Replacing Uncertainty With Predictability at Xcel: Risk-Driven Evaluation of Digital Secondary Systems

Lauren Donati
Xcel Energy

David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
62nd Annual Midwest Power Systems Conference
Saint Paul, Minnesota
November 10–12, 2026

Replacing Uncertainty With Predictability at Xcel: Risk-Driven Evaluation of Digital Secondary Systems

Lauren Donati, *Xcel Energy*
David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper describes the decision-making information needed and the methodology used to evaluate device installation methods as well as digital communications and networking technologies. Xcel Energy's goal is to establish an engineering process that produces digital system designs as reliable as the traditional hardwired systems they are intended to replace.**

Digital programmable relays, controllers, real-time automation devices, and Ethernet switches operate according to software-defined logic. Their features, application-specific functions, and operational behavior configurations are defined using software applications. Protection-related settings, such as instantaneous and time-overcurrent magnitudes, recloser inrush thresholds, rate-of-change-of-frequency limits, and access control permissions, are all established and modified through configuration software. Communications ports, connections, and networks are likewise software-defined, as they are used to replace traditional hardwired protection signals and trip circuits in digital secondary systems.

The utility's objective is to adopt designs that improve reliability while enhancing human performance. They expect the digital secondary system to influence human performance improvement by reducing tedious manual activities of calibration, configuration, and data gathering, thus minimizing opportunities for human error. Configuration files created during the software definition of protection, automation, and control will serve as the foundation for defining the data flows required in the communications system.

I. Introduction

Digital systems offer the opportunity to perform continuous self-testing and automate fault detection and annunciation. They also generate, store, and publish detailed diagnostic and troubleshooting data. Xcel Energy intends to leverage this information to understand the health and behavior of the primary system, equip technicians with better situational awareness, and extend the time between field service visits.

The utility will then evaluate various communications technologies and architectures that can support these data flows and meet established criteria for cost, performance, and long-term maintainability. Of particular interest are the choices for Ethernet communications from the substation yard into the control building to support protection signal communications via IEC 61850 Generic Object-Oriented Substation Event (GOOSE), Sampled Values (SV), and Manufacturing Message Specification (MMS); IEEE/IEC 61588 Precision Time Protocol (PTP); IEC 62439 Parallel Redundancy Protocol (PRP); and open-source manufacturer configuration protocols. It is well understood that the abstract communication service interface (ACSI) defined in IEC 61850-7-2 allows data to be mapped onto non-IEC 61850 protocols without violating the conceptual model of the IEC 61850 standard. The utility will evaluate the risk associated with various manufacturers' nonstandardized protocols, and they anticipate that accommodations will need to be considered for manufacturers that use undocumented, private, and secretive engineering access and configuration protocols.

II. Communications Networks for Secondary Systems Associated With Electric Power Primary Systems

IEC 61850-5 defines the primary system as a "set of all components for generating, transmitting, and distributing electrical energy" in Section 3.1.9. It defines the secondary system as an "interacting set of all components and subsystems to operate, to protect and to monitor the primary system" in Section 3.1.8. It defines the communications system as the "interconnected set of all communication links" in Section 3.1.10 and the substation automation system (SAS) as a "system which operates, protects, monitors, etc. the substation, i.e. the primary system" in Section 3.1.7. Based on these terms, the digital secondary system (DSS) is an SAS that is a collection of digital devices that communicate to operate, protect, and monitor the primary system. The communications links that interconnect these devices to allow data to flow from source devices to destination devices via IEC 61850 and other protocols are a communications system network. Consider the primary system depicted in Fig. 1 and the digital communications necessary for a DSS.

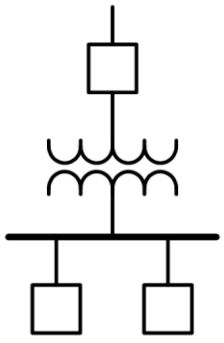


Fig. 1. Substation With Two Feeders

A. Communications System Network

One of the critical early steps to the SAS design is to outline both the logical and physical communications networks by using the SAS data flow requirements to choose protocols and methods to accomplish the data flow based on the system performance criteria. The data flow requirements are established during the initial data flow design steps and documented in data flow diagrams. Other nonperformance, non-data-flow–related criteria are often used as well, including the desire to try new media and protocols as an experiment or because features of chosen devices restrict protocol choices.

Over the years, terminology has evolved to describe various combinations of protocols and methods for different communications purposes to, from, and among intelligent devices within an SAS. Though data buses are rarely, if ever, used any longer in DSSs, the term bus has remained to describe a network that can be virtual, physical, or both. The engineering bus (EB) includes client/server protocols and methods for engineering access to configure and interact with the device. The station bus (SB) includes operational client/server protocols and methods for operator command and control via local and remote supervisory control and data acquisition (SCADA) and operator workstation systems. The process bus (PB) includes machine-to-machine protocols and methods to exchange process signals. In the electrical substation, the process is to monitor, protect, and control the primary equipment in the electric power system. Signals include raw analog current and voltage samples, other digitized analogs such as temperatures and positions, and digitized statuses, alarms, and controls. Electrical system PB protocols include standard Ethernet-based protocols (IEC 61850 GOOSE and SV as well as IEEE and IEC PTP) and point-to-point protocols (Mirrored Bits communications, resistance temperature detector communications, and IEC 61158 EtherCAT®).

Although a device may be described as having only a PB interface, such as a merging unit (MU), it is most likely a merged bus that includes EB and PB capabilities so that the device can be configured and diagnosed. Many MUs often include SB capabilities as well. It is up to the data flow designer to choose which capabilities will be combined or remain separate on physical network segments and which will have redundant physical network ports versus singular. For example, for operational and security reasons, it may be preferable to have one physical port support an EB connection isolated from other communications. In addition, it may be preferred to have two physically redundant SB ports as well as two physically redundant PB ports. This design will have three isolated networks using five physical ports on the device. Another example may have all EB, SB, and PB communications on two physically redundant device ports. SASs that use IEC 61850 methods include a few protocols described within the IEC 61850 standard and numerous other protocols to retrieve reports and records as well as time-synchronize, configure, operate, and maintain the communications-assisted applications. By design, the IEC 61850 standard enables, and enforces, the open inclusion of other public and private protocols and does not prescribe methods for field input/output (I/O) interconnections.

Consider a simple SAS design using IEC 61850 GOOSE, SV, and MMS as operational protocols on a communications network that combines SB and EB conversations. This simple SAS example also has a second, separate communications network with PB and EB conversations. Both networks support engineering access conversations, as EB functions for configuration and maintenance for most PB devices because they combine PB and EB protocols, a condition referred to as merged mode, on their Ethernet interfaces. When using fully featured PB devices that support independent PB and SB interfaces, the EB protocols can be restricted to the SB and simplify the PB design.

Most PB device manufacturers to date only support merged mode and do not use IEC 61850 or other standardized protocols or open-source methods to manage and configure their devices. When these devices are selected, in addition to standard methods and protocols, the communications networks must be designed to support proprietary methods and private protocols as required by the device manufacturer–specific configuration software. These private manufacturer-specific protocols create islands of secrecy within a network that cannot be understood by or maintained by the end user and create security and operational vulnerabilities. The many other SB, PB, and EB protocols, including PTP, Telnet, and File Transfer Protocol (FTP), are not secret, but neither are they defined within the IEC 61850 Substation Configuration Language configuration files. Their configuration needs must be defined separately. This also applies to other non-IEC 61850 protocols in the network, such as Distributed Network Protocol (DNP3) for SCADA.

Methods using the IEEE 802.1 spanning tree algorithm (STA) or software-defined networking (SDN) create a reliable and precise network with sufficiently robust automatic data flow fault detection and reconfiguration. Instead of designing robust, substation-grade, IEEE method-based Ethernet networks, many manufacturers began to rely on IEC industrial duplication methods. When designers choose not to use IEEE or SDN methods for data flow fault detection and reconfiguration, they often rely only on IEC duplication methods, which depend on manual fault detection and repair. This may require the communications network to support High-Availability Seamless Redundancy (HSR) protocol or PRP [1]. Best-known methods include using both fault restoration via STA or SDN and message duplication via PRP.

Time synchronization may be done with another non-IEC 61850 protocol, such as IEEE 1588 PTP. The SAS may be added to an existing utility infrastructure and may also need to support a non-IEC 61850 SCADA protocol, such as DNP3. So, while IEC 61850 protocols perform some of the operations, they are not sufficient for configuration, commissioning, diagnostics, and maintenance. Therefore, the communications network needs to support numerous other protocols to satisfy the full requirements.

