Trans-Alaska Pipeline System— Improved Safety and Reliability Via Main-Tie-Main, Arc-Flash, and Fast Bus Protection Schemes Using IEC 61850 Over a Software-Defined Network

Kevin Lythgoe
Alyeska Pipeline Service Company

Tanushri Doshi, Dwight Anderson, and Kenny Sheffler
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 71st Annual IEEE IAS Petroleum and Chemical Industry Technical Conference, Orlando, FL, September 11–14, 2024.

For the complete history of this paper, refer to the next page.

Presented at the
71st Annual IEEE IAS Petroleum and Chemical Industry
Technical Conference (PCIC)
Orlando, Florida
September 11–14, 2024

TRANS-ALASKA PIPELINE SYSTEM—IMPROVED SAFETY AND RELIABILITY VIA MAIN-TIE-MAIN, ARC-FLASH, AND FAST BUS PROTECTION SCHEMES USING IEC 61850 OVER A SOFTWARE-DEFINED NETWORK

Tanushri Doshi
IEEE Senior Member
Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Ct
Pullman, WA 99163, USA
Tanushri_Doshi@selinc.com

Dwight Anderson
IEEE Member
Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Ct
Pullman, WA 99163, USA
Dwight_Anderson@selinc.com

Kevin Lythgoe
Alyeska Pipeline Service Company
300 Dayville Rd, Mail Stop 777
Valdez, AK 99686, USA
Kevin.Lythgoe@alyeska-pipeline.com

Kenny Sheffler
Schweitzer Engineering Laboratories, Inc.
1597 Cole Blvd, Bldg 15, Ste 350
Lakewood, CO 80401, USA
Kenny_Sheffler@selinc.com

Abstract—An 800-mile long pipeline system transports North Slope crude oil from Prudhoe Bay across the State of Alaska to Valdez. The Valdez Marine Terminal is the northernmost ice-free port in North America, where tankers are loaded to deliver the critical crude oil supply to market. The operator of this pipeline system requires a reliable, safe, and redundant power supply for efficient and safe operation. Any electric power disruption and the associated downtime severely impacts the flow of oil through the pipeline and the loading of the tankers. The electric power reliability and safety is improved via a custom main-tie-main scheme, along with an arc-flash and fast bus protection scheme, using the high-speed IEC 61850 Generic Object-Oriented Substation Event protocol. This solution is also implemented with cybersecurity best practices that are resilient to external threats using a software-defined network supporting a zero-trust architecture and security gateways. This paper dives deeper into the objectives, design philosophy, communications architecture, and testing procedure for this solution. The scheme is standardized and successfully commissioned into service at Valdez Marine Terminal for one medium-voltage and two low-voltage switchgear facilities in 2019. This innovative solution is then scaled to include further switchgear facilities from 2019 to the present.

Index Terms—HIL, MTM, SDN, RTDS, GOOSE, arc flash, crude oil

I. INTRODUCTION

The Trans-Alaska Pipeline System (an 800-mile pipeline), an engineering marvel, is one of world's largest pipeline systems, spanning the remote Alaskan terrain. The Valdez Marine Terminal (VMT) is at the southern end of the 800-mile pipeline, which transfers the crude oil from the North Slope to oil tankers for shipment to the lower 48 states. The VMT consists of crude oil storage tanks and the associated equipment required to load the oil tankers. It is an industrial facility that generates its own power from three steam turbine generators that are fed from three boilers. This generation is supplemented by ultra-low sulfur diesel black start generators. The electrical distribution network comprises 13.8 kV, 4,160 V and 480 V switchgear. Because of the safety and financial consequences of the loss of power, the critical loads are designed to be fed by a primary and alternate power source in the case of a failure or other unforeseen event.

The initial effort was initiated to upgrade the protective relays on the 4,160 V medium-voltage switchgear at the VMT. Part of this upgrade required implementing a customized main-tie-main (MTM) transfer scheme. During the design and planning phase, the pipeline operator had an arc-flash event on the 4,160 V medium-voltage switchgear. The upgraded design is intended to retrofit new relays, implement a residual voltage MTM transfer scheme, and also add arc-flash and fast bus protection schemes. The pipeline operator adopted an arc-flash protection scheme to completely isolate the affected bus. To accomplish this, it was decided to implement a protective Parallel Redundancy Protocol (PRP) network comprising utility feeder protection intelligent electronic devices (IEDs) and software-defined network (SDN) switches. The developed protection scheme and the network architecture were validated and enhanced in a controlled laboratory environment using a real-time digital simulator (RTDS) with a hardware-in-the-loop (HIL) capability. As of the writing of this paper, the pipeline operator has successfully upgraded the 4,160 V IEDs to include MTM transfer function, arc-flash, and fast bus protection. In addition to this, seven upgrades have successfully been implemented on the 480 V low-voltage distribution switchgears using Generic Object-Oriented Substation Event (GOOSE) messaging on the PRP network for MTM transfer function and arc-flash protection. Lastly, the generator control systems and voltage regulators were updated for the 13.2 kV turbine generators.

The redundant Ethernet communications network integrates high-speed protection schemes (e.g., arc flash, fast bus protection, and MTM schemes using IEC 61850 GOOSE), and Supervisory Control and Data Acquisition (SCADA) application, using a combination of Modbus and the DNP3 protocol.

