Western Protective Relay Conference 2024

Teleprotection with MPLS Ethernet Communications - Testing and Experience with Practical Installations

Dan Dietmeyer, Kawika Lawlor, San Diego Gas & Electric Company®
Kourosh Allameh, West Power Energy for San Diego Gas & Electric Company®
Eric A. Udren, *Quanta Technology, LLC*
Ken Fodero and Kamal Garg, *Schweitzer Engineering Laboratories, Inc.*

Introduction

As information technology (IT) advancement drives utility operational data communications towards Ethernet networking, protective relay engineers find that their telecommunications or IT departments are transitioning from legacy teleprotection channels like utility-owned TDM SONET multiplexers and rings or leased paths to Ethernet packet-based wide-area networks (WANs) based on Multiprotocol Label Switching (MPLS) routing technology.

SDG&E® began its migration to Ethernet MPLS communications for mission-critical operational uses in 2016 with the goal of incorporating teleprotection, SCADA, and time-synchronized measurement transport on a common IT-OT Ethernet network. SDG&E has many transmission circuits with line current differential (87L) teleprotection, which had utilized a private SONET multiplexer array. SDG&E worked with multiple teams of technical experts to test MPLS Ethernet based communications for 87L and directional comparison teleprotection in their laboratory environment, with focus on meeting the channel performance demands of 87L. They presented the development and testing program in a 2017 WPRC paper[1].

Packet routing in an Ethernet WAN is less predictable than the deterministic march of data bits in TDM or serial data transmission. MPLS network latency or time delay variations raise concerns for protective relaying applications. Line current differential protection (87L) is the variant of teleprotection with the most stringent real-time communications requirements between line terminals - low delay, low asymmetry between delays in the two directions of packet exchange, and low jitter of latency. High latency slows tripping; asymmetry and jitter reduce 87L security margin and cause risk of misoperation.

In 2024 SDG&E has transitioned the bulk of its transmission lines with 87L teleprotection to its growing private MPLS Ethernet operational WAN. This paper summarizes and builds on the previous WPRC presentation with practical experience on availability and performance of MPLS teleprotection channels. We discuss MPLS network design and configuration considerations as tested, along with field deployment and operating experience.

Utility industry transition to Ethernet IT for OT

A typical electric utility substation contains a diverse range of applications and services that rely on data communications. These services include:

- Substation Control
    - Local and remote substation control
    - Supervisory control and data acquisition (SCADA) management
- Substation data analysis (event reports)
- Real-time protection and automation
    - IEC 61850 Generic Object-Oriented Substation Events (GOOSE) and Sampled Values (SV) messaging services
    - Teleprotection
- Metering and power quality monitoring
- Security
    - Video Surveillance
    - Proximity Alarms
    - Access Control
- Voice communications
- Corporate LAN access

These applications can be categorized into two classes:

1. Operational Technology (OT) services
    a. Real-time data for teleprotection and automation.
    b. Non-real-time data including substation control and data analysis, metering, power quality monitoring, and security.
2. IT services – email, corporate and business applications access, voice communications.

This paper focuses on teleprotection performance. However, it is important to note that a wide area communications network is simultaneously transporting many of the non-real-time operational data services listed above.

There is a clear trend within the industry to move towards Ethernet MPLS for all these applications and services, with the goal of reducing capital costs, standardizing common interfaces to simplify network design, and leveraging the broad advances of IT communications technology and equipment.

Transport technology evolution

The prior paper on this topic [1] gave detailed background on legacy SONET TDM communications systems, the predominant power utility WAN technology for decades and still in use for many of these OT services. TDM synchronously interleaves multiple data streams over the same physical medium, giving each data stream a predefined, fixed length time slot for utilizing the physical connection. All data streams are allocated unique subchannel time slots on the physical channel. Teleprotection communications interface designs evolved to take advantage of the available synchronous TDM interfaces (EIA-422, C37.94, and G.703) and the performance they offered - lower latency and better availability as compared to prior art analog transport systems.

The most common and lowest-order subchannel allocation in TDM networks is referred to as Digital Signal 0 (DS-0) and represents a stream of 64 kbps. Historically, DS-0 channels stem from carrying digitized voice over a network subchannel. In traditional telephony, the audio signal is digitized at an 8 kHz sampling rate using 8-bit pulse-code modulation, resulting in a data rate of 64 kbps. This is why most synchronous teleprotection devices we see today operate at 64 kbps.

The advantage of sending data synchronously versus asynchronously is that data packets from the teleprotection relay can be synchronized to the multiplexer of the communications network. Bytes of data are thus streamed continuously without gaps. Asynchronous serial data transmission relies on start and stop bits to identify the beginning and the end of each byte of data, adding to channel latency.

SONET multiplexers interleave or multiplex multiple DS-0 channels into a higher order or transport level. One popular SONET line rate over backbone network fibers, OC-48 (2.488 Gb/s), can transport up to 32,256 of these DS-0 circuits.

Transition to Ethernet Packets and MPLS

Ethernet with Internet Protocol (IP) has become a convergence protocol for many applications over the past 10 years, supporting an ever-increasing range of OT and IT services. Ethernet with IP supports the creation and cessation of connections and sessions among connected devices, widely used for IT applications. For time-critical OT services, Ethernet packets can be individually routed across the network via a continuously maintained end-to-end connection between applications for minimum delay and more efficient utilization of bandwidth.

Ethernet has evolved to support virtual local-area networks (VLANs), class of service (CoS) or quality of service (QoS) prioritization management, and circuit emulation services (CES) to carry the legacy voice and data circuits still in use today for teleprotection and SCADA. These packet properties also help wide-area network (WAN) switches and routers to sort through the body of packet traffic at each point, giving priority and isolation to the most critical or demanding applications like teleprotection.

There has been a growing debate over the relative merits of packet-based systems versus TDM-based systems as more and more services and applications migrate toward Ethernet. The debate is particularly strong in the power utility industry due to the predominance of TDM systems, notably for mission-critical services like teleprotection, SCADA, and synchrophasor transport. The introduction of carrier Ethernet and of multiprotocol label switching (MPLS) packet-routing technology has added a new dimension to the packet-versus-TDM debate.