Prior to creating the communications network design, it will be necessary to identify the data flow needs to support the SAS

objectives. Much of the data flow within and among the PB, SB, and EB networks within a substation is mission-critical for safe and reliable performance of protection, control, automation, and metering applications. Individual flows will need to be identified for each data object (such as a breaker position or phase current value) or data set (group of data objects) and will include their origins and destinations as well as important communications logistics (real-time publications or near real-time poll and response). It is important to begin data flow design by mapping out the data flow needs followed by documenting them, optimizing them, and documenting them again. It is important to understand the source and destination of each data object or data set, the performance characteristics of how data should be moved, and finally the relative criticality of data to important applications. Then, as the data flows are designed, it is important to understand flow interdependencies and potential interference among the multiple data flows.

The data flow design for digital communications includes multiple data flow diagrams, application architecture drawings, physical architecture drawings, and communications protocol diagrams to satisfy the behavior defined by the configuration software for the devices in the system. The configuration files resulting from this software-defined protection, automation, and communications activity are used to automatically create the required data flow rules for SDN to explicitly deliver messages within the DSS communications network. SDN designers consider data sources, destinations, data sets, timing requirements, and performance requirements. Alternately, designers manually use a handful of settings to influence an STA, using Rapid Spanning Tree Protocol, to allow and disallow messages on various network segments without control of the data flow behavior or performance.

Understanding the purpose and mechanisms for data flow is an important and necessary step in creating a DSS. However, the process to create the data flow design is out of the scope of this paper, which is focused on reliability analysis of the chosen design.

B. DSS Data Flow

The utility expects the DSS to positively influence human performance improvement by reducing tedious manual activities and minimizing opportunities for human error. As stated in the explanation of software-defined DSSs in Section II.A, configuration files created during the software definition of protection, automation, and control serve as the foundation for defining the data flows required in the communications system. After creating the configuration files, the utility then evaluated various communications technologies and architectures that can support these data flows and meet established criteria for cost, performance, and long-term maintainability. Of particular interest are the choices for Ethernet communications from the field into the control building to support protection signal communications via IEC 61850 GOOSE, SV, and MMS; IEEE/IEC 61588 PTP; IEC 62439 PRP; and open-source manufacturer configuration protocols. It is well understood that the ACSI defined in IEC 61850-7-2 allows data to be mapped onto non-IEC 61850 protocols in keeping with the conceptual model of the standard. The utility also evaluated the risk associated with nonstandardized protocols and considered accommodations necessary for manufacturers that use undocumented, private, and secretive engineering access and configuration protocols.

1) Reliability Expectations for Digital Protection Systems

The DSS still requires the same hardwired connections to the primary equipment, so the reliability and risk of failure of this component remains. The lengths of copper conductors from the field to the control house are shortened when terminated to MUs and other devices in the field that perform digitalization (replacing traditional processes with digital communications and logic) and publish messages. Numerous additional devices are then installed in the control house to transport messages, time-synchronize devices, and subscribe to digital messages containing digitized signals in order to perform protection and automation. Although physics dictates that with additional systems and devices, risk of failure will grow, with the use of risk-informed decision-making (RIDM), it is expected that the DSS design will minimize additional risk as well as bring numerous benefits.

2) Digitalization Objectives

The utility's Transmission Engineering department was requested to investigate the possibility of using IEC 61850 in a standard installation in their transmission and distribution substations. The objective was to leverage the newer technology to reduce maintenance costs associated with routine testing. Another goal was to see if there would be any meaningful initial cost savings in comparison to the traditional designs. Safety was another added benefit, as IEC 61850 reduces the number of points where the secondary currents and voltages are as well as eliminates them completely from the electrical equipment enclosure.

New technologies bring a significant amount of uncertainty. As such, some engineering teams are hesitant to adopt new technology until it has been fully proven out, sometimes for many years. Like other evolving digital technologies, DSS is subject to non-evidence-based proclamations and proposals, or false evidence appearing real, which may result in engineers saying, "I simply do not know what may fail" instead of doing work to predict failures. The utility did not want to develop false confidence in new and unproven methods or underestimate the risk of adding DSS technology. Instead of assuming failures may not occur, the utility adopted the approach that even when failures happen, the DSS design would be resilient and satisfy the primary system return-to-service requirements. To accomplish this, the utility embarked on research summarized in this paper to use evidence of device and component quality from manufacturers in order to precisely perform reliability analysis for the new substation design and associated risk mitigation efforts.

In trying to reduce some of the team's hesitancy with the new technology, it was suggested that there could be an analytical approach to evaluating the design to show that there

is no compromise to the reliability of the protection and control system.

C. Defining Reliability for Protection and Control Systems

When evaluating digitization (performing analog-to-digital conversion of electrical signals) and digitalization, reliability of the system is paramount. ASTM E1699-14 is a standard practice used by designers to perform value engineering [2]. In DSS design, the goal of value engineering is to design methods that replace traditional hardwired methods with digitalization that increases functionality without lowering quality, reliability, or performance. By adding additional methods and devices, the utility can likely only lower costs through repetitive reuse of the new design to offset the cost of nonrecurring engineering.

This paper focuses on reliability analysis, which, based on IEC 61850-3, *Communication Networks and Systems for Power Utility Automation – Part 3: General Requirements*, includes dependability, physical security and cybersecurity, availability, maintainability, and restoration capability [3].

1) Mission Time and Engineering Assumptions

Many utilities consider mission-critical components to be continuously operational. Engineering analysis assumes for both the primary and secondary systems that failed components are repairable and that systems can be quickly returned to service. For designs that require N-1 reliability, return-to-service times for failed components are essentially immediate. For example, when installing an N-1 system, it is expected to function correctly from the instant it is energized. This constant operation is expected for the life of the system, and therefore, return to service is expected to be similarly rapid. Transmission utilities in the U.S. use instantaneous (up to 2 seconds) and momentary (lasting less than 1 minute) outage metrics for return to service of energy delivery and often use 72 hours as the return-to-service metric for replacement of a failed primary system device.

RIDM is used to translate uncertainty to measurable, where possible, or predictable risk [4].

2) Building the Digital System Model

The utility's team spent a great deal of time talking with other utilities and manufacturers who have adopted IEC 61850 to learn what others have already determined through their trial and error. As part of this, it was decided early on that the system design would be kept as close to the utility's current standard as possible. This meant keeping a single function in a single relay, i.e., a dedicated breaker failure relay that does the reclosing for its breaker. The initial investigation was going to look at only a single line position in a breaker-and-a-half substation with a single breaker failure relay. This allowed for the testing setup to remain small scale and hopefully simpler. The intent was that the team would be comfortable with the small-scale laboratory configuration before it would expand to include other types of equipment zones of protection. As such, in this paper, the authors assume that the bus, transformer, capacitor, reactor, etc., are all traditionally hardwired. Another major decision was to have the network topology use PRP. This would be for both the SB (SCADA, engineering access, PTP, etc.) and the PB (protection-level GOOSE messages and SV).

III. DSS Failure Modes and Consequences

Traditional hardwiring methods require very few decisions to be made; a utility essentially chooses between termination methods with increasing dependability from twisted bare wire to forked lugs to circular spade lugs. Failure modes include wiring mistakes, contact failures, and trip circuit failures.

DSS failure modes include these failures plus communications failures, firmware and software failures, configuration errors, timing failures, and Ethernet port and switch failures. Hardwiring failures may remain undetected until field testing. The complex DSS technologies include hidden failures in the form of undetected communications degradation, silent undetected and unannounced redundancy or duplication loss, path failures, and incorrect failover behavior. Regardless of the DSS fault, the consequences of DSS failures include failure to trip, false trip, delayed trip, and loss of situational awareness.

The goal of DSS reliability analysis is to predict the likelihood that each component is now, or will be, unavailable to protect the primary system. The goal of risk-informed design is to make sure that DSS failures are detected and corrected fast enough to allow the utility to avoid a power system fault or mitigate an outage within the previously mentioned 72 hours. Though several references for this paper use the older estimate of 48 hours as the industry average for mean time to repair (MTTR), advancements in products and maintenance have shortened this time frame to 24 hours for DSS devices, which allows engineers to better understand DSS return to service to prevent power delivery from being interrupted for more than 72 hours.

