to be considered as a specific feature. All parts of this solution are present in the other solutions, including:

- A relay for protection and control.
- The electrical interface of the relay (considered in the relay itself or in the MU in all solutions).

The fault tree for this solution is shown in Fig. 6. The loss of any analog or digital signal is the main event. Although the relay also serves as an IMU and IEC 61869-9 Class d MU, these functions are not necessary for the bay protection applications in this analysis.

It should be noted that the result of zero unavailability is not the total unavailability of the system. Because it is a comparative analysis, all non-zero values for unavailability in all solutions can be interpreted as the main differences between those solutions and the field-installed relay solution.

An advantage of the field-installed PCM5 relay/CPC/IMU plus IEC 61869-9 Class d MU capability is that it can also provide SV for other applications besides bay protection. Fig. 7 shows a hardware solution that incorporates protection and control functions in addition to the MU functions. Thus, there is the protection and control of the bay with high availability and also sharing of the signals for other applications. Fig. 7 shows, as an example, the provision of SV for the differential busbar relay. Because we are only analyzing the reliability of the protection and control for the bay, the equipment needed to provide the signal for the differential busbar relay is not considered in the unavailability calculation.

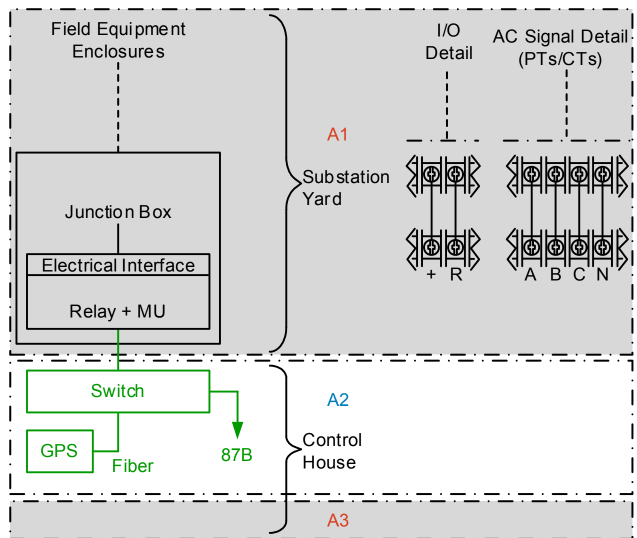

Fig. 7. Block diagram for a field-installed relay with MU functionality.

VII. Cost Analysis and Ease of Detection of Failures

The reliability analysis shows that the field-installed relay solution has the lowest unavailability of the solutions analyzed. However, other aspects are commonly considered by companies for investment decisions. This section provides an analysis of the costs and the ease of failure diagnostics and maintenance to make a more complete comparison between each solution.

A. Cost Analysis

Table III shows the hardware and services needed to implement each solution. Because we are doing a comparative analysis, we used the criterion of elimination of common items to determine a ranking of costs. The field-installed relay solution represents the lowest cost, followed by the MU with a point-to-point link, and then the MU in an Ethernet network.

TABLE III
COMPARATIVE COST ANALYSIS

Item/Solution		**MU Ethernet**	**MU Point-to-Point**	**Field Relay**
Hardware	Protection and control relay	X	X	X
	MU	X	X	
	Switch	X		
	GPS	X	X	X
	Ethernet fiber interface	X	X	X
Services	Relay panel design	X	X	X
	Project panel MU	X	X	
	Automation panel design	X		
	Fiber launch	X	X	X
	Relay configuration	X	X	X
	MU configuration	X	X	
	Network configuration	X		
Cost Rank*		3	2	1

* Lower is better.

B. Analysis Regarding Ease of Maintenance and Fault Diagnostics

Table IV shows the tools and knowledge that the maintenance team would need to diagnose failures in each solution. As in the cost analysis, the criterion of elimination of common items was used to determine a ranking of ease of maintenance diagnoses. The field-installed relay solution represents the greatest ease of use, followed by the MU with a point-to-point link and then the MU in an Ethernet network.

