Teleprotection with MPLS Ethernet Communications - Development and Testing of Practical Installations

Tariq Rahman and James Moralez, San Diego Gas & Electric Company
Solveig Ward and Eric A. Udren, Quanta Technology, LLC
Michael Bryson and Kamal Garg, Schweitzer Engineering Laboratories, Inc.

Presented at the 44th Annual Western Protective Relay Conference
Spokane, WA
October 17-19, 2017

Introduction

Today's information technology (IT) advancement is driving both non-operational and operational data communications within a substation towards Ethernet-based communications networks. As a result, protective relay engineers are finding that the telecommunications industry is transitioning from legacy teleprotection channels such as leased circuits, Time Division Multiplexed Synchronous Optical NETetworks (TDM SONET) multiplexers and rings, over to Ethernet packet-based wide-area networks (WANs). The current, most common WAN packet routing technology is Multi-Protocol Label Switching (MPLS).

Traditionally, packet based IP routing in an Ethernet WAN has been fundamentally less predictable than the deterministic flow of data bits in a fixed, point to point TDM or serial data communications circuit. Changes in network latency or packet delay variations in the past have raised concerns when considering it for use in protective relaying applications. High latency in any network slows tripping and can result in miscoordination of the protective relay system. Current differential line protection (87L) is particularly sensitive to jitter or variation in latency, in addition to asymmetry or the difference in latencies in the two directions of the protection channel data exchange. To validate the MPLS design and in preparation of migrating substation production relays from TDM to MPLS within the San Diego Gas & Electric (SDG&E) system, laboratory testing was performed at the SDG&E Integrated Test Facility (ITF). The testing conducted included both fundamental network testing and the Real Time Digital Simulation® or RTDS® system model applied to protective relays, using MPLS routers and proposed MPLS network configuration models

This paper describes the technical requirements developed by SDG&E for critical transmission high voltage teleprotection applications, and provides a high level comparison of SONET versus MPLS Ethernet communications. The paper also covers laboratory testing approach, test results of the MPLS proposed solution, and redundancy considerations. This paper also includes impact on protection scheme due to channel asymmetry, latency, failover, channel availability, and tools available for MPLS monitoring the communication link for troubleshooting and analysis.

SDG&E System Overview

San Diego Gas & Electric (SDG&E) provides natural gas and electricity to San Diego County and southern Orange County in southwestern California, United States. SDG&E is a regulated public utility that provides energy service to 3.6 million people through 1.4 million electric meters and 873,000 natural gas meters in a service area that spans 4,100 square miles. The company is a subsidiary of Sempra Energy (NYSE: SRE), a Fortune 500 energy services holding company based in San Diego.

Currently SDG&E uses a TDM network, which consists of direct fiber, multiplexers, microwave radio, lease-line equipment, and channel banks that are the backbone of the existing mission-critical communications system supporting Teleprotection and SCADA

(Supervisory Control And Data Acquisition) services. Much of the current network was implemented based on project driven requirements or regulatory compliance. The TDM network consists of a mix of T1 Multiplexers and higher-order TDM SONET rings. In 2005, the company began investing in connecting all substations by company-owned fiber for SONET rings. The fiber effort will continue and may take approximately 10 more years to achieve the goal of fiber to every substation.

MPLS Ethernet is the current business standard being widely adopted in service-provider networks for cellular back-haul, cable communications, data centers and other business environments. MPLS is also becoming widely accepted and used heavily in other ICS (Industrial Control Systems) environments such as water, Public Safety Networks, land mobile radio backhaul, in addition to other city services. As MPLS is adopted into substation communications (replacing instead of upgrading older technology) it is anticipated that it will deliver significant benefit to overall utility communications with superior monitoring capability, high service availability, and reduction in maintenance costs.

MPLS Drivers

Today's electric utility industry is moving towards a consolidated Ethernet communications network that will provide transport to all business services over a single platform. These multiservice networks are being designed and built to meet all the business and operational needs, including integration of legacy devices. While data requirements for most substations typically do not require high bandwidth, bandwidth requirements are increasing for business services used within a substation, including IP phones, RTUs, security access and video, and synchrophasor data from PMUs.