A. Engineering Responsibility

Design engineers are responsible for using math and science to predict failures, identify and implement failure mitigation strategies, and continually reduce the risk of failures. The commonsense concept that continuously finding and addressing small failures reduces the risk of large failures is supported by research [5]. By studying electric power grid resilience to weather events, researchers found that by identifying small, precursor failure patterns in distribution grids, they could address minor anomalies before they cascaded into major outages. By treating resilience as a continuous process, not a one-time hardening effort, they reduced large-scale failures by intervening early when small deviations appeared.

Though it is hard to prove that appropriate engineering design and DSS robustness prevent unplanned outages that do not occur, it is nonetheless the responsibility of design engineers to design for reliability. A difference when transitioning to DSS is that there are many realistic solutions fit for the purpose of mission-critical communications, as well as information technology (IT) methods fit for use but not yet demonstrated to be fit for purpose. Because of dozens or hundreds of options, care must be taken to avoid decision

fatigue, normalization of deviance where unsafe or improper practice becomes accepted as normal because it does not immediately cause visible failure, and self-serving bias and attribution error where people blame the system for failure rather than their lack of rigorous engineering and design.

B. Reliability Modeling Methodology

Event tree analysis (ETA) is a method of understanding potential events and predicting the consequences if no mitigation action is taken to protect the system from succumbing to the event. This type of analysis uses data about the potential consequences and the available methods to protect against the event to predict, "Given that this event occurred, what happens next?" One type of ETA, attack tree analysis, provides an event tree method that was used to quantify the risk of a successful cyber attack to a DSS by analyzing identified cyber vulnerabilities [6]. Fault tree analysis (FTA) is a popular tool to assess DSS robustness with a top-down modeling approach that is useful to assess failure to trip and false trip based on manufacturer quality data, historical utility data, and industry reliability data, which are used by a DSS expert to predict failure metrics. Using field-measured metrics such as mean time between failures (MTBF) and MTTR, simple statistical mathematics enables insight into potential DSS components, which may mean the system is unavailable to perform its intended function [7]. Using FTA, the past performance of DSS components allows for a mathematical calculation of the probability that the DSS will fail on demand. FTA of communications failures within the PB provides insight into the new potential failures separate from the traditional hardwired approach. IEC 61508-1, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 1: General Requirements*, explains the different failure modes as dangerous detected (DD) failures, which are detected and immediately announced to drive repair, and dangerous undetected (DU) failures, which remain hidden until they are potentially found during periodic field testing [8]. The utility uses a field test schedule of 5 years, so DU failures represent a probability of failure on demand that may occur any time between 1 second after to 1 second before a field test for an average of 2.5 years.

C. Potential Cost Savings

When the impact of the control house size is excluded, an architecture that deploys MUs or relays in the switchyard can be approximately 50 percent less costly to install than a traditional hardwired design. The cost reduction results from several factors including the following, as mentioned in [8]:

- Simplified system design, requiring fewer engineering and drafting resources.
- Decreased use of installation materials such as cables, trenches, conduits, and duct systems.
- Lower labor requirements for civil construction activities, including trenching and duct placement.
- Reduced installation, wiring, and testing time during project execution and commissioning.

IV. Redundancy, Restoration, and Operational Reality

As with the primary system, the DSS was designed with an N-1 philosophy. The expectation is that any failure is not a single point of failure and that failures creating an N-0 scenario are promptly corrected to return the DSS to N-1 status. SDN technology was chosen for the Ethernet network due to its pre-engineered data flow capabilities with active path redundancy management, fast fault detection, and near instantaneous data flow path reconfiguration. PRP was chosen to provide duplication. This represented the crux of the reliability analysis due to inherently hidden duplication degradation caused by the failure of the link redundancy entity to include monitoring. Availability analysis was scoped to compare a standard PRP system with a PRP system augmented with additional nonstandard safeguards [7].

A. RIDM and Risk Registers

Recognized risk management standards, including ISO 31000:2018 *Risk management — Guidelines*, document the use of risk registers as a tool to support RIDM [4] [9]. One use of a risk register is to identify and aggregate all the potential threats that could cause failure of a system to assess, prioritize, monitor, and manage risks.

The intention of the DSS is to reduce the complexity of adding functionality, not to increase it. The utility's intention is to create a PB design that makes the substation simpler and more manageable via availability and self-announced status and alarms that provide evidence of the health and behavior of both the primary and secondary systems.

IEEE and other organizations are exploring legitimate and helpful ways to use artificial intelligence (AI) as a tool. One such use is to create risk registers to help engineers identify and understand threats to their designs. AI has access to publicly available documents that describe the work that has been done to date and, in this case, it has prepared a list based on that work that is a starting point to do new work. From this list, a strategy for how to build upon it was generated. Table I illustrates a risk register created by AI to list points of failure that are different between a single relay hardwired to the primary equipment versus a subsystem consisting of a single intelligent MU (IMU), network, fiber, and relay. This generic risk register illustrates components including failure mode, cause, effect, likelihood, consequence, risk ranking, and mitigation scored qualitatively as low, medium, and high.

