Dependable and Secure Line Current Differential Protection Over Packet-Based Wide-Area Networks With Parallel Redundancy Protocol (PRP)

Brian Smyth, Motaz Elshafi, Kale McCarthy, and Douglas Taylor
Schweitzer Engineering Laboratories, Inc.

Presented at the
79th Annual Conference for Protective Relay Engineers
College Station, Texas
March 30–April 2, 2026

Dependable and Secure Line Current Differential Protection Over Packet-Based Wide-Area Networks With Parallel Redundancy Protocol (PRP)

Brian Smyth, Motaz Elshafi, Kale McCarthy, and Douglas Taylor, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Ethernet-based packet transport solutions, including multiprotocol label switching (MPLS) and virtual synchronous networking (VSN) systems, are becoming increasingly common in utilities as the industry moves away from traditional time-division multiplexing (TDM) communications. The adoption of these Ethernet-based wide-area network (WAN) transport technologies presents challenges to traditional communications-based protection schemes, such as line current differential, which must meet strict performance standards. Stringent channel delay, asymmetry, and data-loss limits contribute to this challenge.**

This paper demonstrates how Ethernet-connected protective relays interfacing with various packet-based WANs can improve data availability using Parallel Redundancy Protocol (PRP). When Ethernet networks span geographically separated sites, line current differential schemes face data-alignment challenges due to communication delay. To overcome packet delay variations (PDVs) in a single direction or delay variations in transmit and receive directions from the perspective of each relay, the data can be time-stamped and aligned by using globally synchronized time. Technologies such as IRIG-B or IEEE 1588-2019, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, commonly referred to as IEEE 1588 Precision Time Protocol (PTP), can provide this globally synchronized time to the relay.

In this paper, we validate the ability to provide secure and dependable line current differential protection over packet-based WANs using PRP in multiple laboratory environments. Using utility-grade communications networks, performance data are provided to showcase the redundancy, reliability, and security gained. An evaluation of the solution with various scenarios and network topologies, including data captured using diverse equipment manufacturers, is also provided.

I. Introduction

Utilities are seeking ways to enhance the reliability and security of their protection schemes as renewable energy integration and system loading grows, which increases the complexity of power system protection. Line current differential offers the dependability, security, and speed needed to meet these modern protection challenges. One major component of a line current differential scheme is a robust communications channel.

Potential cost savings are driving utilities to consider transitioning away from traditional time-division multiplexing (TDM)-based networks to packet-based technologies, such as multiprotocol label switching (MPLS), creating new challenges.

Line current differential is commonly applied using synchronous teleprotection protocols, such as IEEE C37.94-2017, *IEEE Standard for N times 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment*, and ITU-T standard G.703, thus demanding strict path delay, symmetry, and redundancy in their communications media. However, migration to nondeterministic packet networks introduces variable delays and the increased possibility of data loss, thereby complicating compliance with these requirements. Therefore, protection applications could benefit from the use of protocols like Parallel Redundancy Protocol (PRP).

II. Line Current Differential Protection Principles

When compared to other traditional line protection schemes, line current differential provides enhanced performance with respect to selectivity, speed, and sensitivity. This protection scheme requires relays located at each line terminal to measure the current entering and leaving the zone of protection. Since the relays need to share data with their peer relays in the scheme, and those relays may span long geographical distances, a communications channel is required.

Fig. 1 illustrates the basic principle of a line current differential scheme.

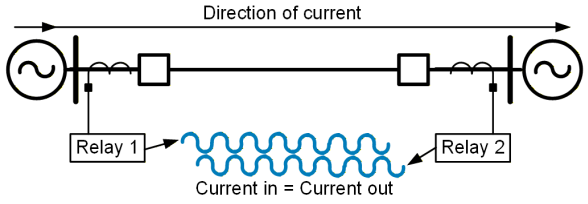

Fig. 1 Diagram of line current differential protection.

Line current differential is based on Kirchhoff's current law: the sum of currents entering and leaving the protected zone should be zero under normal conditions and during external faults. In theory, a deviation from zero indicates an internal fault. In practice, factors such as measurement inaccuracies, current transformer (CT) saturation during external faults, line charging current, and data misalignment can produce false differential currents. Additionally, communications channel availability is critical because data from all line terminals (i.e., relays) must be available and properly aligned for the differential algorithm to operate reliably. These challenges require mitigation strategies. Modern microprocessor-based relays incorporate advanced algorithms to address these issues.

For example, external fault detectors help reduce the impact of CT saturation during external faults by decreasing the sensitivity of the element when saturation is detected, while charging current compensation or carefully engineered settings mitigate the effect of line charging current on high-voltage overhead lines and underground cables.

The communications channel introduces delay for the data that are being shared between the relays and needs to be accounted for using data alignment. Data alignment between the relays is achieved using either channel-based or time-based synchronization methods. Channel-based data alignment uses a ping-pong message exchange to calculate the round-trip delay (RTD) and then estimates the one-way channel delay, as shown in Fig. 2.

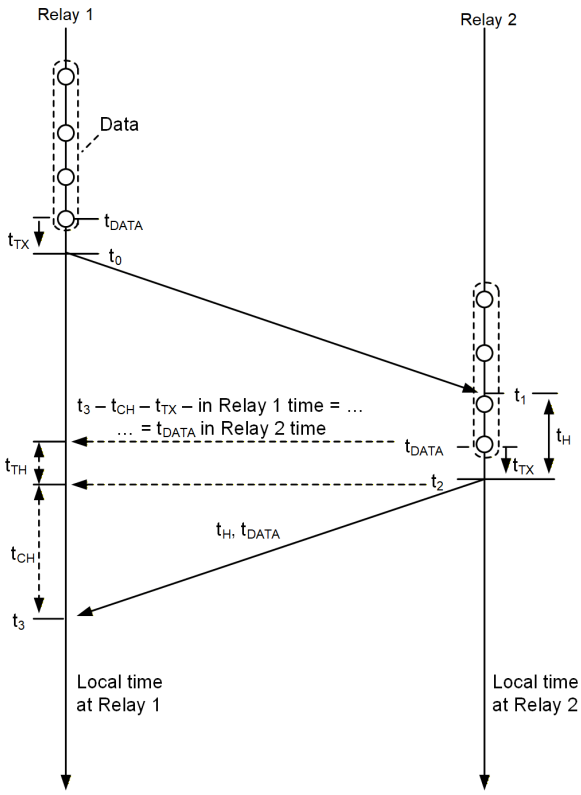

Fig. 2 Illustration of the channel-based (ping-pong exchange) data alignment [1].