It should be recognized that teleprotection communications services is one of many services within the substation that a utility network needs to provide. Yet, while teleprotection tends to have the smallest amount of traffic with respect to amount of data being passed, along with a small and fixed bandwidth requirement, it is the most critical service in support of electric power system operations. Figure 1 illustrates a traditional approach to the different services requiring data transport over a utility network, grouped in three categories: system critical, system priority, and system administration and support. The horizontal axis represents the required restoration time, in the event of an outage, and indicates that the required performance of low latency and high criticality should be met by using dedicated circuits. Services that can accept higher latency and are less critical for power system operations are cost driven and can be transported over shared networks. For a utility Ethernet network, the "dedicated circuits" can be translated to MPLS, and the "shared networks" to IP.

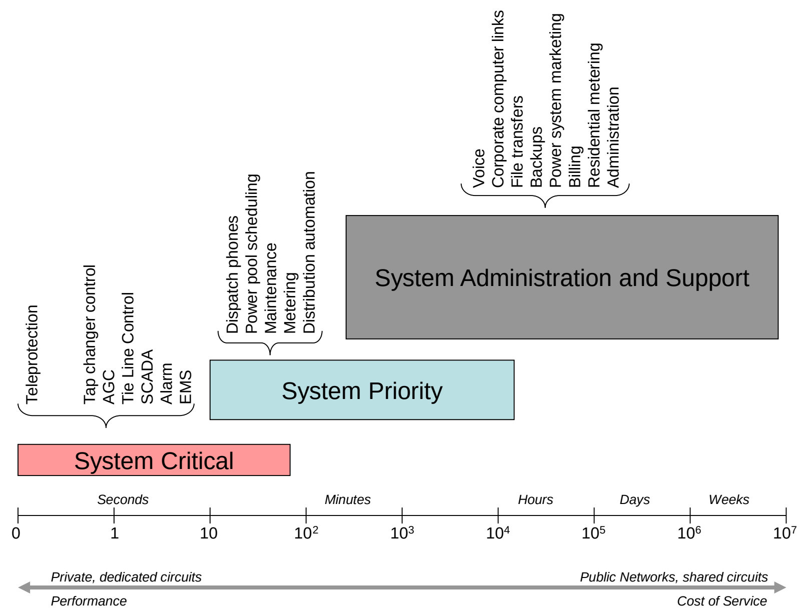


Figure 1: Utility Communication Services

SONET versus MPLS Ethernet Communications

Early teleprotection communications circuits used hardwired (pilot wires), over PLC (Power Line Carrier), and later audio tone over analog leased telephone circuits. Today, depending on the type and size of an electric utility, most or all of these services may still be in use.

The telecommunications industry is continually evolving as new technologies are adopted or applied to vendor equipment to increase reliability, detection and clearing speeds of their equipment. Figure 2 illustrates telecommunication technology life cycles over time. What started out as a telephone network with manual switching is becoming a telecommunications network optimized for data networking, using packet-based switching. Protective relaying continually adopts to new technologies, however, due to the criticality of the monitoring equipment required for power system reliability and long development times, teleprotection communications circuits typically lag behind in time, as illustrated under the graph in Figure 2. For example, 64 kbps digital communications circuits were introduced for telecommunications in the mid 1960's, but current differential relays and teleprotection using 64 kbps interfaces did not become commercially available until around 1990.