TABLE I
AI-GENERATED RISK REGISTER FOR THE UTILITY'S DSS PB

ID	Category	Architecture	Failure Mode	Cause	Effect on Protection Function	Likelihood (1-5)	Consequence (1-5)	Risk Score (L x C)	Risk Rank	Mitigation / Controls	Residual L	Residual C	Residual Score
HW-01	Signal Path - Copper (Baseline)	Hardwired (Baseline)	Long-run CT/VT copper conductor open circuit or high resistance connection	Vibration, corrosion, thermal cycling, rodent damage, mechanical damage over long cable run (hundreds to thousands of ft) between yard and control building	Open CT secondary produces dangerous high voltage arc/fire risk and loss of current signal to relay, potential misoperation or failure to trip	3	5	15	High	Periodic secondary injection testing, CT shorting block procedures, visual cable inspection programs			
MU-01	Signal Path - Digitized	Process Bus (New)	Merging unit failure (digitization/sampling hardware fault)	Internal MU electronics failure, power supply fault, ADC/sampling clock fault, firmware crash	Complete loss of digitized current/voltage signal for all subscribed relays/functions fed by that MU - single point of failure for potentially multiple protection functions	3	4	12	Medium	Redundant/dual MUs per bay, MU self-supervision alarms, MU health monitoring via SCADA/NCIT, spare MU stocking strategy			
HW-02	Signal Path - Copper (Baseline)	Process Bus (New)	Short copper run (primary equipment to MU) open circuit or degraded connection	Same mechanical/environmental stressors as HW-01, but exposure length is dramatically reduced (typically <50-100 ft vs. thousands)	Loss of primary signal into MU only; localized fault, easier to trace and isolate	2	4	8	Medium	Reduced exposure length is itself the mitigation; still requires standard CT/VT wiring practices and periodic testing			
MU-02	Signal Path - Digitized	Process Bus (New)	Sampled Values (SV) stream data corruption or packet loss	Network congestion, switch buffer overflow, EMI-induced bit errors on fiber transceivers, faulty SFP/optical transceiver	Relay receives corrupted or incomplete waveform data, may trigger SV supervision alarm and block protection function, or in worst case use corrupted data	2	4	8	Medium	SV stream sequence number checking, relay-side SV quality/validity flags, redundant network paths (PRP/HSR per IEC 62439-3), network monitoring			
MU-03	Signal Path - Digitized	Process Bus (New)	Analog-to-digital conversion error / scaling error in MU configuration	Incorrect CT/VT ratio programmed into MU, incorrect SCD engineering, commissioning error	Systematic misrepresentation of primary current/voltage to all subscribing relays - silent error not caught by normal supervision, can cause misoperation on all downstream functions	2	5	10	Medium	Rigorous SCD/ICD configuration management and peer review, commissioning primary injection testing at the relay (not just MU), configuration version control			
NET-01	Network - Fiber Plant	Process Bus (New)	Fiber cable cut or connector damage (long run, yard to control building)	Excavation/dig-in damage, rodent/animal damage, connector degradation, physical damage during other maintenance	Loss of all Sampled Values and GOOSE traffic for every device on that fiber path - potential total loss of protection for affected bay(s)/relays	2	5	10	Medium	Redundant/diverse fiber routing, dual-homed switches, PRP/HSR redundancy protocols, fiber path documentation and dig-permit process, regular fiber loss testing (OTDR)			
NET-02	Network - Ethernet Switches	Process Bus (New)	Process bus Ethernet switch failure or misconfiguration	Switch hardware failure, power supply loss, firmware bug, VLAN/multicast (IGMP) misconfiguration, switch overload from broadcast storm	Loss of SV/GOOSE delivery to some or all connected relays; potential loss of an entire protection zone depending on switch topology	3	5	15	High	Redundant switches with RSTP/PRP/HSR, switch health/port monitoring via SNMP integrated to SCADA, spare switch inventory, strict change management on switch config			
NET-03	Network - Ethernet Switches	Process Bus (New)	Network congestion / bandwidth saturation on shared process bus	Excessive multicast SV/GOOSE traffic, improperly segmented VLANs, too many MUs sharing one switch/network segment, non-protection traffic sharing the network	Increased latency or dropped SV samples/GOOSE messages, exceeding IEC 61850 performance class timing requirements (e.g., Type 1A trip messages)	2	4	8	Medium	Dedicated process bus network segregated from station bus/corporate traffic, proper VLAN and multicast filtering design, network bandwidth engineering per IEC 61850-90-4 guidance			
NET-04	Network - GOOSE Messaging	Process Bus (New)	GOOSE message not received or delayed beyond protection time budget	Network congestion, switch queuing delay, misconfigured GOOSE retransmission timers, subscriber processing delay	Interlocking, trip, or blocking signals (e.g., breaker failure initiate, bus differential trip) fail to arrive in time - loss of coordination/selectivity or failure to trip	2	5	10	Medium	GOOSE supervision (quality/heartbeat monitoring at subscriber), engineered worst-case latency analysis, dedicated deterministic network design, redundant GOOSE paths			
NET-05	Network - Common Mode	Process Bus (New)	Single Ethernet switch or fiber path serving as an unintended common-mode dependency across redundant protection systems (e.g., Main 1 & Main 2)	Inadequate network architecture/segregation design; both protection systems inadvertently routed through shared switch or fiber trunk	Defeats intended primary/backup protection redundancy - single failure disables both protection systems simultaneously	2	5	10	Medium	Physically and logically independent networks for redundant protection systems (fully separate Main 1 / Main 2 networks per good practice), independent network audits during design review			
TS-01	Time Sync - IRIG-B (Baseline)	Hardwired (Baseline)	Loss of IRIG-B time reference to a relay	GPS antenna/receiver fault, IRIG-B wiring fault, clock failure	Loss of accurate event/fault timestamping; protection function itself typically continues to operate correctly since legacy relays are not sample-synchronized	2	2	4	Low	Redundant time sources, relay internal free-run clock holdover, alarm on loss of time sync			
TS-02	Time Sync - PTP	Process Bus (New)	Loss of PTP grandmaster clock or GPS antenna signal to grandmaster	GPS antenna failure, GPS signal jamming/spoofing, grandmaster clock hardware failure, satellite constellation issue	If merging units lose absolute time reference, sample synchronization across MUs may degrade, causing sampled-value misalignment between phases/bays feeding differential or synchro-check protection - can cause misoperation or blocking of protection	3	5	15	High	Redundant/dual grandmaster clocks, holdover-capable oscillators (rubidium/OCXO) in clocks and MUs, GPS antenna diversity/anti-jam antennas, PTP monitoring and alarming			
TS-03	Time Sync - PTP	Process Bus (New)	PTP path delay asymmetry or network-induced timing error	Non-PTP-aware (non-transparent) intermediate switches, asymmetric fiber path lengths, incorrect PTP profile configuration (not using IEC 61850-9-3/C37.238 Power Profile)	Subtle sample misalignment between MUs not caught by simple loss-of-sync alarm - degrades accuracy of current differential and phase angle measurements, potential nuisance trips or failure to detect real faults	3	4	12	Medium	Use only PTP-aware (boundary/transparent clock) switches throughout process bus, adherence to Power Profile standard, commissioning-time path delay verification, periodic PTP performance audits			
TS-04	Time Sync - PTP	Process Bus (New)	GPS spoofing or PTP cyberattack (time source manipulation)	Malicious actor spoofs GPS signal or injects false PTP messages onto network	Deliberate manipulation of sample timing across substation - can induce incorrect differential protection operation (trip or block) as an attack vector; this failure mode does not exist in legacy hardwired scheme	2	5	10	Medium	Anti-spoofing GPS receivers, PTP authentication/security extensions where available, network segmentation, IDS on process bus network, NERC CIP-013 supply chain and CIP-005/007 controls			
CYB-01	Cybersecurity	Process Bus (New)	Unauthorized access to process bus network (MU, switch, or relay compromise)	Weak network segmentation, unpatched switch/MU firmware, insufficient access control, insider threat, supply chain compromise	Attacker could inject false GOOSE trip/block commands or manipulate sampled values - directly causes misoperation; this attack surface (IP-networked protection signals) does not exist in a hardwired copper scheme	2	5	10	Medium	NERC CIP compliance program extended to process bus assets, network segmentation/firewalling, GOOSE/SV message authentication where supported, regular vulnerability scanning and patch management, asset inventory of MUs/switches/clocks as BES Cyber Assets			
CYB-02	Cybersecurity	Process Bus (New)	Malware or unauthorized firmware on merging unit or switch	Supply chain compromise, unsecured engineering access (USB/serial port), lack of firmware integrity verification	Compromised device could report false data or silently fail; harder to detect than a hardwired open circuit which trips supervision immediately	1	5	5	Low	Firmware signing/verification, secure engineering access controls, configuration change detection/alerting, periodic firmware integrity audits			
ENG-01	Engineering / Interoperability	Process Bus (New)	Multi-vendor MU-to-relay interoperability failure	Differing vendor interpretations of IEC 61850-9-2/9-2LE, incompatible SV publisher/subscriber implementation, SCD/ICD mismatch after a device replacement or firmware update	Relay fails to properly subscribe to or interpret SV stream after a component change - loss of protection function discovered potentially only during testing or an actual event	3	4	12	Medium	Standardized engineering process (SCL/SCD management), interoperability testing (UCA IOP or equivalent) before deployment, factory acceptance testing (FAT) for every MU-relay pairing, strict MOC (management of change) process for firmware/config updates			
ENG-02	Engineering / Interoperability	Process Bus (New)	Configuration/commissioning error not caught by traditional wiring-based test procedures	Field commissioning teams trained on traditional point-to-point wiring verification, unfamiliar with SCD file review and network-based testing methods	Latent misconfiguration (wrong VLAN, wrong multicast address, wrong dataset mapping) not discovered until a real fault - protection fails to operate as expected	3	4	12	Medium	Specialized process bus commissioning procedures and checklists, staff training/certification on IEC 61850 engineering tools, end-to-end primary injection testing through the full digital chain, independent design review			
HF-01	Human Factors / O&M	Process Bus (New)	Loss of institutional knowledge / skills gap for troubleshooting digital process bus	Existing protection technicians experienced with copper/analog troubleshooting (meters, multimeters) but not with network analyzers, SCD tools, or PTP diagnostics	Extended outage restoration time (MTTR) during a fault, since diagnosis requires different skill set and tools than traditional wiring faults	4	3	12	Medium	Dedicated training program, standardized troubleshooting procedures/runbooks, network diagnostic tooling (SV/GOOSE analyzers), vendor support agreements, cross-training between protection and network/IT-OT staff			
HF-02	Human Factors / O&M	Process Bus (New)	Increased number of discrete components increases aggregate failure opportunities	Architecture adds MU, switches, clocks, fiber patch panels, and SFPs as new components in the signal chain that did not exist in hardwired design (each with its own failure rate)	Even though each new component may be individually reliable, the increased component count can increase the overall probability of some failure occurring in the signal chain, though consequence per event is often more localized/graceful than a hardwired failure	3	3	9	Medium	System-level reliability/availability modeling (not just component-level) during design, N+1 redundancy at every new layer (MU, switch, clock), preventive maintenance program covering all new asset classes			
HF-03	Human Factors / O&M	Process Bus (New)	Loss of intuitive visual/physical fault indication	Copper wiring faults are often traceable via voltage/continuity testing at accessible terminal blocks; digital signal path faults are not visually or electrically apparent without specialized tools	Delayed fault detection and diagnosis, particularly for subtle issues like SV misalignment or partial packet loss that do not immediately trip an obvious alarm	3	3	9	Medium	Comprehensive self-supervision and alarming architecture (MU health, switch port status, PTP status, SV quality) reported to SCADA/HMI, centralized network monitoring dashboard			
PHY-01	Physical / Environmental	Process Bus (New)	Merging unit environmental exposure (yard-mounted electronics vs. control-building-mounted relay)	MU is mounted in the yard (often in a marshalling cabinet) and thus subject to more severe temperature extremes, humidity, and vibration than a relay in a climate-controlled control building	Reduced MTBF for yard-mounted digital electronics compared to control-building-mounted equivalent; the baseline hardwired design keeps all electronics in the benign control building environment	3	3	9	Medium	Environmentally hardened/rated MU enclosures (extended temp range per IEC 61850-3 / IEEE 1613), climate-controlled marshalling cabinets, appropriate ingress protection rating			
PHY-02	Physical / Environmental	Process Bus (New)	Optical transceiver (SFP) degradation over time	Laser diode aging, thermal cycling in yard environment, dust/contamination on optical connectors	Gradual signal degradation leading to intermittent SV/GOOSE errors before outright failure - can be difficult to diagnose as root cause	2	3	6	Low	Optical power budget monitoring/alarming, scheduled SFP inspection and replacement program, connector cleaning procedures, spare SFP inventory			