II. POWER DISTRIBUTION SYSTEM

The power system at the VMT features two 4,160 V medium-voltage switchgear lineups fed from two separate 13.8 kV medium-voltage switchgears through a delta-wye-grounded distribution transformer. The dual 4,160 V switchgear lineups feed the 4,160 V loads and four 480 V low-voltage switchgears via delta-wye-grounded transformers. The types of loads fed at this station include air, gas, and vapor compressors; water pumps; and motor control centers (MCCs). The 4,160 V and the 480 V switchgears feature MTM and arc-flash protection schemes. In addition to this, the 4,160 V switchgear features the fast bus protection scheme. Each 480 V switchgear has a source from the 4,160 V Bus A and from the 4,160 V Bus B. Multiple MTM designs provide redundancy at every voltage level to ensure power delivery to critical loads. The system configuration for the VMT discussed in this paper is illustrated in Fig. 1.

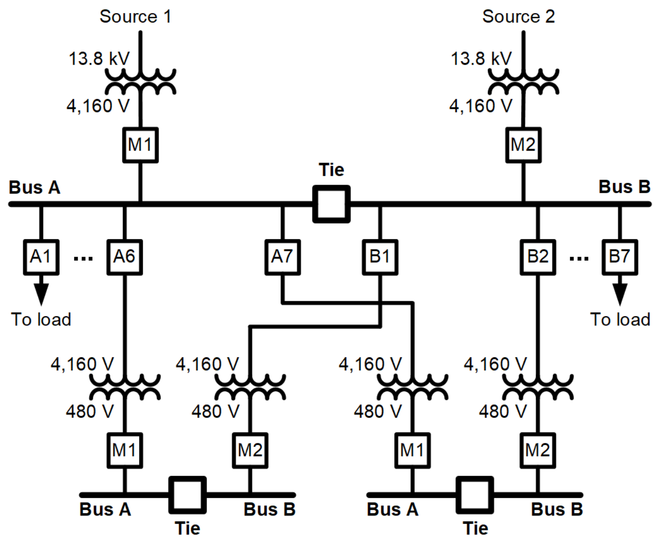

Fig. 1 System Configuration

Source 1 and Source 2 are on a 13.8 kV bus, connected together via a tie breaker. There are two turbine generators on the Source 1 bus and one turbine generator on the Source 2 bus. Normal operation is with the tie breaker on this 13.8 kV bus closed. During normal operation, the 4,160 V and 480 V main breakers (M1 and M2) are closed, and the tie breaker (tie) between the two switchgears is open. The 13.8 kV switchgears, 4,160 V main, and tie breakers are designed and specified to be capable of supporting all loads on the 4,160 V Bus A and Bus B at any given time.

III. PROTECTION, CONTROL, AND AUTOMATION DESIGN

The solid-state relay upgrade to an IED at the VMT allows for more robust and advanced MTM schemes, arc-flash protection, and fast bus tripping schemes to be implemented. These upgrades alone can boost safety and redundancy of the system, but redundant design is also used throughout the schemes. The arc-flash trips are sent over GOOSE with a parallel hardwired trip to critical protection devices upstream and downstream. The arc-flash scheme can therefore still function if there is a loss of communications. Furthermore, MTM schemes are implemented at both the 4,160 V and 480 V switchgears. Since the 480 V switchgear is fed from the 4,160 V switchgear, the 480 V system not only has an MTM scheme, but the supply for this switchgear has an MTM scheme. These multilevel redundancies provide additional assurance that safety and power system reliability are maintained even if there is a system contingency, such as a loss of sources or loss of communications. The following safety enhancements provided by the IEDs are also implemented: a breaker fail trip, breaker fail to close, and 10-second delay to close the breaker and allow operators to exit the switchgear room.

A. Residual Voltage MTM Functionality

When a source fails, the MTM scheme's function is to automate the process of opening the main breaker with the lost source and to close the tie breaker. The remaining main breaker then supplies power to both the buses in the switchgear. The MTM schemes are applied using customized user logic on industrial feeder protection digital IEDs. The IEDs receive current and voltage measurements from the current transformers (CTs) and potential transformers (PTs) as well as the breaker status from their respective breakers. They are configured with trip and close outputs to control their respective breaker. All other information, such as the breaker status of the other breakers in the scheme and alternate source health, are communicated over the Ethernet network via GOOSE messaging. Each main IED is configured with two voltage inputs, one from the source-side PTs and the other from the bus-side PTs. The tie IED is configured with PTs located on Bus A and Bus B.

The MTM scheme is configured to manually transfer/retransfer and automatically transfer for a loss of source. Additionally, the schemes have additional logic for a simultaneous or staggered loss of both sources. The MTM scheme is designed so that it can be disabled locally or remotely on all of the IEDs involved at any time if necessary.

1) Manual Transfer/Retransfer

The manual transfer/retransfer process provides the option to configure the switchgear to be fed from one source, through the tie breaker, in a closed transition. This results in an uninterrupted transition and is intended to be used when maintenance is required on one of the main breakers or associated upstream equipment with no need for downtime.

When the tie breaker is manually closed, provided the close permissive is met, a preselected main breaker opens. Additionally, when the opened main breaker is manually closed, the selected tie breaker opens. The main breaker to be opened must be selected to trip via the dedicated selector switch on the relay panel. The tie breaker must then be closed locally or remotely. After the tie breaker closes, the main breaker opens after a configurable time delay. Intentional delays are programmed between the manual close and open commands from the relay panel and the actual breaker closing or opening for the safety of the operator.

The manual restoration process brings the system back to the normal operating scenario with the mains closed and the tie open. The tie must be selected to trip via the dedicated selector switch. The currently open main breaker must then be closed locally or remotely. After the main breaker closes, the tie breaker opens after a configurable time delay. Once the tie breaker is opened, the system is back to the normal operating scenario.

2) Automatic Transfer on Loss of Source

The automatic transfer process supervises two automatic functions within the MTM scheme: main automatic open and tie automatic close.