Both Carrier Ethernet and MPLS offer improved performance over standard Ethernet by providing operations, administration, and management/maintenance (OAM) mechanisms to enable specific routes or engineered paths for teleprotection services through the network. These routes can emulate the point-to-point connections provided natively with SONET/TDM based systems.

If an Ethernet path fails in an MPLS-based WAN having redundant or alternate path choices, path switching times may typically be as long as 150 ms. MPLS cannot achieve the 5 to 10 ms switching times of purpose-built SONET and TDM systems widely used by utilities carrying teleprotection circuits for decades. To achieve these failover switching speeds we have developed a new solution based on having a live backup circuit on hand at all times and letting the protective relay execute the failure detection and switchover as illustrated in a section below. This solution leverages the high total bandwidth of the MPLS WAN which can support a live backup channel in operation at all times to be available instantly when needed.

With widespread use, increasing performance, decreasing costs, growing availability of compatible applications, and ability to consolidate all OT traffic on one network – MPLS Ethernet is becoming the communications interface of choice. This maximizes the value of the capital investment in the Ethernet networking and eliminates the need for an array of varied communications systems for specific operational uses.

Line current differential (87L) protection relays are only now beginning to adopt MPLS Ethernet as a communications protocol. The relays have been designed over the years to take full advantage of the performance attributes of TDM networks. While current Ethernet MPLS networks provide circuit emulation services (CES) to carry TDM based traffic, the overall performance of these circuits do not exactly match the perfectly deterministic performance of SONET based systems.

Line current differential relays initially used channel-based timing to measure channel latency. In a ping-pong exchange, a pair of relays determined the round trip channel time and divided by 2. In an MPLS Ethernet network, the times in the two directions may be asymmetric, yet the relay algorithms assume symmetry. Milliseconds of asymmetry can seriously erode the security margin of an 87L relay.

Most modern line current differential relays offer time-based channel delay measurements, with reference IRIG-B or GPS time used at each end, as an alternative to channel based timing. Time based measurements can report channel asymmetry as well as delay or latency in each direction.

MPLS Ethernet routers encapsulate TDM services such as DS1 or DS0 synchronous 64 kb/s data for transport with an emulation (pseudowire) circuit implemented in an interface module. Protection circuits are typically carried using TDM over IP (TDMoIP) encapsulation. TDMoIP is best suited for encapsulation of channelized DS1 traffic. This allows for DS0 or 64 kbps channels. Structure Agnostic Transport over Packet (SAToP) is another standard intended for bulk transfer of the DS1 traffic. These methods work well for traditional telephony but may fall short of efficiently providing the stable low latency performance required for teleprotection over Ethernet.

The most recent MPLS routers include special design features like jitter buffers which accumulate packets whose timing has some randomness to deliver them with precise output timing, at the expense of additional latency. In modern routers operating on typical networks, the jitter of packet arrivals is low enough for stabilization via jitter buffering of just a millisecond or two, so that overall path latency can be 2-5 ms and well suited for 87L teleprotection.

An alternative to pseudowire emulation that can provide SONET/TDM performance over Ethernet networks is Virtual Synchronous Network (VSN) technology. VSN provides synchronous circuit connectivity with SONET-like channel delay performance over MPLS networks while controlling circuit asymmetry and delivering comprehensive performance monitoring and reporting. VSN can manage teleprotection services separately from the core management of MPLS Ethernet services.

Relaying over MPLS Ethernet

Although MPLS Ethernet networks have been in use for many years in the telecom industry, power utilities are in the early days of running TDM based teleprotection services over them.

Hardware technology refresh rates for telecom networks are at least 4 times those of teleprotection devices. Application of legacy teleprotection to the next generation of telecom technology has historically presented challenges. Some examples include leased analog services to private analog microwave, analog microwave to digital microwave, and now TDM to packet networks. We have learned in the past that the noise detection and security methods to prevent misoperations need to be adjusted to better match the characteristics of the new technology. This is much simpler with modern digital teleprotection systems in use today but there are always lessons learned.

	Current differential			Directional comparison		
	Latency (ms)	Asymmetry (ms)	Failover (ms)	Latency (ms)	Asymmetry (ms)	Failover (ms)
Critical or EHV	5	0.5	5	5	5	5
High voltage	10	1	10	10	10	10
Subtransmission	15	1	50	15	10	50

Table 1 – Requirements for current differential versus directional comparison relaying from [2]

SDG&E teleprotection schemes

SDG&E line teleprotection schemes are primarily based on a redundant array of relays performing line current differential protection (87L) and on directional comparison permissive overreaching transfer trip (POTT) protection (21L).

- The most frequently used configurations include one line current differential (87L) relay pair and one POTT (21L) relay pair.

- The 87L relay pair uses a dark or dedicated optical fiber pair when available as the primary teleprotection channel.
- For 500 kV line protection, a second redundant 87L relay pair operates over dark fiber if available.
- If no dark fiber pair is available, the two 87L relay pairs cross-connect to the two MPLS Ethernet router pairs via channel 1 and 2 (or X and Y) outputs as shown in Figure 3 below.
- Separately from the 87L relay path, the redundant 21L relay pair uses C37.94 serial data via MPLS.

Table 1 above shows how the tolerance for circuit latency and channel asymmetry are very different for 87L versus 21L.

Latency requirements

There are many IEEE and IEC standards and reports that specify channel latency requirements for teleprotection networks. Ultimately it is up to the relay protection engineer to determine if a specific latency value is acceptable for the safe, secure, and stable performance of the protected line and power system. The determination is based on critical fault clearing (CFC) times for the worst faults from planning studies, on coordination with adjacent circuits, or on acceptable risk of damage from increased fault duration. Latency is added to relay response time and breaker current interrupting time; the latter is often longer than the protection operation time.

Historically, latency performance has improved over time from 12-15 ms for the analog systems of the early 1980s to 2-5ms for the digital systems of the late 1990's. Figure 1 is excerpted from the IEEE PES Technical Report TR-76 [2] which considers different latency and asymmetry values based on 60 Hz Critical, High Voltage and Sub transmission systems. Critical would be for protection systems on lines with low CFC times whose delayed tripping could lead to loss of system stability, or for locations with high fault current levels that could result in equipment damage or advanced aging.