With this method, a packet is time-stamped with the internal clock of the relay at transmission, t_0. The remote relay includes its hold-up time (t_H, the interval between receiving the packet and sending a response) in the payload of the next outgoing line current differential response message, which is returned to the local relay. When the local relay receives the response, it time-stamps the packet again (i.e., t_3) and calculates the RTD using (1).

$$\mathrm{RTD} = t_3 - t_0 - t_H \quad (1)$$

The one-way channel delay is then determined by dividing the RTD by two, thereby assuming that the communications channel is symmetric. If the channel is in fact asymmetric, the ping-pong exchange can incorrectly calculate the one-way channel delay, leading to a misalignment of the data causing false differential current, which can affect protection performance. Line current differential algorithms, such as the generalized alpha plane, can provide some resilience to asymmetric communications channels. For more information on the generalized alpha plane or the ping-pong method, see [2].

If the channel asymmetry exceeds permissible limits, which are dependent on the characteristic and settings used, time-based data alignment is an alternate option. The time-based method uses an external high-accuracy and globally synchronized time source to align the data. This method eliminates the impact of channel asymmetry from a data synchronization standpoint. However, channel asymmetry can still affect the speed of the protection scheme and may result in sequential tripping. For applications connected over Ethernet, time-based synchronization is required due to the path delay variation (PDV) also known as jitter in the communications network. Ethernet transport solutions, such as MPLS, can limit path asymmetry to some extent; however, we recommend the network administrator and protection engineer evaluate channel asymmetry to determine if it is within tolerable limits.

Standards such as IEEE 1646 [3] and IEC Technical Report (TR) 61850-90-12 [4] define key performance requirements for communications channels supporting protection schemes. Table I, obtained from [5], summarizes the communications channel requirements outlined in these standards.

TABLE I
COMMUNICATIONS CHANNEL PERFORMANCE REQUIREMENTS FOR PROTECTION CIRCUITS [5]

Scheme	Delay (ms)	Asymmetry (ms)	Restoration Time (ms)
Line Current Differential	5	<0.5	5
Pilot Protection	8	5	5
Direct Transfer Trip	10	5	5

Historically, protective relays have used a serial connection as the interface into the communications network for the line current differential communications channel. A serial interface requires a dedicated port for each serial channel. The protective relay is therefore limited by the number of communications ports available and the number of remote relays to which it can communicate with.

Line current differential relays are trending towards the use of Ethernet interfaces, which allows the relay to connect to many remote relays through a single interface port.

The combination of stringent performance criteria and increasingly complex communications networks emphasizes the need for robust redundancy protocols to ensure reliable and secure operation of line current differential protection schemes. MPLS supports its own self-healing mechanisms; however, because these algorithms can experience restoration times up to 50 ms [6]—and even higher in some testing (clearly in violation of Table I)—supplemental and alternative technologies need to be explored. The following sections address how these technologies can be used to provide dependable and secure communications for line current differential applications.

III. Solutions for Time-stamping Data

Clocks provide the critical function of synchronizing end-devices to a common global time reference. When an end device, such as a protective relay, uses an external time source to synchronize its internal clock, it must know the reported accuracy of the time source relative to the Coordinated Universal Time (UTC) time. International standards were developed to define the behavior of time distribution for various applications. These standards include, but are not limited to, IEEE C37.118-2011, *IEEE Standard for Synchrophasor Measurements for Power Systems*, IEEE 1588-2019, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, commonly referred to as IEEE 1588 Precision Time Protocol (PTP), IEEE C37.238-2017, *IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications*, and IEC 61850-9-3.

The standards mentioned specify that information needs to be encoded in the time message to convey the accuracy of the clock, commonly referred to as time quality. These data allow devices to assess whether the source clock meets their synchronization requirements. For example, certain protection and monitoring functions follow IEEE C37.118, which requires time alignment within 1 µs of UTC. If the external time source reports a quality exceeding that threshold, the device may reject the signal and revert to its internal clock for timekeeping.

Time sources can distribute synchronization signals to multiple devices using a variety of protocols and media. Traditional methods rely on direct or distributed cabling from the clock, such as IRIG-B, while modern approaches support time distribution over local-area networks (LANs) and wide-area networks (WANs) with IEEE 1588 PTP.

For cable-connected time distribution, the signals can be directly connected via coaxial cable, such as RG-58, from the clock to the end device. Alternatively, the clock can use a communications processor to distribute the signal through existing serial connections to save on installation costs. Fig. 3 represents a typical time distribution system using direct cable and a communications processor to connect to multiple intelligent devices (IED in Fig. 3), such as a relay.

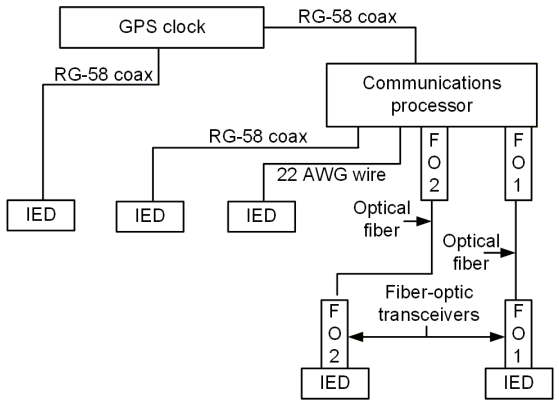

Fig. 3 Typical IRIG-B signal distribution.