The risk register in Table I is a comprehensive list of concerns generated by the AI agent's knowledge of the subject based on technical papers and other publicly available documents. The utility then created a specific evaluation of a subset of the register based on measured MTBF of devices being considered for the DSS PB subsystem comprising an IMU, an Ethernet network, fiber cables and interfaces, a clock, and a relay. The goal was to minimize the added risk by choosing the most available physical subsystem design.

B. Unavailability Modeling Methodology

Comparison of the MTBF of two relays provides a deterministic indication of which is more likely to fail but does not provide definitive information about the probability of if or when they may fail. This present or future failure may initially be considered random but is actually probabilistic [4]. The quantity of failures for a specific population of relays, and other devices, is predictable and known as the failure rate. The duration of time that the product functions correctly, from the

time it starts or resumes operations until it fails in service, is the mean time to failure (MTTF), as illustrated in Fig. 2.

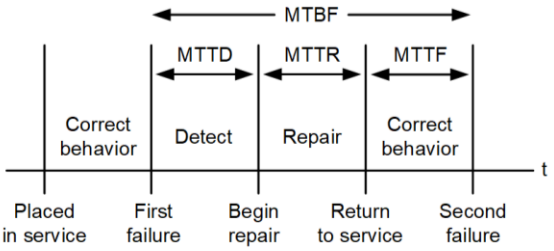


Fig. 2. Failure and Repair Cycle

The mean time to diagnose (MTTD) is the duration of time between the instant that a failure is detected and the instant in time that the failure previously occurred, as shown in Table II. For the utility's relays and other devices that have self-testing, fault monitoring, and self-announcing of failures, the MTTD is deterministic. However, when devices do not automatically detect and announce failures, the time between failure and detection cannot be known and the MTTD is probabilistic. Failure of a communications-assisted protection scheme may result from the failure of an unmonitored device or component, such as a hardwired termination or standardized PRP local-area network (LAN), which is detected when it fails to mitigate a problem when called upon, and the result can be a missed or unintended operation, which may lead to a power system outage. Modifications to NERC TPL-001-5.1 were recently suggested to handle unmonitored single points of failure. At the utility, failures of unmonitored in-service DSS components are detected when they are removed from service and tested periodically. The utility uses a test period of 5 years, and failed components are repaired and the unit that was detected during periodic testing is returned to service. Each of these failures reveals that "the power system was vulnerable to a hidden failure for an undetermined period of time or that the test process induced the failure" [4]. As mentioned previously, failure of unmonitored components can occur moments after or moments before field testing or any time between. The utility uses the traditional value of the mean, or half, of their 5-year periodic test cycle, or 2.5-year MTTD, for unmonitored components.

TABLE II
UNAVAILABILITY CALCULATED FOR VARIOUS DETECTION TIMES AND 24-HR MTTR

		Unavailability: $q \cdot 10^{-6}$ (Where Lower is Better, More Available)			
Device	**MTBF Years**	**Automatic MTTD With 24-hr MTTR**	**1-Year MTTD With 8,784-Hr MTTR**	**2.5-Year MTTD With 21,924-Hr MTTR**	**5-Year MTTD With 43,824-Hr MTTR**
Hardwire Termination	5,000	NA	100	250	500
Fiber Termination	5,000	0.5	100	250	500
Relay A	1,250	2.2	402	1,002	2002
Relay A Ethernet Port (5)	25,000	0.1	20	50	100
Relay B	228	12	2,203	5,495	10,977
Relay B Ethernet Port (5)	4,560	0.6	110	225	549
OT SDN Switch	1,900	1.5	265	660	1,318
OT SDN Switch Ethernet Port (28)	212,800	0.015	2.4	5.9	11.8
Ethernet Switch	242	11.3	2,078	5,177	10,342
Ethernet Switch Port (28)	27,104	0.1	19	46	93
Clock A	1,200	2.3	419	1,044	2,086
Clock A Ethernet Port (5)	24,000	0.1	21	52	105
Clock B	228	12	2,203	5,495	10,977
Clock B Ethernet Port (5)	4,560	0.6	110	225	549
IMU A	1,250	2.2	402	1,002	2,002
IMU A Ethernet Port (5)	25,000	0.1	20	50	100
IMU B	228	12	2,203	5,495	10,977
IMU B Ethernet Port (5)	4,560	0.6	110	225	549

The unitless value representing unavailability, q, is the result of the formula in (1), which can now be evaluated mathematically for the utility's design choices [10].

$$Unavailability\ q = \frac{MTTR}{MTBF} \quad (1)$$

When evaluating the reliability of a protection, automation, or control system, it is essential to distinguish between device failure characteristics and the probability that equipment will be unavailable for service at a given point in time. Therefore, there must be a clear differentiation between unavailability and MTBF.

> Availability and unavailability are usually expressed as probabilities. 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. [11]

A 5,000-year MTBF per wiring point is predicted by [12], and [13] predicts a 4,400-year MTBF for terminal block connections due to degradation associated with heat, corrosion, and loss of the clamping force in screw and lug terminations. The utility used a 5,000-year MTBF for this paper and the aforementioned 2.5-year MTTD of DU field faults, making the unavailability of a copper contact termination $250 \cdot 10^{-6}$. The industry MTBF for properly installed and sealed fiber terminations is considered nearly infinite because glass fiber does not degrade and failures are typically associated with external events and not component wear. However, until the utility has more experience, the large noninfinite value of 5,000 years is used so as to not unduly influence the analysis [11]. However, fiber connection failures are immediately evident due to the detection of a loss of signal, which results in a value for unavailability of $0.6 \cdot 10^{-6}$, based on the 24-hour time to repair or replace. Manufacturers of Relay A, the operational technology (OT) SDN switch, the clock, and the Ethernet switch provide MTBF values corresponding to their usage by the utility. IMU A has the same hardware and firmware design as the relay and is assigned the same MTBF.

In practice, port failures are often less common than power-supply failures, so the MTBF of individual ports can be substantially higher than the device MTBF. Common industry practice is to allocate a fraction of the DSS device total failure rate to Ethernet ports using a first-order estimate, a quick, simplified, order-of-magnitude approximation that assumes 25 percent of failures are Ethernet port–related so the port-related MTBF will be four times the device MTBF. For a device with multiple ports, the port-related MTBF represents all of the ports and common industry practice is to allocate a proportional amount of port-related MTBF to each individual port; the relay, Ethernet, switch, and clock Ethernet port MTBF = device MTBF • 4 • port count.

For manufacturers that do not calculate MTBF, a common industry MTBF prediction based on component models is 57 years. Approximating the Relay B MTBF by increasing the industry-predicted value by a factor of four, 228 years, is considered a technically defensible approach by explicitly acknowledging that field-return MTBF data are not publicly available. Though IMU B and Clock B are potentially simpler and more reliable than Relay B, they have a much smaller installed base and their MTBF is approximated to be the same as Relay B.