Current differential 87L protection demands substantially better performance than directional comparison protection, especially for asymmetry where large values that might have minimal impact on DC schemes like POTT can lead to misoperation of 87L. However, 87L is growing massively in popularity due to its sensitivity and security that promise reliable protection as the grid transforms to high penetration of DER, stressed operations, and new configurations of protection zones. Directional comparison schemes that have been popular for standard applications may be challenged to operate or restrain as they should, and present setting maintenance challenges that 87L eliminate. Accordingly, the industry objective is to meet communications performance requirements for 87L.

MPLS Ethernet router impacts

Frequently observed raw transport times for packets between MPLS Ethernet routers in separated substations can be 1-2 ms. However, variation or jitter of transport times from packet to packet introduce random comparison delays that may exceed 1-2 ms and acceptable thresholds for timing errors in 87L schemes. Two elements are addressed eliminate this problem:

- Network application: Router settings for QoS that impact priority, and for assignment of dedicated bandwidth, and for behavior for transport layer problems must be configured to minimize and stabilize packet delays as much as possible – should be under 2 ms variation in a solid application.
- Router feature: MPLS routers intended for teleprotection should include a jitter buffer which accumulates packets for a given teleprotection scheme and issues them with timed stability to a serial interface module, so the relay sees a fixed and stable channel delay. If a particular path suffers more severe jitter, the jitter buffer must be set for greater depth to absorb these variations. The jitter buffer depth adds to the path latency and slows down protection by a corresponding number of milliseconds.

<u>SDG&E Requirements</u>

The internally and externally driven requirements developed by the System Protection, Automation and Control Engineering (SPACE) department went beyond technical performance requirements for the communications channels, and included requirements for design, OT services supported, expandability, maintainability, incident response, and reporting requirements. The main performance requirements for teleprotection circuits based on both internal and external business drivers are:

1. High availability: 99.95% or better, based on WECC 500 kV teleprotection channel requirements. The network availability cannot be determined in a lab environment and will be evaluated during the field trial period. Unavailability can either be due to solid path downtime or to intermittent packet delivery – these have different causes and remediations and should be tracked separately.
2. Low latency: to be as good as or better than existing latency for these circuits. The existing SONET links in the SDG&E network provide 5 ms one-way latency on average. It was agreed between IT network deployment team and SPACE to use 5 ms or better as the criterion for laboratory testing and network configuration of the MPLS circuits used for the field test relays.
3. Low asymmetry: the asymmetry limit was set at first to less than 2 ms, based on recommendations from the manufacturers of the current differential (87L) relays to be deployed. For field test relay commissioning, a benchmark of less than 0.5 ms is used since MPLS routers have proven to be capable of this low asymmetry; anything higher indicates misconfiguration of the network communications channel.
4. Fail-over time: less than 3 ms, to reflect the performance of existing SONET substation multiplexers. This could not be achieved with MPLS routers connected to relays in the same way as was the case for SONET multiplexers; the MPLS failover times approached 150 ms. However, by using redundant communications channels in the relays themselves,

channel change-over for the teleprotection is still achieved in less than 3 ms by the relay switching to its redundant fixed-route channel that is already operating over an independent path. This relay channel redundancy is enabled by having more bandwidth and more channels available with MPLS. System A relays have redundant teleprotection paths over System B routers and network paths, and vice versa. The connection scheme is shown in the Testing Overview below. The overall design has more redundancy and robustness than a System A and System B relay pair using separate channels in a SONET network.

Lab Testing Overview

The SDG&E performance objectives as listed in the last section for the new MPLS communications system were evaluated in the company's Integrated Testing Facility (ITF) lab using a real-time digital simulator (RTDS®) for a transmission grid section. An RTDS model was developed for a section of the 500, 230, 138, and 69 kV transmission systems; the reduced system model was validated against reference short circuit models of SDG&E's transmission system. The reduced model can fit into an RTDS rack of processing units. Figure 1 shows an example model of the SDG&E transmission network.