Alternatively, technologies that distribute time over Ethernet networks are becoming more common. IEEE 1588 PTP defines how to achieve high-accuracy time distribution over a complex network that experiences PDV. PTP was developed to compensate for buffering delays and account for packet residence time, thus ensuring accurate time distribution over these networks that have variable packet delays. The design of a PTP network plays a critical role in the resilience of global time reference. While multiple interconnected switches that are PTP-aware can be used, it is recommended to have less than 15 hops in a PTP LAN installation [7]. Limiting the number of hops guarantees an accuracy better than 1 µs, which is required for time-sensitive applications. This budget assumes 250 ns of error from the grandmaster (GM) clock, plus approximately 50 ns per network hop. Applying VLANs to segregate PTP traffic can help ensure the traffic is only sent to connected applications that need it, as explained in [7].

IV. WAN Connectivity Models

Line current differential can be applied between substations that span long distances, hence the need for a WAN instead of a LAN to interconnect the relays in the protection scheme. WAN delays are typically much higher than LAN delays due to propagation delays through fiber optics. The longer the fiber-optic distance, the higher the delay. Relays applying line current differential benefit when resilient connectivity is possible across multiple WAN paths.

WAN connectivity types include:

1. Direct fiber optics, sometimes referred to as dark fiber, are fiber optics that have been reserved and become illuminated when used for an application. The pros of direct fiber optics per application include low delay, reliability, and simplicity. The cons are lack of path resilience, cost per fiber-optic run, and management.
2. Wide-area, shared communications network technologies, like legacy SONET MUX and modern Ethernet-based MPLS transport profile (MPLS-TP), MPLS Internet Protocol (MPLS-IP), and virtual synchronous networking (VSN), offer mechanisms for network administrators to build and overlay Ethernet circuits.

Direct fiber offers the lowest possible symmetrical latency for a path between two sites, since there are no transport devices like switches or routers adding buffer and queue delays. The only contributor to path delay is the propagation delay through the fiber itself.

A direct fiber-optic cable run is not path resilient. If an issue occurs in the fiber, there is no dynamic path healing. Additionally, the labor and materials can make it cost-prohibitive for a utility to dedicate an entire fiber-optic cable for a single connection or application, no matter how critical the application. Plenty of utilities recognize this constraint and leverage shared fiber-optic runs for multiple applications using technologies like course wavelength division multiplexing and dense wavelength division multiplexing.

Monitoring fiber-optic health can be a concern. Since it is simply a physical medium, there are limited ways to manage and monitor the health of a fiber-optic connection without

disrupting connected devices, aside from monitoring fiber-optic health via statistics obtained from the connected applications. Statistics collected from connected applications typically include the transmit and receive power levels across the fiber optics, and if power levels degrade, the network administrator can act and remedy the issue.

Transport technologies, on the other hand, offer pros like inherent fiber reuse, ease of management, and path protection. The cons include added management complexity due to additional devices, infrastructure buildout and maintenance costs, equipment replacement, and additional training.

Transport technologies allow for the deployment of Ethernet circuits. Ethernet circuits are logical Ethernet connections that can behave as point-to-point (P2P) connections. Internet Engineering Task Force (IETF) standards call this circuit type a virtual private wire service (VPWS). The connection appears as a transparent P2P fiber-optic-like connection linking exactly two devices. Ethernet circuits can also behave as point-to-multipoint (P2MP) connections. IETF standards call this type of circuit a virtual private LAN service (VPLS). The connection appears as a logical Ethernet switch that can link two or more devices. A single transport network allows network administrators to build and overlay as many Ethernet circuits as needed.

A fiber-optic connection between two transport devices offering VPWS and VPLS services can be shared by many applications. When a centralized network management system (NMS) is employed, the network administrators can easily deploy and monitor VPWS and VPLS services along with terrestrially distributed timing services, voice, and other data applications using the same equipment.

Although path delay will not be as low as connecting an application across a dedicated direct fiber, transport technologies offer mechanisms to minimize the added delay due to queuing and buffering. Quality of service (QoS) rules can be employed, prioritizing critical protection traffic over less critical applications like voice and IT data. This allows critical traffic to attain very high priority queue treatment, thus minimizing PDVs that result from queuing delays.

Transport technologies can offer some resiliency in the event of a fiber-optic break or device failure along the path between multiple sites. VSN networks offer ring-based circuit designs that support primary and backup paths, and these circuits heal extremely quickly in under 5 ms, regardless of circuit type (P2P or P2MP). MPLS networks provide VPWS services that can leverage primary and backup paths with dynamic path healing. MPLS networks provide VPLS services, which can behave as a typical rapid spanning tree (RSTP) or multiple spanning tree (MSTP) network where one or more spanning tree instances help determine a loop-free topology for connected applications and dynamically heal when a link in the spanning tree is disrupted.

Because transport technologies necessitate additional devices, these devices, in turn, increase network complexity beyond one direct fiber-optic connection per application. However, implementation and proper training regarding the use of an NMS simplify management and monitoring of the transport system. Initial costs can be high, and due to cyclical equipment replacement that is typical with MPLS transport networks, costs can increase over time.

V. Evolution of TDM to MPLS and VSN

Due to the criticality of power system protection, the communications system needs to be reliable. TDM was the preferred WAN solution, since it is deterministic and synchronous; it offered dedicated bandwidth, and it transported data with a common clock for synchronous data transfer. TDM is still a viable technology, but fewer vendors are supporting it, and many systems are reaching their end of life.