The initiator for an automatic transfer is a source undervoltage. The main breaker opens if a source undervoltage of a configurable threshold or lesser exists for longer than a user-settable time delay to ride through the voltage transients in the power systems. The automatic transfer process is supervised by several permissive elements and must pass through all MTM IEDs for an automatic transfer to occur. Both the main IEDs and the tie IED are continuously exchanging permissive and status information via GOOSE communications.

After an undervoltage is qualified, the associated main IED trips on the automatic transfer trip logic. Additionally, the feeder IEDs see the undervoltage condition and trip their respective breakers after their respective undervoltage pickup has timed out. The tie IED implements an open transition and is expected to close after the following criteria of a voltage and timing check are met: the bus residual voltage is below the user-settable threshold, and the user-settable time delay has elapsed after the main breaker has opened. The 4,160 V MTM and 480 V MTM automatic transfer timing is identical, so the main breakers are expected to trip at the same time and the tie breakers are expected to close at the same time. Lastly, the feeder breakers that tripped on undervoltage should be manually closed to complete the transfer.

The system is returned to the normal configuration through the manual retransfer process described in the previous section. Automatic retransfer is not applied due to the critical nature of the loads and the safety of the operators.

3) Simultaneous Loss of Both Sources

Additional logic is required for the corner case, where both 13.8 kV sources are lost at the same time. The MTM logic eliminates a transfer, and the main breakers open based on the 52b contact from the upstream breaker. The MTM scheme is defeated because both sources are unhealthy. The feeder breakers and downstream 480 V MTM breakers are tripped via the undervoltage element. The downstream MTM is also defeated because both the upstream 4,160 V Bus A and Bus B are dead. At this point, the whole system is dead. The system is manually restored to normal with the 13.8 kV breakers closed first, followed by the 4,160 V mains and the 480 V mains, respectively.

4) Staggered Loss of Both Sources

Lastly, the MTM scheme addresses the scenario where the 13.8 kV sources are both lost but at different times. After the first source is lost, the 4,160 V MTM scheme and 480 V MTM scheme undergo an automatic transfer. The feeder IEDs that see the undervoltage condition trip on undervoltage protection.

After the second source is lost, the second main IED trips. The remaining feeders trip on an undervoltage condition after their assigned delay expires. The downstream 480 V main opens. At this time, the tie breakers for the MTM schemes remain closed. There is additional logic to trip the tie breaker after a user-settable time delay if both main breakers are opened. The MTM scheme is disabled because both sources are unhealthy. The downstream MTM is also disabled because both the upstream 4,160 V Bus A and Bus B are dead. At this point, the whole system is dead. The system is manually restored to normal with the 13.8 kV breakers closed first, followed by the 4,160 V main breaker and the 480 V main breaker, respectively.

B. Arc-Flash Protection

An arc flash is a dangerous condition associated with the release of light and thermal energy caused by an electric arc. It can cause life-threatening injuries to personnel and damage equipment. Simple routine tasks (e.g., racking in and racking out of a circuit breaker), human error, or equipment failure can produce an arc flash. Statistics documented in [1] show that there are about 30,000 arc-flash incidents every year. These incidents resulted in an average annual total of 7,000 burn injuries, 2,000 hospitalizations, and 400 fatalities per year. Therefore, arc-flash mitigation, safety measures, and appropriate personal protective equipment (PPE) are very critical. IEEE 1584-2018 [2] and National Fire Protection Association (NFPA) 70E [3] cover some important information about arc flashes, associated calculations for incident energy, the safe working distance from equipment, and PPE requirements.

In 2019, the pipeline operator experienced an arc-flash event in their 4,160 V switchgear, requiring the replacement of a circuit breaker, associated cabinet door, and relay. Due to this event, the pipeline operator decided to upgrade their existing system to include digital IEDs with an arc-flash detection (AFD) feature. The additional high-speed, reliable communications network was then leveraged to trip the entire switchgear via communications protection trips over the IEC 61850 GOOSE protocol. A comprehensive trip scheme was deployed for the 4,160 V switchgear. If an arc-flash is detected by any feeder, main, or tie on the 4,160 V medium-voltage switchgear, the entire 4,160 V bus and the upstream and downstream breakers are cleared. The main and tie IEDs also used hardwired trips in parallel with the GOOSE messages for added reliability, in case of a contingency due to network failure.

1) *Arc-Flash Protection Design*

While there are various methods to achieve AFD, using the light detection feature supervised by current-sensing technologies applied with high-speed output contacts provides highly reliable and fast detection of an arc-flash followed by isolation. The energy produced by an arc-flash event is proportional to the voltage, current, and the duration of the event (V • I • t) [4]. IEEE 1584-2018 specifies that the arc time is linearly proportional to the incident energy. Therefore, reducing the fault-clearing times is critical.

In this implementation, the digital IEDs with an AFD feature are configured by using arc-flash light sensors supervised by phase- and neutral-overcurrent elements to securely and reliably trip for an arc-flash event [5]. Two types of light sensors are implemented: point and loop sensors. Point sensors are omnidirectional and best used for individual switchgear compartments, where an arc-flash is most likely to occur, such as breaker stab points. Loop sensors are clear-jacketed fibers that are best used for distributed equipment, such as bus ducts and busbar sections.

2) *Benefits of Arc-Flash Protection*

When an arc-flash occurs, a tremendous amount of energy is released. The incident energy released depends on the AFD IED clearing time. Therefore, if the arc-flash can be cleared quickly, less incident energy is released. The AFD IED implemented in this scheme trips in 2 to 5 ms with high-speed hybrid output contacts. The breaker open time must be included with this short detection time to determine the total incident energy of the arc-flash event.