TABLE IV
COMPARATIVE ANALYSIS OF DIAGNOSIS AND MAINTENANCE

Item		**MU Ethernet**	**MU Point-to-Point**	**Field Relay**
Tools	Relay software	X	X	X
	MU software	X	X	
	Switch	X		
	GPS software	X	X	X
	Conventional test enclosure	X	X	X
	SV test enclosure	X	X	
	Network analyzer	X		
Knowledge	Protection engineering	X	X	X
	SV network engineering	X		
Maintenance Rank*		3	2	1

* Lower is better.

C. Other Considerations Related to IEC 61850 SV

1) Sampling Rate

A standardized sampling rate is one of the main requirements for achieving interoperability between MUs and protection and control relays. The IEC 61850-9-2LE guide defines a sampling rate of 4.8 kHz for protection and operational metering applications and 15.36 kHz for power quality and disturbance recording [5]. These defined sampling rates result in limitations for some applications already used today:

- Modern protective relays have oscillographs with sampling rates on the order of 8 kHz, allowing for more detailed and accurate analysis of event transients [15].
- Relays that have protection functions in the time domain require a sampling rate on the order of 10 kHz. These functions allow transmission protection times up to ten times faster than phasor-based elements [16].
- Traveling-wave fault locating requires sampling rates between 1 and 5 MHz, depending on the technology employed. This technology allows accurate fault locating, independent of the attributes and length of transmission lines [17].

The solution shown in Fig. 7, a protective relay with MU functionality, allows all these applications that require a sampling rate above that established by IEC 61850-9-2 LE to be implemented in the MU hardware. As IEC 61850 evolves, it is being superseded by IEC 61869, which has expanded numerous process bus definitions to improve interoperability and provide flexibility for much higher sampling rates.

2) *Time Synchronization*

Another aspect to be considered in relation to the use of MUs is the need for external time synchronization. In this paper, we only evaluate unavailability of the GPS device and its Ethernet connection to the process bus. However, there are other factors to consider, such as antenna reliability, GPS holdover, and the ability of the GPS device to connect with different network constellations [18].

VIII. Conclusion

Working Group K15 of the IEEE Power System Relaying Committee on Centralized Substation Protection and Control describes CPCs, MUs, RIOs, PIU/PIDs, and IMUs for digital secondary systems. IEC 61869-9:2016 describes four conformance classes of MUs compatible with IEC 61850-9-2 for SV and IEC 62271-3. These classes roughly match up with the IEEE PIU/PID, RIO, MU, and IMU devices.

This work shows that the allocation of protection and control IEDs in the substation yard presents the best index regarding reliability, costs, and ease of maintenance and fault diagnosis. The point-to-point MU solution presents the second best performance. The MU in an Ethernet network solution ranks last. The field-installed relay with built-in MU functions has the advantage of making analog and digital values available for other applications and is the most reliable scheme.

There are some limitations of application imposed by the sampling rate provided by IEC 61850-9-2 and the need for an external timing source, which makes the protection less available. For an MU in an Ethernet network, the inclusion of protection features in the MU itself is recommended to increase the reliability of the protection and control systems.

IX. References

[1] P. Lima, J. Ferreira, G. Rocha, A. Rufino, "Subestação Disgital: Qual a Solução Mais Confiável e Econômica?," proceedings of the Seminário Nacional de Produção e Transmissão de Energia Elétrica, Curitiba, Brazil, October 2017.

[2] D. J. Dolezilek and A. Kalra, "Comparison of Standardized Protocols Available to Replace Substation Copper Field Wiring With Digital Communications," proceedings of the 14th International Conference on Developments in Power System Protection, Belfast, United Kingdom, March 2018.

[3] G. W. Scheer and R. E. Moxley, "Digital Communications Improve Contact I/O Reliability," proceedings of the 7th Annual Western Power Delivery Automation Conference, Spokane, WA, May 2005.

[4] Working Group K15, "Centralized Substation Protection and Control," IEEE PES Power System Relaying Committee Report of Working Group K15 of the Substation Protection Subcommittee, December 2015. Available: www.pes-psrc.org/kb/published/reports/IEEE_PES_PSRC_WG%20K15_Report_CPC_Dec_2015.pdf.