With electrical utilities transitioning to MPLS networks, it is important to understand the benefits and shortcomings of MPLS. MPLS is a telecommunication protocol that routes data from node to node without using network addressing. The data instead are encapsulated within the MPLS packet and assigned labels, allowing the protocol to route traffic using predefined circuit paths engineered for the virtual private networks. The routers in the network forward the packets based on information contained within the label information base and operate between Open Systems Interconnection (OSI) Layers 2 (data link layer) and 3 (network layer). The MPLS layer is sometimes referred to as OSI Layer 2.5. MPLS can transport different kinds of traffic, including SONET, Ethernet, and IP. With networks transitioning to packet-based infrastructures, many utilities are hoping MPLS will reduce their operational expenses.

MPLS, with the assistance of traffic engineering and resource reservation protocols, can offer better performance and bandwidth use than traditional IP routed networks. QoS allows certain types of traffic to be granted higher priority treatment and guarantees appropriate information rates to reduce the impacts of traffic congestion.

MPLS supports static or dynamic predefined paths. Static circuit paths help ensure more predictable performance by minimizing sudden changes in network delays. MPLS networks can provide path healing using restoration functions for improved circuit resiliency after path failure; however, path restoration may not meet the strict demands of line current differential protection. Two other shortcomings of packet-based networks built on MPLS when compared to TDM are that they operate asynchronously and use shared bandwidth.

An alternative Ethernet transport technology is VSN. VSN was built to deliver TDM-like performance to packet-switched networks [5]. VSN preserves the characteristics of TDM and transmits data synchronously to create a deterministic Ethernet channel. Each circuit crossing a VSN link is assigned dedicated bandwidth. VSN systems allow the creation of low-speed serial circuits as well as Ethernet (i.e., P2P and P2MP) circuits. VSN guarantees path asymmetry to be under 5 ms, and VSN equipment is designed to minimize cyclical equipment replacement. Data loss is minimized because circuits with redundant paths are guaranteed to heal within 5 ms. The VSN approach meets the high demands of line current differential protection channel performance.

VI. Proposed WAN Solutions With PRP

PRP is an Ethernet technology defined by IEC 62439-3. The IEC 61850 standards promote the use of PRP in conjunction with process bus LANs. Its purpose is to provide hitless performance from any single Ethernet network path failure, wherein each Ethernet frame is duplicated across two independently switched networks, and the first copy to arrive is the one that is processed. Since the slower of the two PRP frames is discarded, the end application will not receive duplicate frames.

PRP is designed to be used with two independent network infrastructures, each comprised of one or more network switches known as LAN A and LAN B. Each of these dually attached nodes (DANs) [8] then has a redundant path, allowing a path disruption across one LAN to be transparent to the end application.

Data travels very quickly through each of the LANs since high-performance switches incur low (submillisecond) delays per hop. Network traffic can cross a typical industrial-rated Ethernet switch network in as low as tens or hundreds of microseconds, depending on device and network link speeds, which vary between 10 Mbps to 1 Gbps per link.

In an IEC 61850 substation, protective relays typically communicate with other local relays or process interface units (PIUs). Protective relays communicate using Sampled Values protocols for the purpose of protecting a transmission or distribution line. However, there are situations where a local relay may need to communicate with a remote relay for applications, such as line current differential protection or even a PIU located in a separate substation, reachable across one or more WAN connections or paths. Having data span larger distances requires additional consideration to ensure reliability and security, as the data are now outside of the substation and subject to more potential points of failure. With the requirements of modern power system protection, circuit recovery time may not be acceptable, especially when protecting critical high-voltage power lines. Rather, true hitless recovery is desired.

PRP can achieve hitless path recovery with proper network design. Hitless recovery is dependent on multiple factors, including, but not limited to, the end device of the application and the performance of all switches and routers that form paths through the network. Performance is impacted by traffic forwarding capabilities and ingress and/or egress data buffers.

Although delays across a WAN are typically higher than a LAN, one may protect traffic across independent WANs (such as WAN A and WAN B) with PRP and engineer the WAN paths to have comparable delays. We contend that if the delays across WAN A and WAN B are relatively similar, then PRP can offer hitless failover if one WAN path experiences disruption.

One ought to consider how line current differential relays process properly received packets and discard erroneous ones. A line current differential protection scheme requires a continuous stream of data that is received in the proper sequence to avoid erroneous calculations. Therefore, limits in channel delay differences between the two WANs should be designed to avoid losing sequential data upon path switching. We demonstrate in Section VII that, if the path delay difference between WAN A and WAN B exceeds this limit, then switching WANs would lead to packets arriving out of sequence and the relay would record one or more lost packets. Once the relay starts to receive steady data, it resumes line current differential protection functions, but switching WANs in this configuration does not result in a hitless failover.

PTP can also be applied over the PRP network to provide global time synchronization between protective relays. In this type of application, information is duplicated on two separate LANs or WANs. Fig. 4 demonstrates this type of configuration.

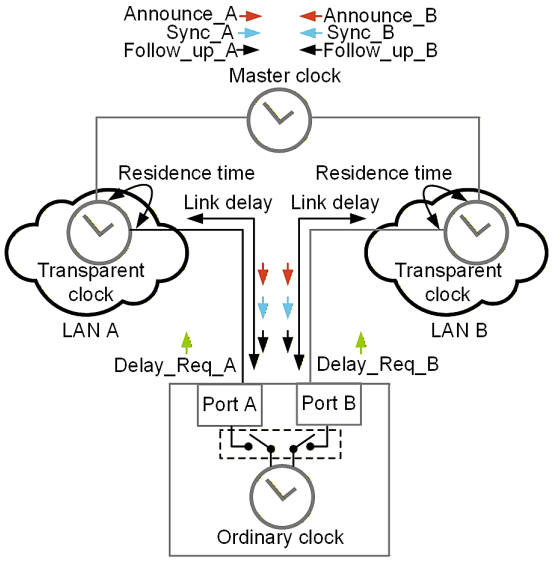

Fig. 4 PTP time synchronization of a PRP network.