C. Return-to-Service Time

> It is very important to understand that unavailability is not an indication of the risk that a product will fail over time—that is MTBF. Unavailability is a unitless value that gives the relative likelihood that a device is failed in service at some point during the time being considered. [4]

Uncertainty about the possibility of a DSS device being unavailable, now or in the future, to prevent or mitigate a primary system fault is replaced by predictability of the same possibility. As expressed above, unavailability is proportional to the time required to detect device failure. Several references for this paper used 48 hours as the industry average to repair or replace (MTTR) a DSS device. Advancements in products and maintenance have shortened the industry average to 24 hours. Using 24 hours for MTTR, unavailability is calculated for DD failures for which repair begins immediately (MTTD = 0) based on automatic detection and self-announcement of failures. The robust designs of the electric power system in the early and middle parts of the previous century meant that outages were uncommon due to large budgets available for redundancy and networking. The success of the system to prevent primary system faults from causing outages lulled the general public into thinking that faults were far less frequent than they actually were. In the following decades, untold numbers of electromechanical relays without detection or alarming were unknowingly and simultaneously failed in service and only a few were discovered when they failed to operate during a primary system fault. These cases highlight how undetected protection system failures can create a false sense of security, causing operators and engineers to overestimate the availability of protective functions.

Not only does better monitoring enable prediction of true failure rates, but failures are also more likely to be present, now and in the future, and repairs begin long after DU failures with lack of automatic detection occur. These realities, plus copper wire contact DU failures, are often found via periodic field testing, and the delayed corrective action increases unavailability, as shown in Table II.

D. Return-to-Service Considerations

Unless a failure is detected during a misoperation, traditional hardwired systems experience latent failures that are only discovered during a periodic test. In one maintenance cycle, resources for repair and replacement must address the accumulated failures that have occurred during the previous period. Since numerous concurrent issues may exist, this creates a concentrated demand for maintenance personnel,

spare parts, testing equipment, and outage coordination. In contrast, systems like DSS with automatic failure detection and real-time alarming identify each failure as it occurs so that repair or replacement can be started immediately. Therefore, in addition to the infrequent bulk work to repair failures found in periodic tests, maintenance staff must now be constantly available to repair DD failures as they occur distributed over time rather than grouped together. Also, even though the new DSS repairs may also require outage coordination, they require different maintenance staff skills, spare parts, and testing equipment. A 24-hour MTTR in unavailability analysis assumes that repair will begin immediately after the DSS DD failure alarm occurs.

The focus of this paper is the impact on reliability of the continuous-duty DSS, which is analyzed by calculating the availability of various system architectures to react on demand and requires repair of any DSS component immediately after detected failure.

Human performance risks are real considerations when migrating to new technology. Creativity, critical thinking, and collaboration are durable skills that remain useful for long periods of time. The skills to understand and hardwire instrumentation and control to the primary equipment are durable and remain essential. “Skills to understand and apply first principles of protection signal transfer via digital methods are durable. However, as the best-known methods change with technology, the skills associated with specific methods, tools, and suppliers are perishable” [11]. The authors of this paper are aware that digitization requires new skill sets, new job descriptions, and new tools. Although the focus is on component reliability, other considerations include the transition from hardwiring, which requires only a handful of decisions, to digital communications, which includes multiple options for each of the following:

- Data flow design
- Protocols
- Communications media
- Network design
- Cybersecurity
- System and device timing and time synchronization
- Redundancy and duplication
- Configuration management

Though the paper does not address organizational challenges, the authors recognize and acknowledge the need to reduce uncertainty about these realities, including those discussed in the following subsections.

1) Maintainability, Ownership, and Manufacturer Dependency

It is important for a system owner to consider availability of internal and external expertise, responsibility for life cycle management of components and tools, and the ability of the organization to maintain, support, and enhance the solution. When relying on a single manufacturer, proprietary technologies are often useful and appropriate as long as knowledge transfer is not inhibited by secrecy. Other concerns include licensing constraints, if they exist, and reduced flexibility to adopt alternative solutions in the future. Health and transparency of the manufacturer’s long-term market presence need to be considered to ensure long-term sustainability, operational resilience, and strategic independence.

2) Open Standards Versus Proprietary Protocols

Open standards, such as IEC 61850, are publicly available for a fee and specify details that enable multiple manufacturers to make products and applications that communicate and operate together for a subset of necessary system functions. Though this may reduce the reliance on a single manufacturer, the development of standards is done by a committee and therefore represents technology that is years or decades old and inhibits innovation. In contrast, proprietary protocols are most often created by a single manufacturer to solve a specific purpose not presently addressed by open standards. These innovations are often emulated years later by the developers of the open standards.

3) Manufacturer-Agnostic IEC 61850 Architectures

Use of the standardized communications models, logical nodes, and data structures defined in IEC 61850 can increase flexibility when documenting operational and maintenance information for the primary and secondary systems. This approach may improve life cycle sustainability and enable DSS devices to be selected based on technical merit. However, innovative features are often available from progressive manufacturers far in advance of their appearance in international standards. Customers often find success by requesting solutions that require some functions to be standards-based solutions while allowing manufacturers to also offer additional sole source improvements [14] [15].

4) Hidden Costs of Proprietary Engineering Tools

Secretive and undocumented communications protocols for device configuration, diagnostics, and engineering access introduce significant costs throughout the life cycle of a system. While such tools simplify product development by the manufacturer, they restrict interoperability, limit access to engineering data, prohibit the use of manufacturer-agnostic engineering tools, and create long-term dependence on the original equipment manufacturer software licenses and computer operating system versions. Future concerns include complex and less transparent data flow design, expenses related to software licensing, specialized training, and manufacturer-managed upgrades.

5) The Risk of Subscription-Centric Architectures

Though digital protective relays first virtualized primary system protection over 40 years ago and centralized logic based on remotely digitized data followed soon after, several activities exist today to create new virtualization and standardization methods in the cloud and on supercomputers. IEC 61850 grew from Utility Communications Architecture (UCA) and other efforts to break up the monopolistic behavior of a handful of SCADA manufacturers, and it allows end users to choose interoperable products best suited to each purpose. The new centralization and virtualization efforts are being

promoted to replace individual devices performing interconnected logic and protection with monolithic software applications. As seen in the electric power system before UCA, as well as multiple other industries today, the annual subscription model introduces structural risks that directly degrade the end user experience. Also, individual relays and controllers are designed and engineered by specialists with deep knowledge of primary equipment behavior. Designs reflect deterministic logic, validated through decades of field experience and rigorous type testing.

However, subscription-based protection platforms rely on people and AI agents skilled in the art of developing large software applications but less familiar with the physical realities of power system equipment. The mismatch between domain expertise and development responsibility may introduce negative impacts and software patch–driven instability. Software subscription support channels may lack specialized protection knowledge, and protection availability will become dependent on subscription status, manufacturer cloud services, and licensing infrastructure.

V. Case Study: Comparing IEC 61850 Architectures at the Utility

The utility decided to continue the evaluation using a PRP network architecture for both the SB and PB. The individual networks would be a single-switch star topology. The initial design has these networks on isolated hardware without the use of virtual LANs for separation of traffic. As part of the overall evaluation of IEC 61850, the team wanted to ensure that the design did not introduce any unforeseen reliability issues when transitioning from traditional copper to a digital system. To do this, it was decided that a statistical availability comparison between the two systems would be performed to validate the IEC 61850 design performance against the traditional design. Hardwiring to the primary system is present in both traditional and DSS designs. Analysis is performed to evaluate the predicted unavailability of the traditional system as well as the change to this unavailability by adding a DSS, which is also hardwired to the primary system.

A. Evaluation of Design Alternatives

FTA was performed to evaluate the additional physical risk to protection, namely the detection and trip circuit, introduced by the added equipment for digitization. The utility considered numerous designs and settled on a single-switch star system architecture deployed as duplicate PRP LANs. Fig. 3 shows the analysis of the chosen design based on the reliability and unavailability results listed in Table II. Many other architectures can be modeled using the same metrics. The utility analyzed the subsystem hardwired to the primary equipment for a single protection application based on 88 I/O connections with 176 contacts wired to a single relay with the results shown in the figure. Since IMU unavailability is approximated to be the same as the relay, System *q* for Relay A and IMU A are the same and System *q* for Relay B and IMU B are the same.

Next, the limited vulnerability design concept, which "is an iterative design technique that improves system performance by identifying application gaps, evaluating the risk they represent, and then mitigating the risks," was used to choose among numerous topology and architecture choices [4]. A reliability evaluation for the addition of the PRP network architecture for Relay B, IMU B, Clock B, and the traditional Ethernet switch was performed based on standardized PRP LAN duplication without LAN error detection, as shown in Fig. 4. The lack of error detection means that the first LAN failure would only be detected during periodic field testing (MTTR = 8,784 hours) and a second simultaneous failure would be immediately detected (MTTR = 24 hours) [4].