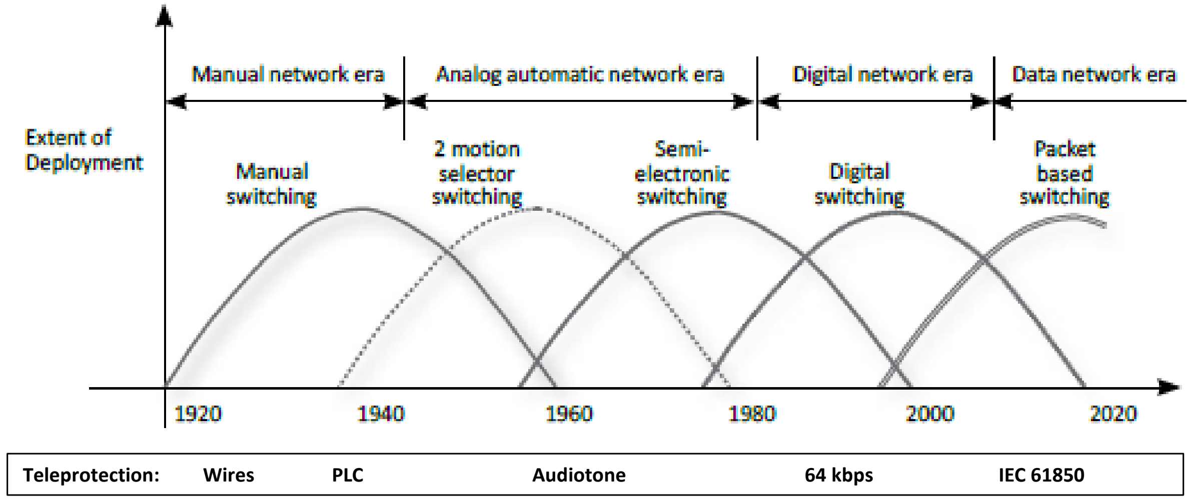


Figure 2: Telecommunications technology evolution

It should also be recognized that teleprotection communications have unique characteristics and performance requirements that are challenging to accommodate with standard telecommunications technology that was originally designed to transport two main type of services: data and voice.

Data is intrinsically different from voice. By definition, data is information which originates in the form of digital representation (binary 1s and 0s) and therefore does not need to be converted to digital within the network, unlike a voice type service that originates as an analog signal. There are several key differences between the characteristics of voice and data and hence different requirements for effective communications. To complicate matters, teleprotection communications have requirements for legacy networks that are a mix of voice and data, as compared to all data services for new networks. By nature, teleprotection digital communications is data that operates in real-time, like voice. However, the relatively high error tolerance and relatively moderate latency requirements for voice are not acceptable for teleprotection. Table 1 summarizes many of the most important differences.

Table 1: Communication services requirements

	Data	**Voice**	**Teleprotection**
Delay (latency) tolerance*	High	Moderate/Low (100 ms)	Very low (<20 ms)
Jitter (variation in delay) tolerance*	High	Moderate	Very low

Stream/burst transmission	Bursts	Stream	Stream
Interruption tolerance	High	Moderate (0.5 sec)	None/very low
Asymmetry tolerance	High	Relatively high	Scheme dependent: from very low (87L) to a few ms (21L) to NA (DTT)

* Note that reducing jitter will increase latency and vice versa. Jitter is minimized by increasing buffering, hence increasing the latency.

Teleprotection using 64 kbps interfaces have been successfully utilized over utility TDM T1/SONET network that can meet teleprotection communications requirements; engineered for 99.999% and higher availability. This is because circuit-switched networks create a dedicated circuit, or channel, which is used for the duration of the transmission. They are connection-oriented using a fixed path that remains constant and fixed in place with dedicated bandwidth for teleprotection. Utility SONET networks typically provide very low latency on the order of a few ms, partly due to their limited size and extensive use of fiber. Redundancy is typically provided by network rings, where fail-over to a healthy path takes place in as little as 2 – 5 ms by a substation multiplexer sending data simultaneously using two data paths, or less than 50 ms for a standard telecom grade multiplexer. Symmetry (equal transmit and receive latencies) is provided by using network technologies that switch transmit and receive paths simultaneously during a fail-over operation. Symmetry is guaranteed by the nature of the technology and protocol in use. TDM locks transmit and receive paths to the same timeslots, thus guaranteeing that the performance is the same in both directions.