This network architecture enables an end device to synchronize to a common clock source delivered over two independent LANs. The same approach can be applied to a PRP WAN configuration. The Best Master Clock Algorithm (BMCA) selects the master clock based on the highest accuracy and lowest path delay. When the device receives timing data from LAN A on Port A and from LAN B on Port B—both originating from the same GM—the BMCA determines the optimal path. This dual-LAN configuration provides resiliency: if one LAN fails (e.g., due to switch failure), the other can continue delivering time. The diagram also includes transparent clocks (Ethernet switches), which update correction fields based on GM timing and forward the timing information without acting as master clocks.

Although it was designed for redundant LANs, we propose that a network administrator could leverage PRP technology when interfacing Ethernet-connected line current differential relays over two independent WANs. WAN A and WAN B can be built using similar or varied technologies. For example, WAN A can simply be a long-distance direct fiber-optic link, while WAN B can be a VPWS or a VPLS service across MPLS. Alternatively, WAN A can be a VPWS or a VPLS service across MPLS, while WAN B can be an Ethernet circuit across a VSN network.

VII. Testing and Results

A. Laboratory Testing of WANs With Similar Delays

PRP was applied over two independent and completely disjointed WANs to avoid a single point of failure. The relays were configured to use time-based synchronization for the line current differential channel and used IRIG-B for the time distribution from the common clock. Various scenarios were tested to demonstrate the ability of PRP to provide hitless recovery upon disrupting one of the WANs. To prove the value PRP adds, we decided to eliminate MPLS healing and, instead, focus on removing the WAN link from the relay when creating failures.

Three WAN types were used during laboratory validation, all using short fiber-optic links with submillisecond delay introduced from the fiber-optic cables. The one-way delays reported by the relays using each WAN type are reported in Table II.

TABLE II
BASELINE DELAY MEASUREMENTS FOR EACH WAN

WAN Type	Measured One-Way Delay (ms)
Direct fiber	0
MPLS	0
VSN	0.1

Note that the reported measurements using MPLS are shown as 0 ms due to the resolution of the relay used. From our experience using more precise test sets, MPLS contributes approximately 20–30 µs per hop, assuming 1 GB links between MPLS routers.

Table III provides the scenarios and the results of the tests, which indicate that there were no lost packets during the failure of either WAN.

TABLE III
TEST RESULTS FOR VARIOUS WAN CONFIGURATIONS

Test Case	WAN A	WAN B	Difference in Delay Between WAN A and WAN B (ms)	Dropped Packets Upon WAN B Failure
1	Direct fiber	Direct fiber	0	0
2	VSN	Direct fiber	0.1	0
3	VSN	MPLS	0.1	0
4	MPLS	Direct fiber	0	0
5	MPLS	MPLS	0	0

The tests established a baseline with the WAN combinations outlined in Table III and confirmed that the communications links experienced no lost packets under ideal conditions when both WANs were functional. The relays under test each provided a communications report for the line current differential channel, and in that report are the number of lost packets in the past 40 s and 24 hr.

Note that relay models may vary in their determination of a lost line current differential packet. This specific relay performs a binary checksum (BCH), verifies that the packet arrives within the expected time window (4 ms ± 1 ms), and confirms the packet received is the next one expected in the packet sequence. For the expected time window, the ±1 ms is based on the Ethernet jitter tolerance, which is a setting in the relay. Based on these checks, a line current differential communications report indicating that a packet was not lost confirms that the communications channel has met all of these requirements. This is why the line current differential communications report was chosen to verify how the relay performs when a failure is induced in a single WAN path. This report also provides received path delay measurements to avoid the need for additional test set equipment. A line current differential communications report from a relay is shown in Fig. 5.

```
87L APPLICATION STATUS
                    2E - Two terminals over Ethernet
                    MASTER

MEDIUM/PROTOCOL     Configuration                 Status
Ethernet Port A     1000BASE-SX, PRP              In use
Ethernet Port B     1000BASE-SX, PRP              In use
Synchronization     External-time-based           High precision

TIME SOURCE         Local Status                  Remote Status
                    Locked                        Locked

CHANNEL ADDRESSING
Local Address       01-30-a7-01-01-01
Remote Address 1    01-30-a7-02-02-02
VLAN Tag            1

STATISTICS          Channel 1
Channel Status      OK
Channel Role        In use
Receive Status      OK
Synch Config        Ext-time-based
Synch Status        Ext-time-based
Synch Accuracy      High precision
Time Status         Locked
High Lost Packet Count OK
Receive Delay (ms)     0.0
Lost Packet Count 40s  0
Lost Packet Count 24hr 0
```

Fig. 5 Sample line current differential communications report.

Fig. 5 illustrates a line current differential communications report taken at steady state where WAN A and WAN B are fully operational. It shows that the relay Ethernet Ports A and B were configured in PRP mode, how that the relay used a high-precision synchronization source, and that no lost packets were recorded in the past 40 s or 24 hr. The relay line current differential element was configured to use time-based synchronization via an external IRIG-B time reference instead of the ping-pong (channel-based synchronization) method described in Section II. These tests were performed while independent WAN transmit and receive delays remained symmetrical.