Additionally, with a communications and hardwired scheme acting in parallel and being redundant, an arc-flash is cleared by the upstream breaker, even if the local breaker does not open. This scheme also clears the 4,160 V and 480 V buses, so backfeed contribution from motor loads are eliminated from sustaining the arc.

3) *Trip Scheme*

The tripping scheme for this application uses hardwired and GOOSE trips to clear the local breaker and surrounding breakers. Fig. 2, Fig. 3, Fig. 4, and Fig. 5 illustrate the trip scheme for an arc-flash detected by the 4,160 V main, 4,160 V tie, 4,160 V feeder to the 480 V system, and 480 V main IED. A blocking signal is provided to the tie breaker IED in the event of an arc-flash event to disable automatic MTM actions.

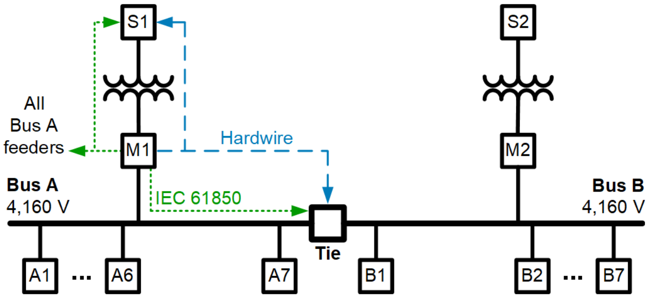

Fig. 2 Arc-Flash Trip for 4,160 V Main M1

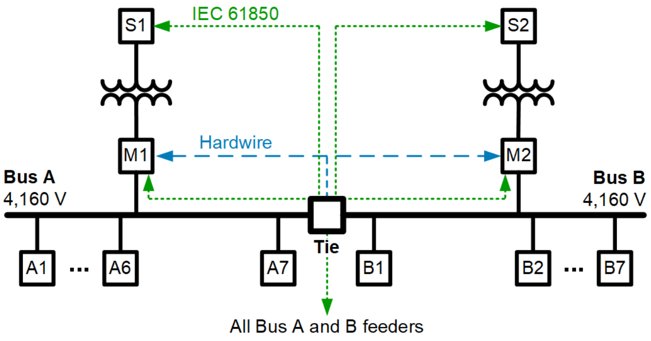

Fig. 3 Arc-Flash Trip for 4,160 V Tie

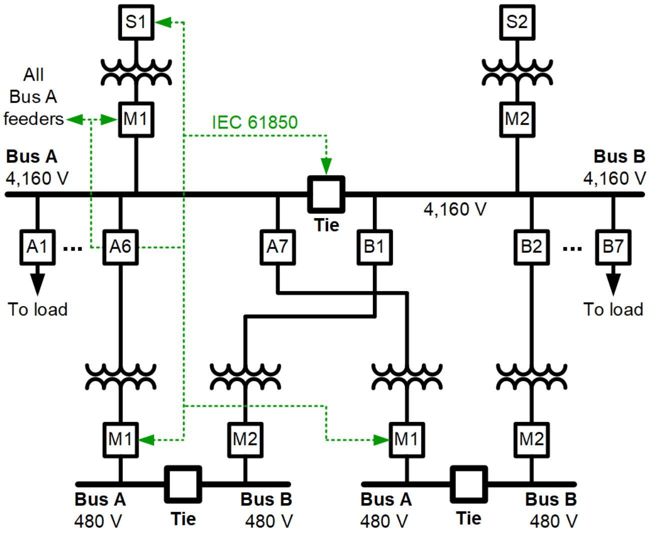

Fig. 4 Arc-Flash Trip for 4,160 V Feeder A6 to 480 V Switchgear

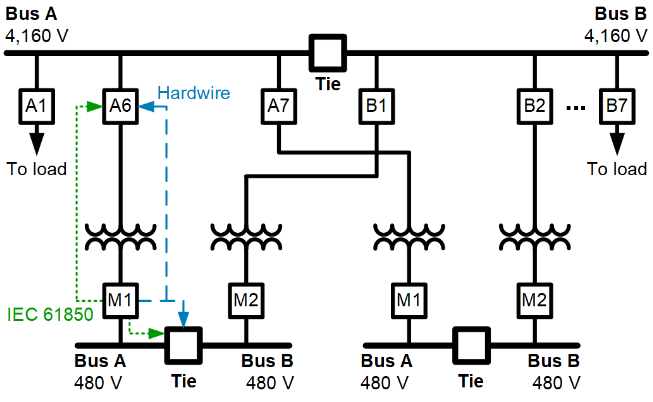

Fig. 5 Arc-Flash Trip for 480 V Main M1

C. *Fast Bus Tripping*

A fast bus tripping scheme uses peer-to-peer IED communications to reduce tripping time for bus faults. In this scheme, the fast bus trip scheme is implemented with GOOSE communications through the SDN switches.

If a fault is downstream of both the feeder and the MTM IEDs on the 4,160 V Bus A or Bus B, the feeder IED trips and the MTM IED does not. Under these conditions, the MTM IEDs receive a blocking signal via a GOOSE message from the feeder IED. Both the MTM and feeder IEDs see the fault. The fault lasts for a duration greater than the $50D_{Main}$ delay of the upstream MTM IEDs, but the downstream feeder clears the fault before the MTM can trip on the time-overcurrent element time-out. This causes the feeder IED to trip, but the blocking virtual bit via GOOSE messaging prevents the instantaneous element in the MTM IEDs from tripping. This provides selectivity, and the MTM IED continues to provide service to the rest of the feeders on Bus A or Bus B.