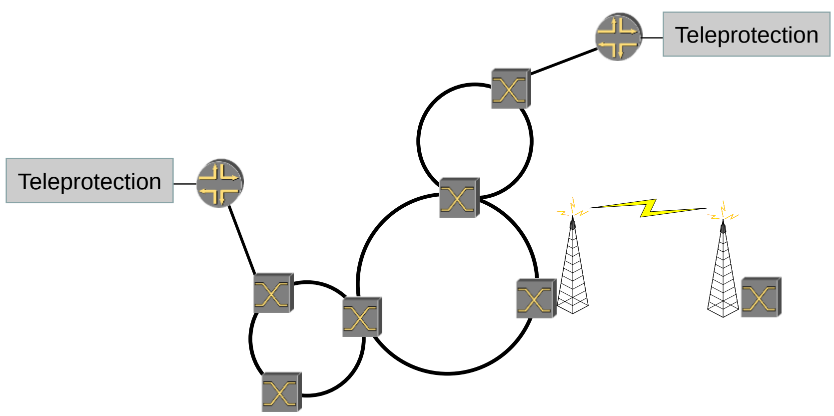


Figure 3: SONET communications network

A disadvantage with TDM is that TDM does not make efficient use of available bandwidth. The use of TDM wastes bandwidth capacity in order to guarantee deterministic behavior. Packet networks are seemingly more efficient as they allow for flexible bandwidth assignment and usage. Networks using Ethernet, MPLS, and IP are packet-based networks. Today's MPLS uses pre-configured LSPs or label Switched Paths, which are not dynamic, but rather are specified “pinned-up” paths through the network. Typically, as long as the network remains static, a path won’t change. A dynamic action of the network happens when a network fault or outage occurs and the network must reroute around it, at which point the IP will pick the shortest, most efficient path through the network based on the route-tables. This connection-oriented, dynamic routing communication mechanism results in the potential for dynamic bandwidth assignment and network latency as the path through the network changes. The main disadvantage for teleprotection in the past had been that the latency was non-deterministic in IP networks with the potential for asymmetry, due to different transmit and return paths.

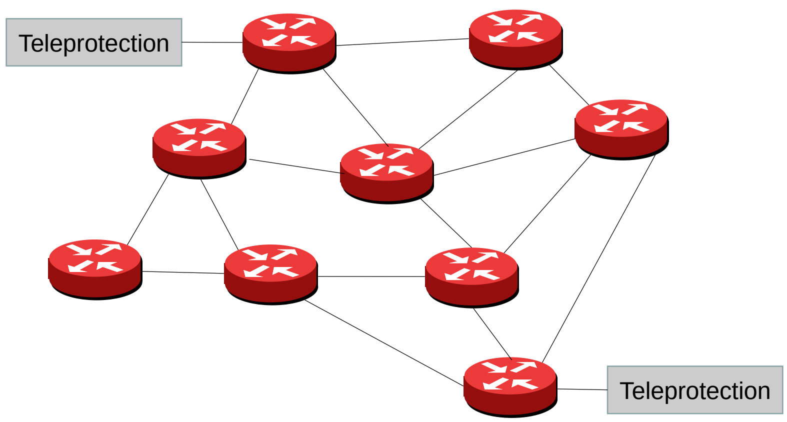


Figure 4: Ethernet communications network

The non-deterministic nature of basic IP communications previously disqualified this technology for use with teleprotection communications interfaces and applications. MPLS (Multi-Protocol Label Switching) was initially introduced to minimize latency in each node by providing a simpler label and forwarding table to direct traffic along a pre-determined path (Label Switched Path or LSP). MPLS offers the added capability of circuit emulation services that allow the emulation of legacy services, such as serial RS-232 communications onto network edge, while still having packet-based switching in the core. (It is outside the scope of this paper to describe the MPLS technology in detail, but it is mentioned here merely to explain how MPLS can meet the requirements for teleprotection communications.)

MPLS networks use several features to meet latency and asymmetry requirements for teleprotection communications, such as:

- MPLS provides a low latency advantage which comes from using label switching in the pre-defined path, and by having small data jitter buffers. Jitter buffers create a packetization delay in the data being sent. This feature ensures the flow of data during network effects (i.e. fade or drift in a microwave connection). Latencies on today's MPLS network equipment, over a relatively limited utility network size, approaches that of a SONET network, and are on the order of 3 - 5 ms when buffer settings are optimized.