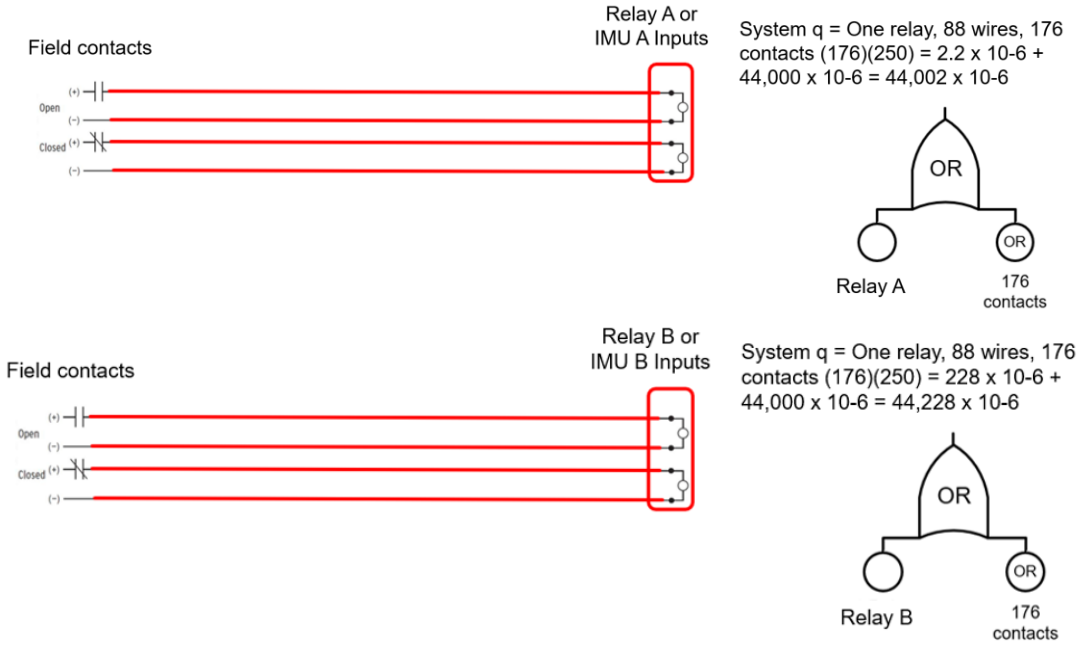


Fig. 3. System Unavailability (*q*) Calculated for DSS Devices Hardwired to the Primary System

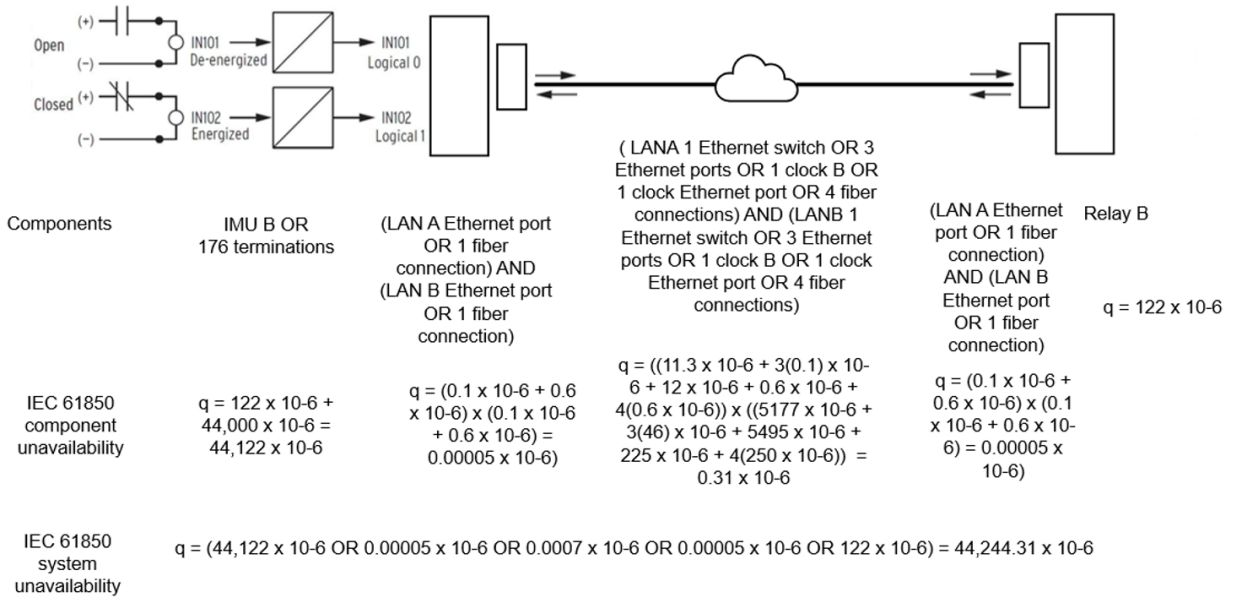


Fig. 4. Change to System Unavailability Calculated for the Addition of DSS PB Devices Using Standard PRP Without Error Detection

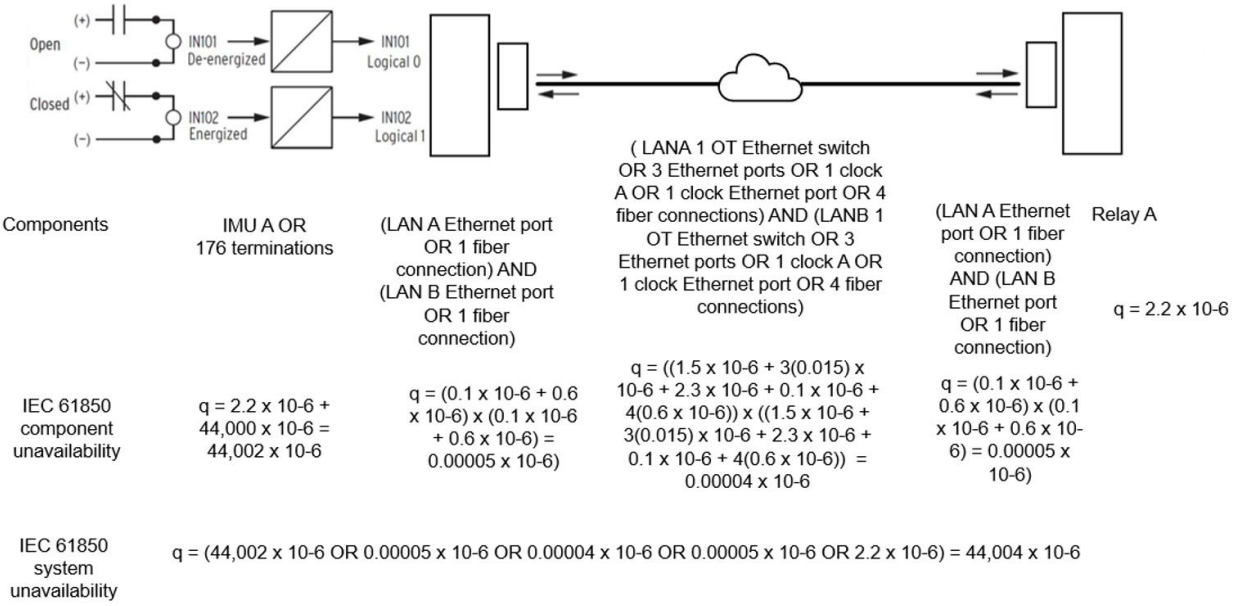


Fig. 5. Change to System Unavailability Calculated for the Addition of DSS PB Devices Using PRP Error Detection Enhancement

Next, evaluation for the addition of the PRP network architecture for Relay A, IMU A, Clock A, and the OT Ethernet switch was performed based on Manufacturer A standardized PRP LAN duplication enhancement of LAN error detection, as shown in Fig. 5. Immediate detection of a PRP LAN failure means that failure of either LAN A or LAN B components would be immediately detected (MTTR = 24 hours) [4].