1) Fast Bus Tripping Overview

A fast bus trip scheme is intended to speed up bus fault-clearing times when a bus differential relay is not present. This is done by setting the MTM IEDs with a high-speed definite-time overcurrent element set to operate for bus faults. This overcurrent element is slightly time-delayed to give enough time to receive GOOSE messages over the Ethernet network from the downstream IEDs to block tripping in case of a fault downstream of the feeder IED. The MTM IED is also configured with a traditional inverse-time overcurrent element set to coordinate with the downstream feeder IED inverse-time overcurrent elements. This element provides backup in case the fast bus scheme is disabled or if the feeder breaker fails to clear downstream faults. Fig. 6 illustrates this overcurrent coordination.

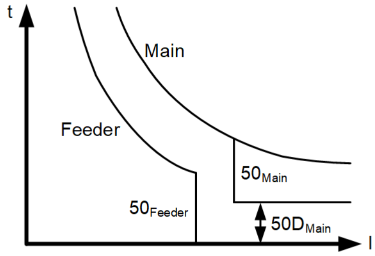

Fig. 6 Fast Bus Tripping Coordination

2) Trip Scheme

The fast bus tripping scheme for the 4,160 V medium-voltage switchgear at VMT is illustrated in Fig. 7.

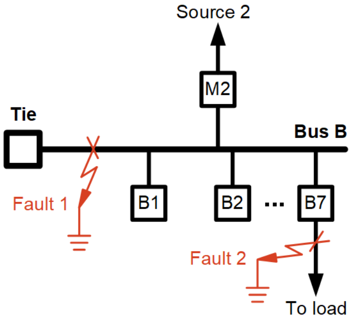

Fig. 7 Fast Bus Tripping Scheme

Fig. 7 illustrates the Bus B of the 4,160 V system. The M2 breaker can be considered closed and the tie breaker considered open. This represents the normal operating scenario where the 13.8 kV Source 2 is feeding the load on the 4,160 V Bus B. Two faults are considered.

The first fault is a bus fault on the 4,160 V Bus B. Since this is a radial system, the only IED that sees the overcurrent condition is the M2 IED. The B1 through B7 feeder IEDs do not see an overcurrent condition and thus do not send a GOOSE block to the M2 IED. If a blocking bit is not received, the definite-time overcurrent element in the M2 IED remains active. Therefore, the definite-time overcurrent element in M2 IED times out after the short communications delay to clear the fault via the M2 breaker.

The second fault is a feeder fault downstream of the B7 breaker. This fault results in both the M2 and B7 IEDs seeing the overcurrent condition. Since the B7 IED registers this fault, a GOOSE message is sent to block the definite-time overcurrent element in M2 IED. The M2 IED continues timing on the inverse-time overcurrent element, but this element is coordinated by traditional methods with the downstream IEDs. The B7 IED times out on its inverse-time overcurrent element and clears the fault.

This trip scheme is replicated for the Bus A and in the tie-breaker IED. The tie-breaker IED receives blocking GOOSE messages from all of the feeders on both the Bus A and the Bus B, because if it is closed, it could be feeding either bus dependent on the MTM configuration.

IV. HARDWARE-IN-THE-LOOP (HIL) TESTING

The design implemented in this project is validated using real-time digital simulation with HIL feature in a controlled laboratory environment before implementing it in the field. The test rack setup includes 13 AFD digital IEDs and 8 SDN switches to mimic the network in the field. All non-MTM feeder IEDs on Bus A and Bus B are wired to illustrate and validate the complete arc-flash protection, fast bus protection, and communication capabilities. The MTM IEDs include the two mains and tie for the 4,160 V MTM scheme and the two mains and tie for the 480 V MTM scheme.

A. RTDS Overview

The RTDS system allows for in-house modeling of the power system circuit and testing of the protection schemes. The RTDS runtime provides real-time controls to the modeled power system. The RTDS supplies the digital and analog inputs to the IEDs under testing. This input from the RTDS input/output (I/O) cube simulates the same signals the IED would see in the actual power system scenario. The IED then issues the appropriate digital output back to the RTDS. This digital output is processed and can be viewed on the runtime (HMI). Additionally, the IED response is captured by the IED LCDs and the Sequential Events Recorder (SER). This test setup provides a platform to simulate many scenarios and corner cases in a laboratory environment, which may be challenging and impossible to test in the field without taking an outage on the in-service equipment. Fig. 8 illustrates the simplified RTDS runtime HMI for the system simulated during laboratory testing.

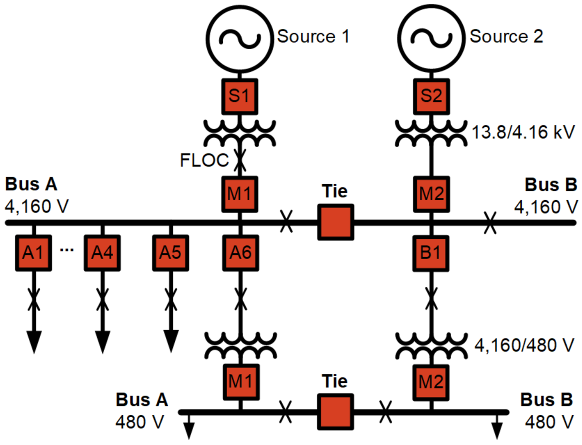

Fig. 8 RTDS Runtime HMI Used During Factory Acceptance Test

All of the boxes represent a breaker controlled by an IED, with the exception of the 13.8 kV Source 2 breaker and the 480 V breaker downstream of the central 4,160 V/480 V transformer. These are dummy breakers used during testing with the RTDS to show the hardwired trips from the relaying on the test racks.