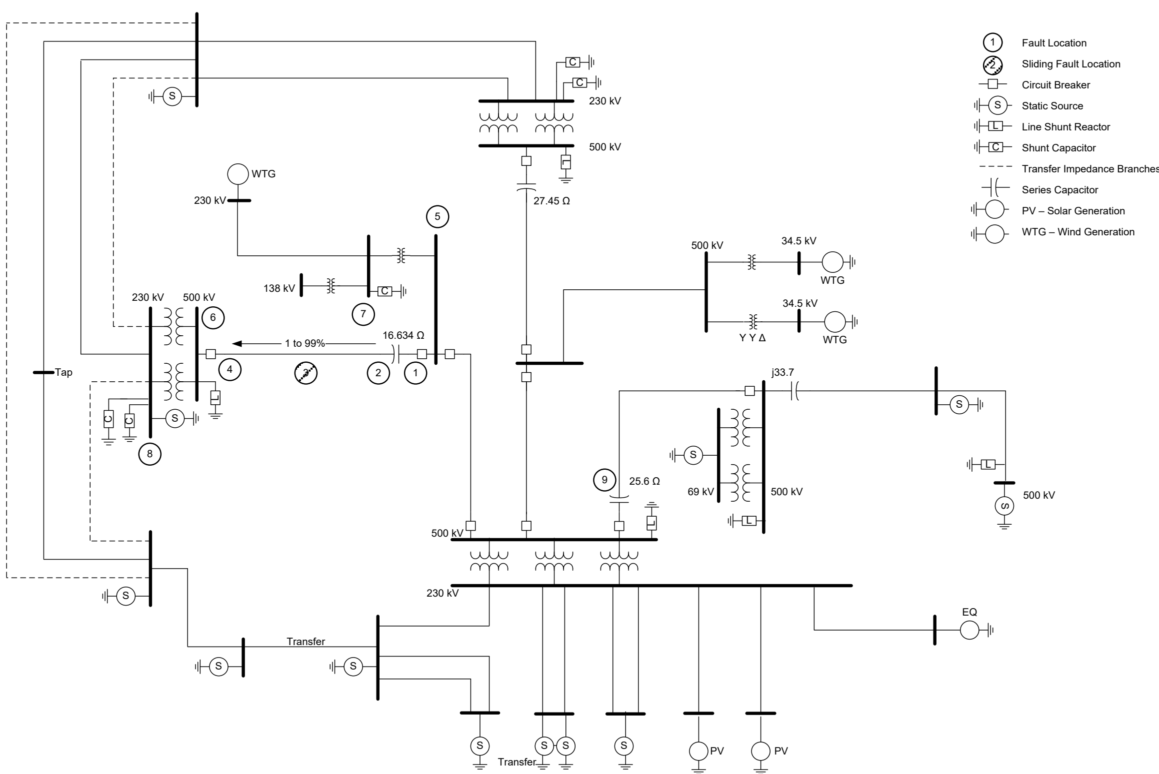


Figure 1 - RTDS Model of SDG&E Transmission Line Network

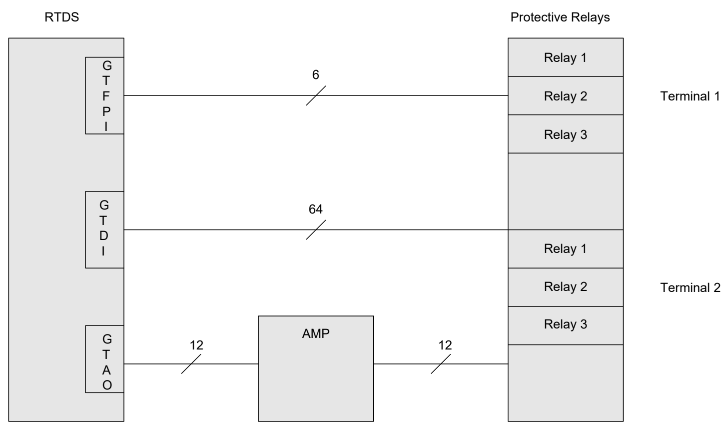


Figure 2 - RTDS test connections

Figure 2 shows the test setup for the RTDS and the protective relays. SDG&E uses three redundant protective relay systems of different models or manufacturers for protection of 500 kV transmission lines. Two of the relays have both 87L line current differential protection and 21L distance element directional comparison protection which is usually a permissive overreaching transfer trip (POTT) scheme. These two relays also include time-step backup distance protection and time delayed overcurrent backup protection. The third relay has 87L protection and time-step backup distance and delayed backup overcurrent protection. SDG&E uses two redundant relay systems for line voltages lower than 500 kV.

The RTDS provides two sets of three phase voltage and current signals (12 analog signals) through an amplifier to the protective relays for a simulated transmission line. The RTDS also provides breaker status outputs (6 digital signals) and receives digital contact output closures (64 digital signals) from the protective relays for trips, permissive signals used in communication based protection schemes, and communication channel status. This configuration of the RTDS and protective relays for each protected transmission line terminal comprise a hardware-in-the-loop (HIL) closed-loop test method in which the relays behave as they actually would when subjected to faults or switching in service. Overall, protection systems for eight different transmission lines were tested in the RTDS lab.

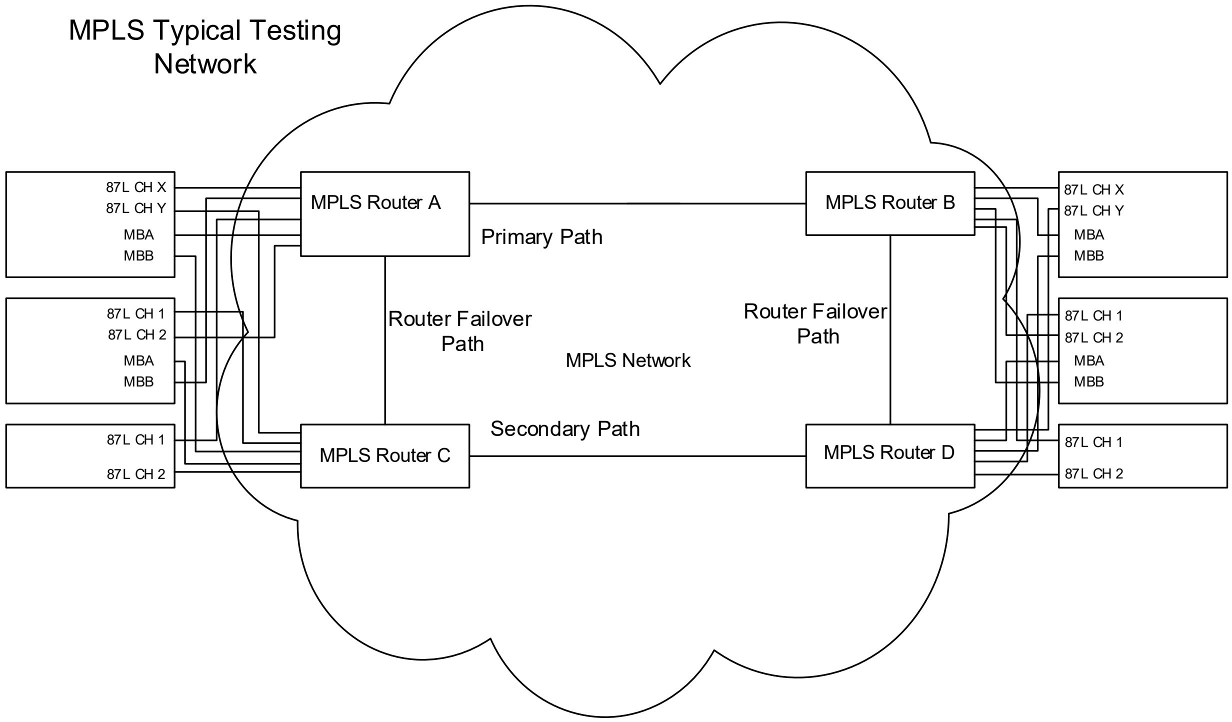


Figure 3 - Protective Relay Communications Test and Field Setup

Figure 3 shows the Ethernet teleprotection communications setup in the RTDS lab for testing. This scheme was used to test performance to specifications along with rapid failover for relay, router, or Ethernet path failures via redundant MPLS routers.