Next, WAN B was disconnected from one of the relays to create a failure, causing the end device to rely solely on data received via WAN A. The change to WAN B is indicated by DOWN for Ethernet Port B, as shown in Fig. 6, a snapshot of the line current differential communications report taken immediately after a failure. Here, PRP functioned as expected, and no lost packets were recorded.

```
87L APPLICATION STATUS
                    2E - Two terminals over Ethernet
                    MASTER

MEDIUM/PROTOCOL     Configuration                Status
Ethernet Port A     1000BASE-SX, PRP             In use
Ethernet Port B     1000BASE-SX, PRP             DOWN
Synchronization     External-time-based          High precision

TIME SOURCE         Local Status                 Remote Status
                    Locked                       Locked

CHANNEL ADDRESSING
Local Address       01-30-a7-01-01-01
Remote Address 1    01-30-a7-02-02-02
VLAN Tag            1

STATISTICS          Channel 1
Channel Status      OK
Channel Role        In use
Receive Status      OK
Synch Config        Ext-time-based
Synch Status        Ext-time-based
Synch Accuracy      High precision
Time Status         Locked
High Lost Packet Count OK
Receive Delay (ms)     0.1
Lost Packet Count 40s  0
Lost Packet Count 24hr 0
```

Fig. 6 Line current differential communications report after a failed WAN.

Communications persisted after every WAN failure event, due to PRP and the availability of at least one WAN. Fig. 6 also indicates that the Receive Delay changed from 0 ms, as seen in the baseline report presented in Fig. 5, to 0.1 ms with the alternate WAN, as seen in the report in Fig. 6.

B. Laboratory Testing of WANs With Varied Delays

Additional tests were conducted to discover limits of WAN delay differences. WAN B is an MPLS network with no added delay impairment, and WAN A is a delay-impaired path with the use of a delay generator. Fig. 7 shows the configuration of the test setup.

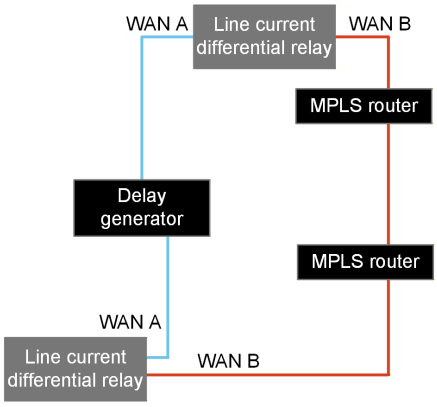

Fig. 7 Variable channel delay test results.

The relay under test expects to receive the next sequential packet 4 ms after the previous one. Even if the packet arrives within this time, if the packet is out of sequence or it fails the BCH check, the packet will be declared lost.

The programmable delay injected into WAN A ranges from 0 ms to 10 ms, and the number of dropped packets upon WAN B failure are shown in Table IV. Results can vary based on the relay in use.

The tests provide confirmation that if the delay difference between the two WANs is less than the 4 ms ± 1 ms Ethernet jitter setting, then the relays will show *no dropped packets* as WAN B fails. Once the 4 ms threshold of WAN delay difference is exceeded, the relay shows dropped packets as it processes data from WAN A. Fig. 8 shows the packet sequence for both WANs and the packets arriving at the remote protective relay for Test Case 8, with 10 ms of delay on WAN A.

TABLE IV
PACKET DROPS BASED ON CHANGE IN DELAY

Test Case	Difference in Delay WAN A to WAN B (ms)	Dropped Line Current Differential Packets Upon WAN B Failure
1	0.5	0
2	1.0	0
3	2.0	0
4	3.0	0
5	3.5	0
6	4.0	0
7	5.0	2
8	10.0	5

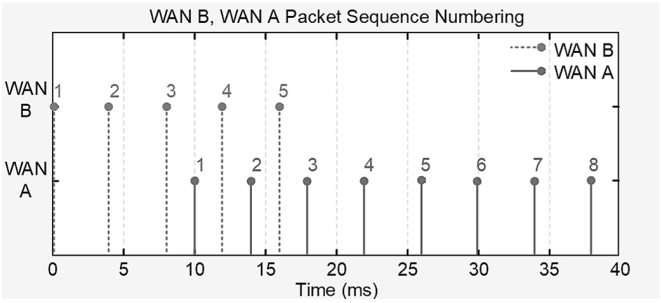

Fig. 8 Packet sequence numbering for WAN A and WAN B, Test Case 8.

In Fig. 8, the WAN A packets are received 10 ms later than WAN B packets. The numbers indicate the packet sequence numbering for the line current differential data received through the two WANs. At the time of transmission, the numbers are identical, as the PRP mechanism in the protective relay creates two identical packets. These packets are then transmitted through the two independent WANs with different delays. Since WAN B is the shorter path delay, the WAN B packets will arrive first and WAN A packets are discarded at the relay per the PRP algorithm. When the connection is broken on WAN B, the relay still receives the data coming from WAN A. However, the protective relay needs the next packet in sequence. As the figure depicts, when WAN B is broken, the remote relay just receives Packet 5. Shortly after, WAN A provides Packet 3 to the relay. The relay declares that this packet is not the next one in sequence, so it determines that the expected Packet 6 is lost. A short time later, WAN A provides Packet 7, which the protective relay determines is the next in sequence. However, the protective relay waits for another consecutive packet to arrive to ensure that the line current differential channel is stable and continues to receive packets in the correct sequence. The relay therefore declares Packets 3, 4, 5, 6, and 7 from WAN A as lost packets because the protective relay has already received Packets 3–5, and Packet 6 arrives much later in time. Therefore, the protective relay registers five lost packets for this scenario, as shown in Table IV and Fig. 9.

```
87L APPLICATION STATUS
                    2E - Two terminals over Ethernet
                    MASTER
                    ALARM ON CHANNEL 1

MEDIUM/PROTOCOL     Configuration                 Status
Ethernet Port A     1000BASE-SX, PRP              In use
Ethernet Port B     1000BASE-SX, PRP              DOWN
Synchronization     External-time-based           High precision

TIME SOURCE         Local Status                  Remote Status
                    Locked                        Locked

CHANNEL ADDRESSING
Local Address       01-30-a7-01-01-01
Remote Address 1    01-30-a7-02-02-02
VLAN Tag            1

STATISTICS          Channel 1
Channel Status      ALARM
Channel Role        In use
Receive Status      OK
Synch Config        Ext-time-based
Synch Status        Ext-time-based
Synch Accuracy      High precision
Time Status         Locked
High Lost Packet Count ALARM
Receive Delay (ms)  --
Lost Packet Count 40s  5
Lost Packet Count 24hr 5
```

Fig. 9 Lost packet count with 10 ms delay difference.