FLOC represents a system fault location. These fault locations are used to validate arc-flash tripping, fast bus trip scheme coordination, and blocking conditions for the MTM scheme. Only one of the 480 V MTM schemes is tested since the second 480 V MTM scheme operates identically.

B. Lessons Learned

The test setup with RTDS allows for the following to be validated during laboratory testing, considering a large number of scenarios and system configurations: 1) MTM scheme, 2) arc-flash trip scheme, 3) fast bus tripping coordination, 4) breaker failure philosophy, 5) communications error alarming, 6) SDN network function testing, 7) design enhancements, and 8) design deficiencies and solutions.

Testing the entirety of the scheme in a laboratory environment saved significant outage time during onsite testing. Additionally, it provided a platform to discuss enhancements to the scheme from operations perspective, make the changes, and validate them.

V. IEC 61850 GOOSE OVERVIEW

IEC 61850 GOOSE is an Ethernet-based protection speed protocol, which is extensively used in protection, control, and automation applications [6]. It requires an Ethernet physical network and typically uses high-speed switches to provide the network connectivity. Other protocols, such as DNP3 and Modbus, can also exist on the same network, since Ethernet is used as the physical layer .

GOOSE is used in this implementation for the MTM scheme, arc-flash protection and fast bus protection, and hardwired I/O on the IEDs. This provides a highly reliable and secure design. With GOOSE, the limitation on the I/O wiring is solved and the design was enhanced with communications between multiple switchgears.

VI. SITUATIONAL AWARENESS

SCADA is an equally integral part of a design, just as the actual protection, control, and automation schemes are to the design. With modern IEDs, the SCADA systems can supervise the power system by collecting data from the IEDs, control circuit breakers remotely, and allow other controls to manage the power system from a central location.

In this implementation, at the local IED level, the front-panel LEDs and pushbuttons are configured on the incoming 13.8 kV IEDs, MTM IEDs, and the feeder IEDs for operator control and status verification. In addition to local control and situational awareness, a remote control is provided via SCADA. The health of the power system can be continuously monitored by analog and digital data (e.g., currents, voltages, circuit breaker status, and trip and fault alarms) collected from the IEDs using communications protocols supported by the Ethernet network. In this application, data are collected by a data concentrator from all the IEDs in various switchgears, based on their location. The data from these individual data concentrators at different locations are collected by a master data concentrator located at a central location via DNP3 protocol, which is passed on to the facility's distributed control system via Modbus protocol.

VII. NETWORK ARCHITECTURE

A. Evaluating the Technologies, Software-Defined Network (SDN) and Rapid Spanning Tree Protocol (RSTP)

There are a number of options to choose from when interconnecting Ethernet networks. In this application for a pipeline operator, interconnecting operational technology (OT) networks based on control packets presented unique challenges. Namely, the design needed to optimize and prioritize the flow of IEC 61850 GOOSE messages (high-priority multicast messages for peer-to-peer communications) across the network to provide operational control, which required precise network engineering. RSTP was evaluated, but this paper shares how using SDN technology to deliver traffic on an Ethernet network afforded superior resiliency, security, and maintainability.

B. Brief Background on SDN

SDN was developed to manage information technology (IT) networks with large volumes of traffic and frequent network topology changes. Even so, SDN found benefits of Ethernet networks located in power substations and industrial controls system networks. For example, in the system network there was not a need for the network to undergo frequent changes. Also, the operational network is responsible for critical processes and high-speed decision-making, as required by an MTM and arc-flash operational requirements; therefore, these applications demand a network that is very predictable, very deterministic, and at the same time, permits updates to the network devices. In early design discussions, protection, automation, and networking engineers evaluated the characteristics of an SDN network and more traditional RSTP network designs [7].

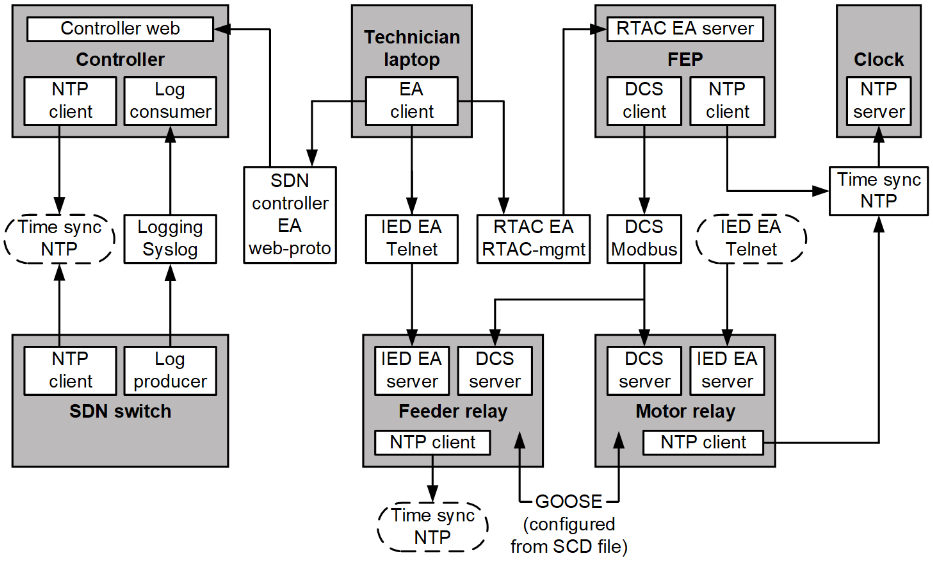

Fig. 9 Example SDN Data Flow Diagram

The example data flow diagram in Fig. 9 is a representation of the various protocols that require permission to flow and, therefore, permit communications between devices. Due to security reasons, the actual data flow diagram is not provided.