- High priority provisioning though the use of QoS (Quality of Service) to ensure that teleprotection traffic packets do not incur added latency from larger, lower-priority packets. This feature helps to guarantee that teleprotection traffic will be left untouched on congested circuits. Traffic with lower priority may suffer from data loss but the teleprotection communications will remain unaffected even during a network congestion scenario.
- MPLS with the use of RSVP-TE (Traffic Engineering) provides techniques to ensure minimal asymmetry, by routing transmit and receive teleprotection paths over the same network nodes.
- Fail-over times with the present MPLS technology vary depending on if the fiber has a hard break or if the network is black-holing (losing data packets) network traffic. Fail-over times can be as fast as sub-50 ms and up to significantly longer 300 ms or greater failover times. In some scenarios MPLS failover cannot match the SONET substation multiplexers used today. However, the impact of this limitation on teleprotection is greatly reduced by adding redundant teleprotection (pilot) channels in the relays themselves, with a fail over time of 0 - 2 ms. This channel redundancy was not always possible for SONET due to limitations of available channels, but with the higher bandwidth provided by MPLS, channel redundancy is accomplished at a very low cost.
- In the SDG&E communications network, due to various vendor monitoring interfaces, there is very little if any, performance monitoring of the legacy TDM network (essentially only good/bad alarming). As a result, this does not provide to the SDG&E operators real-time information as to when a telecommunications circuit performance has become degraded or impaired. MPLS network monitoring tools have the potential of providing improved network monitoring and diagnostics for teleprotection communications. These network monitoring tools are expected to be able to continuously monitor latencies, asymmetry, packet loss and the jitter buffers. One of the main issues today with teleprotection at SDG&E, is being able to accurately correlate relay alarms with network diagnostics so that a relay channel alarm can be compared against an interruption on the network.

SDG&E Methodology for Adopting MPLS for Teleprotection

The SDG&E MPLS network is currently under construction and is not in production at the time of writing this paper. SDG&E System Protection and Control Engineering (SPACE) has developed a plan for qualifying MPLS communications for teleprotection, and migrating production substation relays to MPLS following extensive testing. The plan includes:

1. Development of technical performance requirements based on internal and external business requirements for teleprotection communications.

2. Evaluation of teleprotection and relay performance over a laboratory MPLS networks, observing relay response to network anomalies such as asymmetry, interruptions during fail-over, and changes in latency. This initial benchmark was used to determine network configurations for the subsequent real time digital simulation (RTDS) testing of the relays with applied network traffic that was created through the use of network traffic simulators.
3. Performance RTDS benchmark testing of the existing transmission line protection relay settings to be applied to field test relays installed for extended field testing over production level MPLS circuits to verify correct performance of the schemes.
4. Implement extensive channel monitoring functions, as available by the test relays and routers in the field to collect comprehensive communications channel performance data. [1]
5. Monitoring of all field test relay alarms, functions, and communications over a twelve-month period. This allows for a lengthy test and analysis period that spans all of the seasonal and environmental variations that may occur in a given region. Test relays have been installed on at least eight selected Tie Line circuits (500 kV, 230 kV, 138 kV, and 69 kV). The test relays will operate in parallel with existing production relays, to monitor transmission line voltages and currents, but relay tripping outputs will only be monitored and not connected to other equipment.[2]
6. Assuming successful twelve month testing period, the test relays will be transitioned into production, and the TDM to IP packet migration roll-out will be extended to other circuits as the MPLS communications network expands to other substations.
7. Relay communications utilizing dual-port communication paths where the primary path is on dedicated, direct fiber will remain as-is (unchanged). The standby channel will be transitioned to IP/MPLS to leverage the mesh network and reroute capabilities of the next-generation MPLS network. The primary, dedicated path will be fastest while the standby channel is potentially more reliable due to the reroute capability.

---

[1] While the RTDS testing is utilizing MPLS communications channels, it is not possible to emulate field production MPLS network conditions within a lab environment. To ensure that any issues that may arise during the field test period are related to the communications network, and are not due to a protection scheme deficiency, the schemes and relay settings are thoroughly tested in the ITF (Integrated Test Facility) RTDS lab on a model that accurately simulates the circuit each test relay will be installed on. In doing this, root cause analysis of any protection mis-operations during field testing will not need to involve extensive protection scheme evaluation and testing, since schemes and settings have already been fully verified.