For Test Case 8, which had 10 ms of delay difference between the two WANs, it is observed that the relay registered five lost packets during the changeover to the alternate WAN. If the path delay difference between the two WANs is engineered to be within 4 ms, the communication would be hitless, as shown in Test Case 6 in Table IV.

Result analysis of the tests reveals that Ethernet-connected line current differential relays are successful in leveraging PRP over two independent WANs. In addition, the relay offers hitless failover performance when the delay across both WANs is within its packet arrival threshold.

C. Testing MPLS at a Utility Laboratory

The line current differential PRP performance was tested using MPLS, exclusively, at a local utility that maintains an extensive MPLS laboratory. A four-terminal line current differential scheme was tested on a four-node MPLS network, with a relay at each node (e.g., Relay 4 at Node 4). A simple diagram of the network is shown in Fig. 10. There is a microwave link between Nodes 1 and 2, patch fiber-optic connections between Nodes 2 and 3 and 1 and 4, and 95 km (59 mi) of fiber optics between Nodes 3 and 4. In Fig. 10, the MPLS nodes are depicted simply as numbered circles. The microwave link is ~300 µs of delay. The direct fiber path delays are <100 µs. The 95 km link delay is ~500 µs.

In the first test, the paths taken by line current differential PRP traffic through WAN A and WAN B were automatically selected by the MPLS network itself (“loose” paths). This configuration would not guarantee path diversity but rather results in WAN A and WAN B traversing the lowest delay path. In this test, line current differential packets were lost when the connection between Nodes 1 and 4 broke. The test was repeated several times with 0, 1, 2, or 4 packets being lost during the break. The line current differential communications report of the relay in Fig. 11 captures the case when four packets were lost. The report was captured after breaking the fiber connection between Nodes 1 and 4 and subsequently restoring it. Channel 1 data, as shown in Fig. 11, represent the connection to Relay 1 and show the restored path delay of 100 µs, as expected for a direct fiber connection. The Maximum Values section at the bottom of the report (only Channel 1 is shown) recorded the approximately 1 ms delay (the relay rounds to the nearest 100 µs) when the WAN A and WAN B data were forced to travel the long way around the ring during the path break, traversing the microwave, the patch fiber segment, and the 95 km fiber segment.

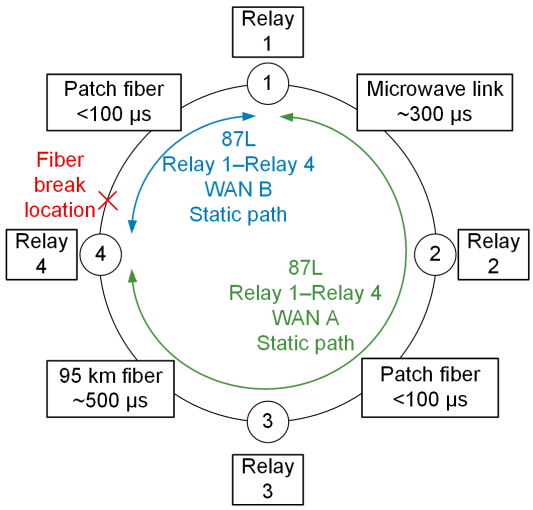

Fig. 10 Utility MPLS Laboratory Test Network for four-terminal line current differential scheme using PRP.

```
87L APPLICATION STATUS
                    4E - Four terminals over Ethernet
                    MASTER

MEDIUM/PROTOCOL     Configuration                 Status
Ethernet Port A     1000BASE-SX, PRP              In use
Ethernet Port B     1000BASE-LX, PRP              In use
Synchronization     External-time-based           High precision

TIME SOURCE         Local Status                  Remote Status
                    Locked                        Locked

CHANNEL ADDRESSING
Local Address       01-30-a7-05-01-04
Remote Address 1    01-30-a7-05-01-01
Remote Address 2    01-30-a7-05-01-02
Remote Address 3    01-30-a7-05-01-03
VLAN Tag            100

STATISTICS          Channel 1       Channel 2       Channel 3
Channel Status      OK              OK              OK
Channel Role        In use          In use          In use
Receive Status      OK              OK              OK
Synch Config        Ext-time-based  Ext-time-based  Ext-time-based
Synch Status        Ext-time-based  Ext-time-based  Ext-time-based
Synch Accuracy      High precision  High precision  High precision
Time Status         Locked          Locked          Locked
High Lost Packet Count --           --              --
Receive Delay (ms)    0.1             0.4             0.5
Lost Packet Count 40s  0              0               0
Lost Packet Count 24hr 4              0               0

MAXIMUM VALUES
Channel 1                       Date and Time (UTC)
Lost Packet Count 24hr 4        03/06/2026 23:23:55
Receive Delay (ms)     1.0      03/06/2026 23:24:23.922
```

Fig. 11 Line current differential performance with MPLS autoconfigured (loose) PRP paths, as reported by Relay 4.