SDG&E Requirement 4 listed in the last section called for a new connection scheme to achieve 3 ms or less failover time for a network problem. The configuration of Figure 4 connects the upper current differential relay pair 87L-X and 87L-Y communications ports through separate isolated redundant router paths, each in continuous operation, with no single point of failure for the two paths. Those relays are using the X ports through routers A and B over the primary Ethernet network path but are simultaneously maintaining communications through the Y ports via Routers C and D and the secondary network path. If the upper path or router fails, the relays continue operation using the already-established lower path, with a transition time of under the 3 ms failover time specification. The 35 to 150 ms recovery time of the failed upper Ethernet network path has no impact. In service, the routers have been configured not to fail over to an alternate path at all. The second and third 87L relay pairs with output ports 1 and 2 are connected to interface modules of the redundant MPLS routers in a similar fashion for fast failover. In two of the multifunction 87L relay pairs, the POTT 21L protection function is also enabled and exchanges status bits via two Mirrored Bits ports and redundant connections to the two routers for failover capability of the 21L teleprotection.

The communication paths from the relays through the MPLS network are shown in Table 1.

Relay	Communication Channel	Protection scheme
Relay 1	87L CH X	Primary 87L Line Current Differential Channel (C37.94)
	87L CH Y	Backup 87L Line Current Differential Channel (C37.94)
	MBA	Primary 21L POTT Scheme Channel
	MBB	Backup 21L POTT Scheme Channel
Relay 2	87L CH 1	Primary 87L Line Current Differential Channel (C37.94)
	87L CH 2	Backup 87L Line Current Differential Channel (C37.94)
	MBA	Primary 21L POTT Scheme Channel
	MBB	Backup 21L POTT Scheme Channel
Relay 3	87L CH 1	Primary 87L Line Current Differential Channel (C37.94)
	87L CH 2	Backup 87L Line Current Differential Channel (C37.94)

Table 1 - Teleprotection communications paths

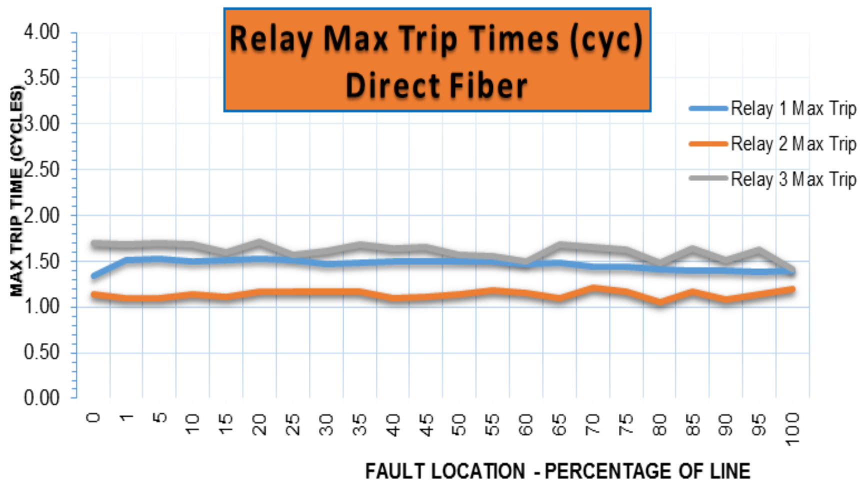
This setup allowed testing for many different router configurations with respect to latency. The test setup in Figure 3 - is for two terminal transmission lines. Three-terminal transmission lines and their protection schemes were also tested.

The latency introduced by the router was controlled by MPLS router settings for Jitter Buffer size and Payload or packet size. Lower latency requires smaller Jitter Buffer and smaller Payload size of Ethernet packets which is inversely proportional to the required bandwidth of the communications channel. Conversely, larger Jitter Buffer setting and Payload size of Ethernet packets results in higher latency and lower bandwidth requirement for the communications channel.

Overall, performance specifications are easily met with no single points of failure in protection or communications.

Latency test results

Figure 4 shows example trip times for the relay schemes tested. The top graph shows maximum trip times for the relays connected back-to-back with direct fiber. The bottom graph shows the same batch test, recording maximum trip times over MPLS. The results show that the relay settings provide practically constant operating times for internal faults, and that the MPLS channel is not introducing trip speed variations.



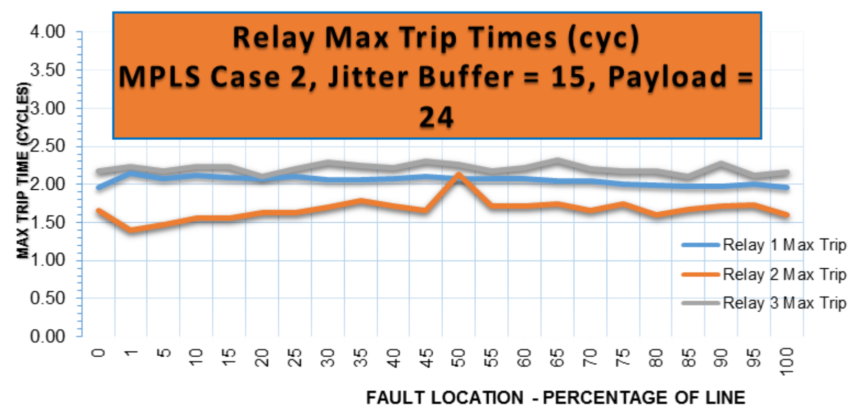


Figure 4 - Trip times back-to-back (top) and over MPLS communications (bottom)

Failover test results

Figure 5 shows the setup for testing of failover from primary to backup communications channel. The primary channel was broken via a fiber optic switch controlled by the RTDS simulation.

The MPLS router failover times ranged from 35 to 50 ms, faster than expected but much slower than the SDG&E failover specification of 3 ms. However, two of the three protective relays could switch from the primary 87L primary channel on the X port to the secondary path via the Y port within 2 ms, faster than the specification. One protective relay's failover time between channel ports was closer to 50 ms – users who adopt this failover scheme should validate that their specific relay types can fail over quickly from one port to the other.