C. Considering the Design Between SDN- and RSTP-Based Network Technologies

In design meetings, it was discussed how RSTP required specific bridge priorities and path costs to create predetermined traffic patterns. Bridge priorities and path cost settings help create a base line of the flow of traffic during normal operations. If engineered well, these settings define where the traffic will flow during a device or link failure. By establishing predefined traffic patterns, it is easier to determine and troubleshoot the network as well as help identify attacks. Deviations of the traffic from the baseline become more evident, and the design can support a network operations center in detecting the difference between normal baseline of traffic patterns, flows, and exceptions.

This same monitoring opportunity is also available by default in an SDN. An SDN requires predetermination or network engineering of traffic patterns. Traffic flows are designed for normal operation and failure conditions. SDN switches are preprogrammed with packet-forwarding instructions from the SDN controller. In the proposed SDN solution, it is very important to note that for these particular SDN switches, the flow controller is not required to be connected at all times to the network. Each SDN switch is preprogrammed with the flow information in advance. Additional flows can be defined that can tag unsupported traffic on the network to aid in identification.

The engineering team looked at the SDN network in similar ways to observe how power systems operate: users predefine a safe and resilient set of actions to take in the presence of a power system failure while designing protection systems. SDN networks know in advance what to do in the case of a network link or device failure. Unlike RSTP, there is no need to negotiate with all of the other switches, so it is, therefore, faster. This predetermination speeds up recovery and minimizes packet loss. The design uses predefined forwarding paths for the applications (e.g., engineering access, GOOSE, or SCADA) regarding MTM and arc-flash communications. The SDN solution allows prioritizing critical traffic and choosing to send it on dedicated links. The team shared how the SDN design was able to assign each application its own path, and this permitted greater utilization and opened up bandwidth [8].

By examining the design from a security perspective, there is a significant difference between SDN and RSTP networks. Network designs based on RSTP attempt to allow communications by default, whereas SDN networks operate from the opposite perspective. The SDN network switches operate with deny-by-default on all communications. For an SDN network, all packets that are not predefined nor authorized are either rejected, or optionally, the packets can be identified with a tag and given a specific route and end location, such as an intrusion detection system (IDS). Since each communications path and packet must be authorized in advance, the SDN solution is more secure. SDN is able to prevent unwanted or malicious traffic on the network. For example, someone attempting to scan the SDN network for vulnerabilities and opportunities to attack will not see any results. Not only will their network inspections be completely blocked, but all attempts can be immediately sent to the IDS for analysis and response.

Another consideration for using an SDN solution is that the network spans a very large geographic area with fairly remote access to various substations. There is a difference if a rogue computer is attached to an SDN network switch versus a legacy switch network. In the case of an SDN network, nothing is communicated, as it is deny-by-default. However, on the legacy switch, the rogue computer may exchange information over the network and possibly gain access into the larger system.

D. Selecting a Network Topology

One of the design challenges is choosing a network topology for protection of the communications network. Various design topologies and methodologies are evaluated, and ultimately, PRP is selected. The fast failover and preprogrammed network paths of SDN support the use of PRP. It is discussed if PRP can even be implemented within a single SDN switch, because it is not typically possible with legacy switch technology, such as RSTP. PRP is chosen as the best network topology, because it keeps communications operational even during maintenance (e.g., updating firmware on a network device). The design choice does increase the cost, since two physical communications network fibers and two SDN switches are required. Also, end devices that do not support the use of PRP require a redundancy box (i.e., RedBox).

A PRP network design utilizes two parallel paths through which duplicate packets travel. Losing one path has no impact on the second parallel path. Fig. 10 shows two parallel and redundant paths, Network A and Network B. In this application, the IEDs will receive and send duplicate packets across the network. The IEDs in this application support the use of a PRP design. If an IED did not support PRP, then it would require the use of a RedBox.

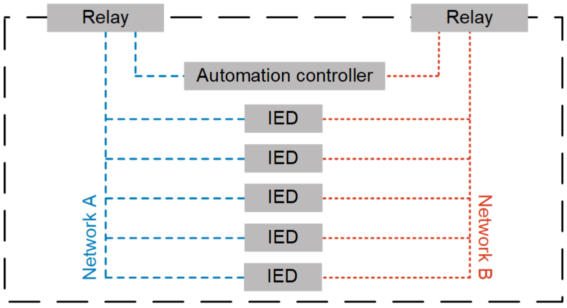

Fig. 10 PRP network example

A PRP network design can use traditional RSTP protocols as well, but it was noted that during faulted network conditions, RSTP can drop or duplicate packets during network healing or reconfiguration for link restoration. As noted in design considerations, if the network switch that is designated as the root bridge fails, it will cause a loss of communications for a few seconds. In large network tests, it was found that when the root bridge comes back online, there can be even longer times for the loss of communications. In some tests of very large networks over 70 switches, reconvergence was never able to complete when the root bridge came back online. This is somewhat analogous to a power system protection islanding. Separation is easier than restoration of an islanded condition. A PRP design avoids the issue, assuming both network paths are operational, but if one network path is taken down to undergo an update and a device or link fails for an SDN-based design, the restoration is in submilliseconds. Since the size of the network can become large, SDN was favored above RSTP, and this eliminated the concern of root bridge failure issues.

The criticality of saving people and preserving the operation of the pipeline favored the use of SDN. As noted in this application, the cost of the SDN switch was also less than the competing RSTP switch that was in consideration.