[2] MPLS network data and relay channel monitoring data will be continuously collected and analyzed, with the use of analytic tools so that relay reports and MPLS network reports can be correlated for any communications errors. This has been a shortcoming with SONET communications where the relays will record channel interruptions that are not observed by network monitoring tools.

Technical Requirements Developed by SDG&E for Critical High Voltage Teleprotection Applications

The internally and externally driven requirements developed by the System Protection and Controls Engineering (SPACE) group went beyond technical performance requirements for the communications channels, and included requirements such as expandability, maintainability, incident response, design and reporting requirement, etc. However, this paper will be limited to discussing the main technical requirements for the teleprotection communications channels. The main 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 test period.
2. Low latency to be as good as or better than existing latency for these circuits. The channel latency is directly added to the protection scheme fault clearing time. The existing SONET links in the SDG&E network provide on average 5 ms one-way latency, and the goal is to match this performance with the MPLS system. It was agreed between IT and SPACE to use 5 ms or better as the criteria for laboratory testing and network configuration of the MPLS circuits that would also be used for the field test relays.
3. Minimal asymmetry. Before performing testing, the asymmetry limit was set to <2 ms, based on recommendations from the manufacturers of the current differential relays to be deployed. For field test relay commissioning, a benchmark of <0.5 ms will be used for the MPLS communications circuits as anything higher than would indicate misconfiguration of the network communications channel.
4. Fail-over <50 ms. This requirement was initially <3 ms based on the multiplexer equipment in use. This could not be achieved with MPLS. However, by using redundant communications channels in the relays themselves, channel change-over for the teleprotection is still achieved in <3 ms by the relay switching to its redundant channel that is routed over an independent path. This relay channel redundancy is enabled by having more than one channel through different fiber or microwave paths.

Testing Methodology and Test Results

The SDG&E defined performance objectives for the new MPLS communications system that were tested in the ITF lab using the RTDS® are as follows:

- Latency < 5 ms
- Asymmetry < 2 ms
- Failover < 3 ms
- Availability > 99.95% (500 kV)

Total latency is defined as the one-way time delay from a transmitted signal such as a permissive trip signal at one protective relay terminal to the receipt of that signal at the remote protective relay (from (a) to (a) in Figure 5). Total latency will include delay through the sending relay communication processing, sending relay communications channel delay such as a C39.94 interface, delay through the MPLS router on the sending end, delay through the MPLS network, delay of the receiving MPLS router, delay through the communications interface on the receiving end and delay through the receiving relay's communication processing. As the relay or teleprotection communications interface is integrated in the relays, the 5 ms requirement applies to the communications network channel latency, i.e. from when the MPLS router receives the data from the relay interface to when the remote MPLS router delivers it to the receiving relay (from (b) to (b) in Figure 5).

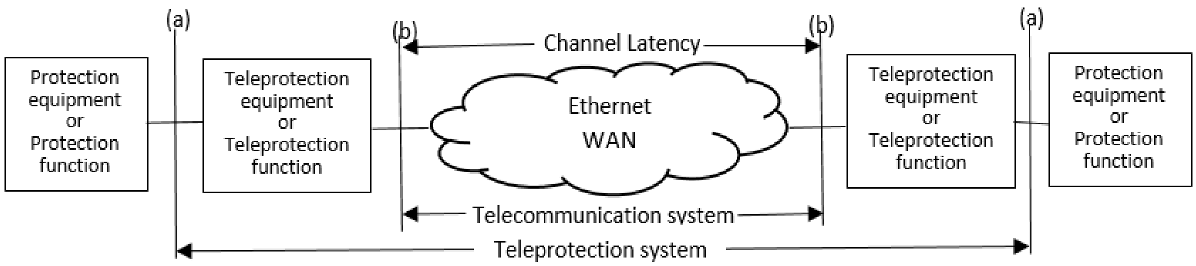


Figure 5: Teleprotection channel latency[3]

Asymmetry is defined as the difference in transmitted versus received signals and must be less than 2 ms.