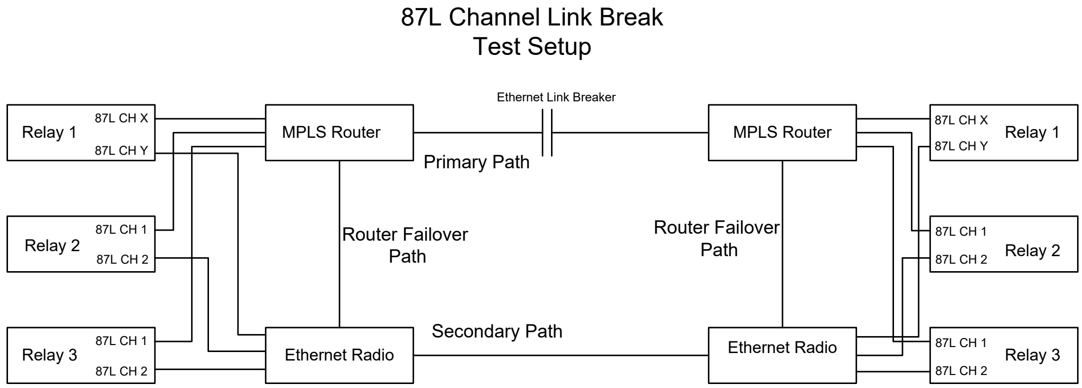


Figure 5 - Communications Channel Failover Test Setup

Asymmetry test results

Figure 6 shows the setup for testing the asymmetry tolerance of the protection system. Asymmetry was introduced by creating delay in the communications channel in one direction only.

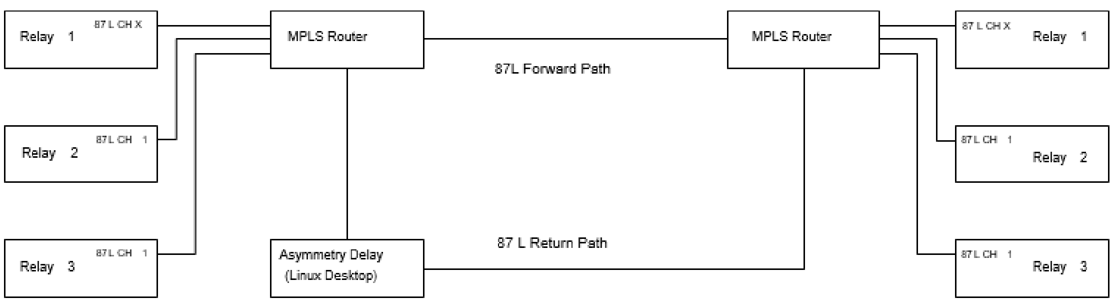


Figure 6 - Asymmetry Test Setup

External fault tests confirmed that relays were secure for asymmetry of up to 2 ms. However, even though we could not demonstrate misoperations, security margin is unavoidably degraded by asymmetry. Field installations are commissioned with 0.5 ms or less asymmetry and achieving this with the selected MPLS routers has not presented problems.

It should be noted that some of the tested 87L relays can use GPS time-based synchronization, which has much higher asymmetry tolerance since measured one-way channel delays are used for compensation. However, SDG&E's standard for field installations is to use channel based synchronization which places high emphasis on channel asymmetry within specifications.

For a few problematic leased data circuits, SDG&E is testing differential protection via the relay Ethernet port with GPS time synchronization to deal with high latency and asymmetry.

Protection performance testing

The project team applied thousands of internal and external faults on or near line models in RTDS and evaluated relay responses via hardware-in-the-loop testing. The operating time results presented just above serve as an example of observed relay performance for internal faults, which was fully as reliable as for direct fiber but with about half a power cycle slower tripping than with direct fiber channel. The direct fiber is faster than would be observed with a DS0 SONET channel, and the difference between DS0 and MPLS Ethernet is under 5 ms and accepted as compliant with SDG&E specifications.

With the MPLS routers configured for compliance with SDG&E specifications, fault protection reliability and security were flawless and equivalent to performance with a fiber connection, except for the additional milliseconds of fault tripping time.

Substation deployment design

For transmission voltages of 230 kV and below, SDG&E generally uses two redundant teleprotection schemes with current differential 87L and POTT 21L, and two redundant channels. For 500 kV substations, teleprotection comprises two redundant 87L relay pairs and a third 21L-only pair with redundant communications paths. We described the major communications use choices under Table 1 above. Dark fibers are the preferred teleprotection channel choice where they are available.

MPLS Ethernet paths are configured in the routers as fixed with no failover action. Most of these paths are fibers; a few are microwave links. If a path fails, the relays transfer to utilize the alternate MPLS path with only milliseconds of delay. MPLS channel integrity is monitored and alarmed by the relays as well as by the SDG&E Network Operations Center (NOC). Operators may manually dispatch and observe an alternate MPLS path before it is engaged for relay use.

A close collaboration is required between the communication designer and the protection engineer to make sure the line relays are compatible with the router cards to which they are connected. This results in a communication block diagram showing relay ports, router ports and the transport devices (fibers, microwave, leased circuits etc.) from end to end.

The MPLS network has been specified and tested for SCADA and for synchrophasor transport, as well as for teleprotection. SDG&E has developed a firewall based secure Ethernet networking design for externally routable communications (ERC). In substations that have been upgraded to Ethernet ERC for operational data, relays are able to communicate operational data types, such SCADA, synchrophasors, and oscillographic and event records, via Ethernet ports on the relays which are separate from the C37.94 ports used for teleprotection. Some of these data types can be transported via the MPLS network that serves teleprotection – routers are configured with Ethernet interfaces and dedicated service allocations for transport of these services.