E. Using a Network Builder Tool That Supports Better Documentation

For this application, the team used a network builder tool that takes a diagram as input and then generates the flows for the SDN flow controller. Taking this approach with this project strongly supports better network documentation. As new items are added onto the network and the Visio diagram is updated, the network builder tool creates the updated flows. One of the authors observed that the network documentation is often created after implementation, and sometimes, it is not created at all. Using the SDN and network builder tool helps avoid this issue and keeps the network documentation up to date. These tools allowed the team to describe the physical and logical network configuration based on Visio drawings. For this project, the tool supports the reporting of differences between the deployed system and the design documents. This greatly aids network engineers during testing and implementation.

VIII. CONCLUSIONS

. This 800-mile long pipeline is a national critical infrastructure system that spans the State of Alaska, delivering crude oil from the North Slope to North America’s northernmost ice-free port in Valdez, Alaska. The crude oil that leaves this port makes up about 4 percent of the nation’s supply. Reliable power system operation and safety to equipment and personnel is extremely critical for uninterrupted flow and loading of the crude oil into the tankers.

The MTM scheme and the fast bus protection designed and implemented in this application help provide continuous power supply to the critical loads in the medium-voltage and low-voltage switchgears at the VMT. The arc-flash protection implemented provides a way to reduce arc-flash energy by providing fast detection and tripping after the onset of an arc-flash. This is critical for personnel and equipment safety.

RTDS with HIL capabilities not only help validate the protection, control, and automation design but also provide the platform to mimic field scenarios that may be challenging or impossible to test in the field. In addition to this, multiple scenarios can be tested in a controlled laboratory environment within a short duration of time. This leads to less field work, which implies shorter and efficient commissioning timelines with limited need for downtime or taking equipment out of service for testing. Multiple network contingencies are simulated in the laboratory environment to validate the system performance. Onsite testing and commissioning further validate the design. The installed schemes are standardized such that they are scalable and can be efficiently implemented on multiple medium-voltage and low-voltage switchgears in the future.

IX. NOMENCLATURE

I	Fault current
V	System voltage
T	Fault-clearing time

X. ACKNOWLEDGEMENT

The authors gratefully acknowledge the contributions of Allen Johnson of Alyeska Pipeline Services Company during the design, development, testing, and field implementation of this project and the continual support during the development of this paper. The authors also appreciate the support and help from David Schmidt, Esteban Cano, Jay Lopes, Kevin Leech, and Tiffany Watson of Schweitzer Engineering Laboratories, Inc. during the commissioning and onsite training phase of this project.

XI. REFERENCES

[1] D. Johnson, “Arc Flash Statistics: 400 Fatalities a Year,” *Industrial Safety & Hygiene News*, May 2013. Available: ishn.com/articles/96001-arc-flash-statistics.

[2] IEEE Std 1584-2002, *IEEE Guide for Performing Arc-Flash Hazard Calculations*.

[3] NFPA 70E, *Standard for Electrical Safety in the Workplace.*

[4] M. Zeller and G. Scheer, “Add Trip Security to Arc-Flash Detection for Safety and Reliability,” proceedings of the 35th Annual Western Protective Relay Conference, Spokane, WA, October 2008.

[5] G. Rocha, E Zanirato, F. Ayello, and R. Taninaga, “Arc-Flash Protection for Low- and Medium-Voltage Panels,” proceedings of the 58th Annual Petroleum and Chemical Industry Technical Conference, Toronto, ON, September 2011.

[6] E. Atienza, “Testing and Troubleshooting IEC 61850 GOOSE-Based Control and Protection Schemes,” proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, March 2010.

[7] C. Gray, “How SDN Can Improve Cybersecurity in OT Networks,” proceedings of the 22nd Conference of the Electric Power Supply Industry, September 2018.

[8] 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, March 2016.

XII. VITAE

Tanushri Doshi received her MS in electrical engineering from Arizona State University and her BTech in electrical engineering from the National Institute of Technology, Nagpur. Tanushri joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2011 as an associate protection engineer. Presently, she is working as an engineering manager for the protection group with SEL Engineering Services, Inc. (SEL ES). Tanushri has experience in power system protection design, relay settings, wildfire mitigation solutions, synchrophasors, commissioning, and testing. She has designed and implemented protection and control schemes with HIL testing using a real-time digital simulator. She is a registered professional engineer in the state of Arizona and an IEEE senior member.

Dwight Anderson received his BS in electrical engineering from Steven’s Institute of Technology. He is now a sales manager for the infrastructure defense division at Schweitzer Engineering Laboratories, Inc. (SEL) in Pullman, Washington. Prior to joining SEL in 2005, he worked 20 years for Hewlett-Packard as an aerospace defense business development manager and systems engineer, working on projects ranging from electronic warfare countermeasures to SCADA system programming. He is a member of the FBI InfraGard forum, regarding the exchange of information related to critical infrastructure protection. He holds the GIAC Security Essentials Certification, and he is a Certified Information Systems Security Professional. Dwight is an extra class HAM radio operator with the call sign WM5F. He enjoys working on the design of high-frequency antennas for restricted space as a hobby.

Kevin Lythgoe is the lead technician at Alyeska Pipeline Services Company (APSC) in the power generation, distribution and protection group. Kevin attended the Ramapo College of New Jersey and University of Alaska Anchorage. Kevin has worked for APSC as a maintenance technician since 1997, specializing in low- and medium-voltage equipment, industrial generation and distribution systems, and electrical protection systems.

Kenny Sheffler earned his ME in electrical engineering from Colorado State University in 2023. He graduated with a BSEE, summa cum laude, from the University of Idaho in 2019. Kenny joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2018 and is currently a project engineer. Kenny has experience in power system protection design, relay settings, automatic transfer schemes, and power system modeling.

Previously presented at the 2024 IEEE IAS Petroleum and Chemical Industry
Technical Conference (PCIC), Orlando, Florida, September 2024.

20240430 • TP7096