[5] UCA International Users Group, "Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2," July 2004. Available: iec61850.ucaiug.org/implementation%20guidelines/digif_spec_9-2le_r2-1_040707-cb.pdf.

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

[7] IEC 62271-3, High-Voltage Switchgear and Controlgear – Part 3: Digital Interfaces Based on IEC 61850, 2015.

[8] IEEE 1646, IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, 2004.

[9] G. W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," proceedings of the 4th Annual Substation Automation Conference, College Station, TX, April 1998.

[10] E. O. Schweitzer, III, B. Fleming, T. J. Lee, and P. M. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[11] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, *Fault Tree Handbook*, NUREG-0492m U.S. Nuclear Regulatory Commission, Washington, DC, 1981. Available: www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/.

[12] G. W. Scheer, "Comparison of Fiber-Optic Star and Ring Topologies for Electric Power Substation Communications," proceedings of the 5th Annual Substation Automation Conference at Texas A&M, College Station, TX, March 1999.

[13] R. Sandoval and J. L. Eternod, "Evaluation of Methods for Breaker-Flashover Protection," proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, October 2004.

[14] W. Denson, G. Chandler, W. Crowell, A. Clark, and P. Jaworski, *Nonelectronic Parts Reliability Data*, Ft. Belvoir Defense Technical Information Center, Griffiss AFB, NY, 1994.

[15] *SEL-421-4, -5 Relay Protection and Automation System Instruction Manual*, July 2016.

[16] E. O. Schweitzer, III, B. Kasztenny, and M. V. Mynam, "Performance of Time-Domain Line Protection Elements on Real-World Faults," proceedings of the 69th Annual Conference for Protective Relay Engineers, College Station, TX, April 2016.

[17] E. O. Schweitzer, III, A. Guzmán, M. V. Mynam, V. Skendzic, and B. Kasztenny, "Locating Faults by the Traveling Waves They Launch," proceedings of the 67th Annual Conference for Protective Relay Engineers, College Station, TX, April 2014.

[18] S. V. Achanta, L. Thoma, R. Rice, and D. Rippon, "Is Your Clock Ticking All the Time? Characterizing Substation-Hardened Clocks for Automation," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2016.

X. Biographies

David Dolezilek is the international technical director at Schweitzer Engineering Laboratories, Inc. and has three decades of experience in electric power protection, automation, communication, and control. He leads a team that 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 has created methods to specify, design, and measure service level specifications for digital communication of signals, including class, source, destination, bandwidth, speed, latency, jitter, and acceptable loss. As a result, he helped coin the term operational technology (OT) 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.

Paulo Lima received his B.S.E.E. from Federal University of Itajubá (UNIFEI), Brazil, in 2012. He has been an application protection engineer for Schweitzer Engineering Laboratories, Inc. (SEL) since 2012, providing technical support for industrial customers in Brazil. Currently working as application engineer and technical support coordinator in Brazil, he is an instructor at SEL University Brazil and has authored and coauthored several technical papers.

Geraldo Rocha received his B.S.E.E. from UNESP (Universidade Estadual Paulista Campus de Bauru, Brazil) in 2001 and specialized in electrical power systems protection at UFRJ (Universidade Federal do Rio de Janeiro). He worked as a protection and automation engineer for CPFL Geração de Energia S.A., where his responsibilities included maintenance, commissioning, specification, and studies of the protection and automation of hydroelectric plants. In 2007, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as an application engineer covering the entire country of Brazil. Since 2017, he has served as the regional sales and marketing manager for SEL Brazil and is the author of numerous technical papers published for national seminars and conferences in Brazil.

Augusto Rufino received his B.S.E.E. from Federal University of Itajubá (UNIFEI), Brazil, in 2007. He received a postgraduate degree in project management (MBA) from Padre Anchieta University, Brazil, in 2014 and a specialist in substation automation from the National Telecommunications Institute (INATEL), Brazil, in 2017. Since 2013, he has been part of the Schweitzer Engineering Laboratories, Inc. engineering services design team, working in the area of protection, control, and substation automation projects.

William Fernandes is an application engineer at Schweitzer Engineering Laboratories, Inc.

20190412 • TP6918-01