System deployment to date

The MPLS Ethernet teleprotection design as described and tested above has been successfully implemented in production installations from 2017 through 2024. To date SDG&E has commissioned MPLS teleprotection communications on 99 transmission lines and for 8 remedial action (RAS) or interconnection protection schemes as part of its telecommunications reliability improvement (TCRI) program. TCRI now encompasses most of the bulk electric system tie line communications networks for secondary protective relay communication paths, with direct fiber primary paths in continuing use. MPLS networks provide system operators the ability to discern in real time if protective relaying availability is suffering a sustained communications outage or degraded communications performance, and this leads to rapid problem resolution. Sustained outages can be observed through network monitoring tools so that troubleshooters are dispatched to investigate, repair, and restore the communication circuits. Degraded performance observed on MPLS networks via monitoring tools can be remedied by rerouting network traffic through alternate paths of acceptable latency, asymmetry, and uptime while affected assets are restarted or removed and replaced. Communications failures are effectively handled at the protective relay level, where communication ports have been observed to fail over between two live paths in 2 ms or less, as compared to MPLS network failover times of 35 to 150 ms. The preferred combination remains a direct fiber communication channel backed up by an MPLS Ethernet communications circuit.

It is essential for IT techs to test line communication paths prior to the MPLS migration day, making sure communication parameters are within the prescribed quality levels. During the migration window, the relay tech prepares two communication reports. The first with existing TDM communication (As Found) and the second after the new MPLS path is connected (As Left). These two reports provide a good migration parameter comparison and serve as a basis for future MPLS quality monitoring.

The procedure utilized by SDG&E for migration of a transmission line to new teleprotection communications includes the following steps:

1. Take the initial "As Found" (AF) communications report on existing communications circuits - typically connections to SONET multiplexers.
2. Disconnect communications from isolated relays, test relay functions, and adjust or validate settings.
3. Connect new communications to the relays.
4. Test teleprotection transmit and receive data functions.
5. Take the final "As Left" (AL) communications report as the last action.

Communications reports (comm reports) obtained by field personnel from the protective relays utilizing MPLS communications have yielded interesting results since the deployment program began in 2017. It has been proven that over time the MPLS network has achieved all four of the main business requirements (latency, asymmetry, failover time, availability) with only rare problems to fix.

```
=>COM 87L
87L APPLICATION STATUS
                       2SS - Two terminals with single serial channel
                       MASTER

MEDIUM/PROTOCOL        Configuration                     Status
Serial Channel 2       850nm C37.94 Fiber                OK
Synchronization        Channel-based                     High precision

CHANNEL ADDRESSING
Local Address          2
Remote Address 2       1

STATISTICS             Channel 2
Channel Status         OK
Channel Role           In use
Receive Status         OK
Synch Config           Channel-based
Synch Status           Channel-based
Synch Accuracy         High precision
Time Status            --
High Lost Packet Count OK
High Latency           OK
High Asymmetry         --
Round-Trip Delay (ms)    6.0
Transmit Delay (ms)    --
Receive Delay (ms)     --
Asymmetry (ms)         --
Lost Packet Count 40s  0
Lost Packet Count 24hr 1781146

MAXIMUM VALUES
Channel 2                          Date and Time (UTC)
Lost Packet Count 24hr 17488218    10/29/2020 03:30:00
Round-Trip Delay (ms)    6.0       05/01/2024 19:17:12.828
Transmit Delay (ms)      0.0       04/04/2020 14:16:22.604
Receive Delay (ms)       0.0       04/04/2020 14:16:22.604
Asymmetry (ms)           0.00      04/04/2020 14:16:22.604

HISTOGRAMS
Channel Round-Trip Delay (last 24 hours)
Delay (ms)             Channel 2 (%)
0 - 2                    0.0
2 - 4                    0.0
4 - 6                   97.2
6 - 8                    2.8
8 - 10                   0.0
10 - 12                  0.0
12 - 15                  0.0
15 - 20                  0.0
20 - 30                  0.0
30+                      0.0

Channel Asymmetry (last 24 hours)
Asymm (ms)             Channel 2 (%)
0.00 - 0.25              0.00
0.25 - 0.50              0.00
0.50 - 0.75              0.00
0.75 - 1.00              0.00
1.00 - 1.50              0.00
1.50 - 2.00              0.00
2.00 - 3.00              0.00
3.00 - 4.00              0.00
4.00 - 5.00              0.00
5.00+                    0.00
```

Figure 7 – 69 kV MPLS Migration Comm Report Excerpt

Figure 7 shows the output of a comm report from an active MPLS circuit within the SDG&E service territory observed in 2024 – it shows real-time evidence of a highly available, low latency, minimally asymmetric MPLS communications path. These standardized comm reports lend themselves to easy search for performance outliers, can be archived in databases for overall statistical averaging, and can provide real-time insight into the performance of the MPLS circuit.

Operating experience

In-service availability has greatly exceeded the WECC 99.95% specification. Random failures of MPLS teleprotection paths have been virtually nonexistent. Here we describe the causes of channel failures which are not associated with basic MPLS or fiber Ethernet network functioning.

There have been a handful of path failures due to microwave path disturbances, including RF noise and earthquakes; and mitigations actions were taken.

MPLS routers initially used were IT products that are found in data centers; these routers are powerful and fast computing platforms which consume hundreds of watts of dc auxiliary power in a 3 R.U. enclosure. They were checked for compliance with IEEE 1613 [3] except that they could not handle the specified temperature range without open enclosures and cooling fans. This led to problems with the dusty environment of utility substation control buildings. Routers suffered premature failures due to dust contamination on the printed circuit boards, fan failures, and moisture or water ingress. These failures were mitigated by replacing the original router circuit boards with conformally coated boards. Fan failures were mitigated by modifying fan speed control logic to reduce typical run speeds. For next-generation designs, MPLS router vendors have been asked for a cooling solution with no moving parts. Lastly, future installation designs add HVAC and dust filters to the control room where routers and other P&C equipment are located to reduce heat and dust failures for all computer-based protection and control equipment.

Monitoring of the MPLS network health, reliability, and other statistics are performed by the SDG&E Network Operations Center (NOC). Real-time monitoring as well as cumulative month-end reports of system performance parameters are conducted and distributed to all network team members and associated stakeholders. Aspects of the MPLS network that are tracked and logged in real-time include:

- Device platform and software inventories.
- Software compatibility limitations within routers and respective tools.
- Alerts and vulnerabilities reports from the manufacturers.
- Incident and problem ticket summaries noting network events and potential causes.
- Node outage summaries, uptime, fan status, power status, and temperature.
- Node CPU & memory utilization.
- Node synchronous timing source identification.
- Hardware failures.