System availability calculations reveal that adding a DSS PB from Manufacturer A provides all the PB benefits mentioned previously with the modest increase of system unavailability from 44,002 • 10^{-6} to 44,004 • 10^{-6}. This represents a 0.0045 percent increase in the probability that the DSS communications system is unavailable when required. This small increase in the risk of DSS failure to operate, above a conventional hardwired system, is due to product robustness that reduces the likelihood of failures and the innovations that change potential failures from DU to DD alarms. System availability calculations reveal that adding a DSS PB from Manufacturer B provides the PB benefits mentioned previously with the increase of system unavailability from 44,002 • 10^{-6} to 44,244.31 • 10^{-6}. This represents a 0.55 percent increase in the probability that the DSS communications system is unavailable when required. This illustrates a larger risk of DSS failure to operate, above a conventional hardwired system, when using Manufacturer B instead of Manufacturer A.

The difference in additional risk between Systems A and B is largely due to the difference in behavior of the LAN components. System B LAN q = 0.31 • 10^{-6} while System A LAN q = 0.0004 • 10^{-6}, which illustrates that limited vulnerability design methods include researching the availability of diagnostics, troubleshooting, and eliminating DU failures. Together, these methods represent the utility

reducing the risk of a failure of the LAN by a massive 77,400 percent.

B. Lessons Learned

The objective is not to digitize for the sake of digitization. The objective is to adopt DSSs only when engineering evidence demonstrates that they maintain or improve the reliability, maintainability, and operational independence of the hardwired systems they replace.

PRP, by itself, does not automatically improve system reliability. Its value is realized only when it is accompanied by effective monitoring that provides visibility into system conditions and emerging network problems.

Without that visibility, organizations can fall victim to the normalization of inappropriate methods, a process in which unsafe practices gradually become accepted as standard operating procedures. Because Ethernet networks are largely invisible to operators and do not inherently indicate how close they are to failure, warning signs are often overlooked or never recognized.

As a result, shortcuts that were initially viewed as temporary exceptions can slowly replace established procedures. Over time, risks that were once considered unacceptable become routine and complacency begins to replace caution.

The absence of incidents can further reinforce this false sense of security. However, the fact that an unsafe practice has not yet caused a failure does not make it safe. In many industries, major incidents are preceded by numerous smaller deviations that were observed, tolerated, or dismissed because "nothing bad happened."

For this reason, organizations should actively question and correct unsafe practices before they become embedded in the culture and accepted as the new normal. Monitoring, visibility, and adherence to sound engineering principles are essential for recognizing and addressing these risks before they lead to operational consequences.

VI. Conclusion

The reduction in availability associated with DSSs is not a consequence of digitalization itself, but rather the failure to provide adequate detection, mitigation, and recovery mechanisms when technology faults occur. As digital communications are applied to a growing number of protection, control, monitoring, and automation functions, corresponding investments in failure detection, diagnostics, and resiliency become increasingly important. Digital systems have the potential to provide significantly greater observability and diagnostic capability than traditional hardwired designs, but these benefits are realized only when supported by sound engineering practices.

Achieving improved reliability is therefore not automatic. It requires rigorous engineering discipline, careful consideration of system architecture, and adherence to fundamental reliability principles. True innovation is not achieved by bypassing established engineering processes or neglecting foundational design concepts. Instead, oversimplified solutions can obscure inappropriate methods and design weaknesses that become difficult to recognize when first principles are abandoned. The result can be hidden failure modes, reduced redundancy, and the introduction of new risks that may not be immediately apparent.

Because of these considerations, reliability should be evaluated using a comprehensive set of metrics that includes availability, risk of failure while in service, and restoration or return-to-service performance. Open, manufacturer-agnostic architectures further support long-term maintainability by providing flexibility for future expansion, modernization, and equipment replacement.

A risk-informed engineering approach transforms uncertainty into measurable and predictable reliability outcomes. Such design processes often demonstrate substantial differences in availability among alternative DSS architectures. When digital PB communications are implemented using sound engineering practices, the predicted reduction in overall system availability can be very small while providing significant benefits. These benefits include safer control house construction and maintenance practices, increased access to operational and diagnostic information, easier redistribution of existing data, simplified integration of new field measurements, and support for the digitalization of both new and traditional utility processes.

VII. References

[1] D. Dolezilek, C. Gordon, and D. Anderson, "Fast Fault Detection, Isolation, and Recovery in Ethernet Networks for Teleprotection and High-Speed Automation Applications," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2016.

[2] ASTM E1699-14, *Standard Practice for Performing Value Engineering (VE)/Value Analysis (VA) of Projects, Products and Processes*

[3] IEC 61850-3, *Communication Networks and Systems for Power Utility Automation* – Part 3: General Requirements, 2013.

[4] D. Erwin, H. Torres, D. Hertel, E. Munch, and D. Dolezilek, "FERC Risk-Informed Decision Making Applied to Digital Protection Systems," proceedings of the 50th Annual Western Protective Relay Conference, Spokane, WA, October 2023.

[5] R. Dubey, B. Reed, and M. Thadani, "Using Machine Learning for Long-Term Forecasting of Extreme Weather-Induced Distribution Grid Failures," CIRED Chicago Workshop 2024: Resilience of Electric Distribution Systems, Chicago, USA, 2025, pp. 1–5.

[6] M. Silveira, D. Dolezilek, S. Wenke, and J. Yellajosula, "Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation," proceedings of the 74th Annual Conference for Protective Relay Engineers, virtual format, March 2021.

[7] M. Ross, J. Bettler, A. Sprenger, J. Silva, A. Wade, D. Dolezilek, M. Silveira, and R. Abboud, "Case Study: Defining and Measuring Protection Signal Transfer Speed, Latency, and Reliability Within Digital Trip Circuits," proceedings of the 75th Annual Conference for Protective Relay Engineers, College Station, TX, March 2022.

[8] J. Bettler, D. Dolezilek, D. Bowen, S. Westervelt, and J. LaBlanc, "Applying Digital Secondary Systems to Optimize Power System Reliability," proceedings of the 59th Annual Minnesota Power Systems Conference, St. Paul, MN, November 2023.

[9] ISO 31000:2018, *Risk Management — Guidelines*, 2018.

[10] 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, Spokane, WA, October 2020.

[11] D. Dolezilek, P. Lima, G. Rocha, A. Rufino, and W. Fernandes, "Comparing the Cost, Complexity, and Performance of Several

In-Service Process Bus Merging Unit Solutions Based on IEC 61850," proceedings of the 15th International Conference on Developments in Power System Protection, Liverpool, United Kingdom, March 2020.

[12] 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.

[13] W. Denson, G. Chandler, W. Crowell, A. Clark, and P. Jaworski, "Nonelectronic Parts Reliability Data 1995," Defense Technical Information Center, Fort Belvoir, VA, 1994.

[14] S. Al Obaidli, V. Subramaniam, H. Alhuseini, R. Gupta, D. Dolezilek, A. Kalra, and P. Sankar, "IEC 61850 Beyond Compliance: A Case Study of Modernizing Automation Systems in Transmission Power Substations in Emirate of Dubai Towards Smart Grid," proceedings of the Southern African Power System Protection & Automation Conference, Johannesburg, South Africa, November 2017.

[15] "Inside DEWA's Digitally Optimized Substation Design Editorial," LinkedIn, September 2, 2026.

VIII. Biographies

Lauren Donati, PE, is a senior engineer in System Protection Engineering at Xcel Energy with more than 14 years of experience in power system protection and control. Lauren holds a Bachelor of Science in Electrical Engineering from Michigan Technological University and is a licensed professional engineer in both Minnesota and Colorado.

In her time at Xcel, Lauren has played a key role in advancing utility protection practices by leading process improvement initiatives focused on reducing construction delays and communication-setting errors and helping establish a program to oversee the protection organization's review of Critical Infrastructure Protection (CIP) software patches. She is a recognized subject matter expert in NERC PRC-004 compliance and recently led Xcel Energy's efforts during a NERC audit of the standard.

Throughout her career, Lauren has evaluated and implemented emerging protection technologies, serving both as a technical lead and project team member on the assessment of new devices for utility applications. She currently leads Xcel Energy's IEC 61850 Substation of the Future initiative, helping shape the next generation of digital substation architecture and protection systems.

David Dolezilek is a fellow 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 information technology applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of Utility Communications Architecture 2 (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.

© 2026 by Xcel Energy and Schweitzer Engineering Laboratories, Inc.
All rights reserved.
20261104 • TP7284-01