The second test was a repeat of the first test but with manually defined paths (“static” paths) for each WAN. For each path, WAN A sends traffic clockwise around the network, from the lower node to higher node (e.g., Relay 1 to Relay 4 LAN A traffic traverses Nodes 2 and 3 clockwise around the network),

while the WAN B path traverses counterclockwise around the network, from the lower node to the higher node, as indicated in Fig. 10. The results from this test, as recorded by Relay 4, were identical to the line current differential communications report in Fig. 11, except there were no lost packets, proving hitless performance during path disruption for WANs with manually defined, static paths. In this case, Relay 4 was using data from WAN B path, since it arrived fastest, but when the fiber break occurred, it forced the relay to start using the WAN A data, the long path.

A key takeaway from the utility MPLS testing is that uninterrupted line current differential protection is possible during a channel loss event, but it comes at the cost of manual traffic engineering of diverse WAN paths for every necessary line current differential communications link. For the 4-terminal system described here, that means 12 separate paths (i.e., 6 unique conversations that are doubled due to the PRP WAN A and WAN B traffic) need to be manually set, and a given path needs to be updated anytime a network layout change impacts its route.

VIII. Conclusion

This paper demonstrates that PRP, when applied across two independent WANs, provides secure, dependable, and hitless communications for line current differential protection. By leveraging diverse WAN technologies, such as direct fiber optics, MPLS, and VSN, utilities can meet availability requirements necessary for dependable differential protection.

Laboratory testing confirms that PRP can deliver truly uninterrupted operation during a single-WAN failure, provided the delay difference between the two network paths remains within the processing and algorithm thresholds of the relay. When this condition is satisfied, the relay continues to receive sequential line current differential data, ensuring continuous protection dependability. Additional tests further confirm that exceeding the allowable delay difference can result in small numbers of dropped packets and prove the need for engineering path delays according to the relay design.

Additional tests were conducted on a utility MPLS network, demonstrating that hitless performance is also achievable when two static, manually engineered MPLS paths are used. Although this approach increases configuration effort, it enables utilities with a single MPLS network to realize the required performance.

These results validate PRP as a practical method for enhancing the reliability of packet-based WANs used in line current differential schemes, even in the presence of variable WAN technologies and path conditions. As utilities continue to transition from deterministic TDM systems to modern Ethernet-based networks, PRP offers the ability to maintain the high standards of delay and dependability required by line current differential protection.

IX. References

[1] *SEL-411L Advanced Line Differential Protection, Automation, and Control System Instruction Manual*. Available: selinc.com.

[2] E. Chen, B. Smyth, M. Rensburg, and M. Rajasekaran, "It's About Time—Considerations and Requirements for DSS and Line Current Differential Applications," proceedings of the 76th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, May 2023.

[3] IEEE Std 1646-2004, *IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.*

[4] IEC TR 61850, *Communication Networks and Systems for Power Utility Automation* – Part 90-12: Wide Area Network Engineering Guidelines, 2020.

[5] P. Robertson, K. Fodero, and C. Gray, "Solving the Inherent Problem of Transporting Serial Teleprotection Circuits Over MPLS," proceedings of South East Asia Protection, Automation and Control Conference, Sydney, Australia, March 2019.

[6] M. Nguyen, "MPLS TE-FRR cannot recovery in less than 50 ms," Cisco Community, September 2011. Available: https://community.cisco.com/t5/mpls/mpls-te-frr-cannot-recovery-in-less-than-50mms/td-p/1766518.

[7] L. Thoma, "Best Practices for Implementing PTP in the Power Industry," 2018. Available: selinc.com.

[8] Cisco Systems, Inc., "Parallel Redundancy Protocol," Cisco IE3500 Series Switch Software Configuration Guide, Cisco IOS XE 17.18, 2025. Available: https://www.cisco.com/c/en/us/td/docs/IIOT/switches/ie35xx/sw-config-guide/17-17/b_ie3500_1717-cg/m-prp.pdf.

X. Biographies

Brian Smyth received a BSEE and MSEE from Montana Tech at the University of Montana in 2006 and 2008, respectively. He joined Montana Tech as a visiting professor in 2008 and taught classes in electrical circuits, electric machinery, instrumentation and controls, and power system analysis. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2009 and is currently a principal engineer in the transmission group. Brian joined Montana in 2014 as an adjunct professor, where he teaches a course in power system protection in addition to working for SEL. He received the Montana Tech Alumni Recognition Award in 2015 in recognition of his professional accomplishments and the IEEE Engineer of the Year for Montana Society of Engineers in 2017. He is a Senior IEEE member and a registered professional engineer in the state of Washington.

Motaz Elshafi is a senior application engineer in the communications group at Schweitzer Engineering Laboratories, Inc. (SEL). His job is to make electric power safer, more reliable, and more economical. He majored in computer engineering and received both his Bachelor of Science and Master of Science degrees from North Carolina State University. He has held various technical positions in telecommunications since 2000.

Kale McCarthy received his Bachelor of Science degree in Electrical Engineering with highest honors from Montana Technological University in 2023. He joined Schweitzer Engineering Laboratories, Inc. (SEL) as an intern in 2022 and was then hired as a product engineer in 2023 in the transmission department. In addition to working at SEL, Kale joined Montana Tech in 2025 as an adjunct professor, where he teaches courses in power system protection. He is an active IEEE member.

Douglas Taylor received his BSEE and MSEE degrees from the University of Idaho in 2007 and 2009, respectively. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2009 and worked as a protection engineer and a research engineer in the Research and Development division. In 2019, Doug joined the system protection group at Avista Utilities and served as principal protection engineer. Doug rejoined SEL in 2024 and is currently a principal engineer. He is a registered professional engineer in the state of Washington, is a member of IEEE, and was formerly a member of the Western Protective Relay Conference (WPRC) planning committee. Doug was selected to participate in the National Academy of Engineering (NAE) 24th Annual U.S. Frontiers of Engineering Symposium. Doug's main interests are power system protection and power system analysis. He holds 4 patents and has coauthored over 20 technical papers in power system protection.

20260320 • TP7248-01