Additional useful information that can be extracted from protective relays include Sequence of Event Records (SER) and event reports which include loss of communications channel, high latency, high asymmetry, and noise burst alarms. These records provide insight into protection system performance including proper tripping, trip speeds, and restraint for external or out of zone faults.

Of specific interest to a protection team is the SCADA and teleprotection service list and states of listed items, as well as the incident and trouble ticket logs. These help to identify if an event or operating problem results from external factors or from network issues which protection engineering would learn only from relay alarms or event reports. SDG&E System Protection and Control Engineering (SPACE) department has created a strong partnership with the NOC to ensure the needed QoS (quality of service) and other operating parameters of the MPLS network. Intermittent failures are noted and repetitively observed failures are brought to the attention of network and telecom troubleshooting personnel for root-cause analysis and remediation.

The results obtained from comm reports, event reports, and laboratory testing correlate well and lead to high confidence in the design and deployment of MPLS technology in protective relay communications.

One exception to program success has been the migration to leased non-SDG&E Ethernet circuits where the service provider's Ethernet performance has not complied with SDG&E specifications. There were several protection misoperations due to excessive delay or asymmetry. The current differential relaying function was disabled on these circuits and only POTT via Mirrored Bits communications were used for teleprotection schemes. SDG&E is currently evaluating the application of differential protection via an Ethernet port on the relay instead of C37.94 serial connections to MPLS routers and external time synchronization for these situations.

Ongoing deployment plans

Practical experience shows that once the communication and substation design has been completed (issued for construction), then 3 to 4 lines can be migrated per month with a higher migration count available if multiple teams are working in parallel.

Deployment plans for the MPLS network include a multi-year approach, spanning most of the remainder of the decade through 2029, in converting the remaining transmission lines and substations to this technology. Outliers which include extremely remote sites or customer owned sites, may be among the last to be addressed as they present the greatest challenge to design and commissioning coordination for such technology where the process is less predictable or outside the control of the utility implementing the service. Strong project management, project scoping, design process oversight and QA/QC review, as well as proper budget estimates and forecasting all play a critical role in the overall success of a project that spans multiple disciplines within the organization. As a result, a strong team needs to be retained to ensure the consistency of the technical expertise applied to maintain budget and schedule commitments. With the advent and commissioning of MPLS based communication schemes, historically provisioned Time Division Multiplexed (TDM) circuits are being sunset as new communication circuits come online each month in a march of progression towards full system integration. Recall that to date there are 99 transmission lines and 8 RAS or interconnection protection schemes with protective relaying accomplished in some form (primary, secondary, or both) via MPLS over the company's routable IT network. At the conclusion of this technological migration, it is expected that a total of roughly

246 transmission lines and a handful of other protective relaying communication needs will be utilizing MPLS thus proving the efficacy of the technology and its reliability and usefulness in modernizing protective relaying communications.

Conclusions

SDG&E has transferred teleprotection communications for 87L and POTT schemes to new MPLS Ethernet transport service in accordance with the connection guidelines explained in the Lab Testing Overview section above. 99 transmission lines and 8 RAS have been migrated, with 246 lines and other services to be migrated in total between now and 2029. Protection communications have been vastly more reliable and secure than with legacy SONET network channels. NOC monitoring of the MPLS private network yields in-depth visibility of consistent performance.

The authors paid special attention to design of the connections and configuration of the routers to achieve specified performance for channel latency (under 5 ms), asymmetry (under 2 ms and specified in the field as under 0.5 ms), and channel failover time (under 3 ms) as explained in the paper. Availability could not be tested in the lab, but in-service availability has greatly exceeded the WECC 99.95% specification. Unavailability causes have been physical issues described above that have been mitigated and are not associated with the basic capabilities of MPLS Ethernet routers for teleprotection.

These results cannot be achieved by simply replacing the SONET channel equipment – the entire installation and connection must be redesigned in consideration of MPLS Ethernet router behavior and configuration (especially failover behavior and time) and should be tested in the laboratory to develop a new protective relaying standard design.

The laboratory testing and standard development work we recommend also educates the utility P&C and network engineering teams over time and helps them develop plans for collaboration in managing the performance and reliability of protection operating on the new IT-managed network. Coordinated data gathering from relays by protection analysis teams, and from MPLS network routers by NOC engineers and experts, can be used to achieve new levels of visibility into the performance and malfunctions of the overall protection systems.

MPLS Ethernet routers have been designed until now as computer-room equipment that will perform most reliably in environmentally conditioned control buildings. Router manufacturers who have focused on utility industry needs have been improving the robustness of products including board coating and improved cooling, with more work on passive cooling in progress. Discuss these environmental concerns with prospective router manufacturers.

The ubiquitous deployment of MPLS Ethernet by IT departments for enterprise networks across industry drives attractive economics and impressive performance and capacity of Ethernet for OT network applications like teleprotection, as legacy SONET technology fades and becomes unsupportable. P&C practice must now adapt to this transition. The change brings great performance and capacity improvements for teleprotection and other services, if new P&C designs properly interface to the features and behavior characteristics of MPLS Ethernet.

Acknowledgement

The authors thank Clint Struth and Cory Struth of SCI Networks for contributions to the creation and completion of this paper.

References

1. T. Rahman, J. Moralez, S. Ward, E. Udren, M. Bryson, K. Garg, *Teleprotection with MPLS Ethernet Communications - Development and Testing of Practical Installations*, 44th Annual Western Protective Relay Conference, October 17-19, 2017

2. IEEE Power & Energy Society Technical Report PES-TR-76, *Channel Performance Considerations for Ethernet Circuits Applied to Teleprotection*, Power System Relaying Committee WG H32, September 2020.

3. IEEE Standard 1613-2023, *IEEE Standard for Environmental and Testing Requirements for Devices with Communications Functions used with Electric Power Apparatus*.