Failover is defined as being the switch from a primary communications channel to a backup protection channel. This failover time must be less than 3 ms.

Availability is defined as the percentage of time that a communications channel is functional. The availability of any protection channel must be greater than 99.95% for 500 kV protection systems. Availability was checked in the laboratory setup, but it does not reflect a true MPLS real life communications network, and availability will be evaluated during the field test relay period. Several models were developed for the RTDS of the San Diego Gas and Electric transmission system. One RTDS model included 500 kV transmission lines and another included 230 kV lines. These reduced set models were validated against known short circuit models of SDG&E's transmission system. The reduced models can fit into an RTDS rack of processing units. Figure 6 shows an example model of the SDG&E transmission network.

[3] Figure from IEEE PSRC WG H32 Teleprotection over Ethernet (draft)

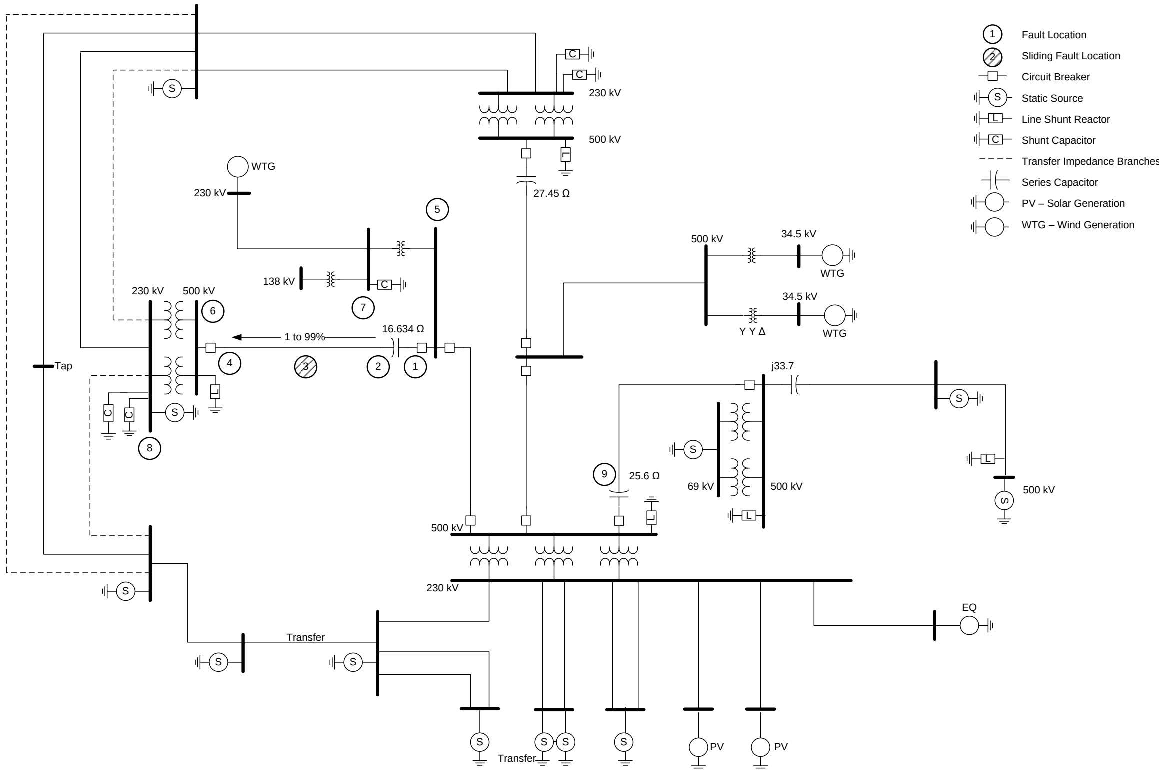


Figure 6: RTDS Model of SDG&E Transmission Line Network

Figure 7 shows the test setup for the RTDS and the protective relays. SDG&E uses three redundant protective relays of different models and different manufactures for protection of their 500 kV transmission lines. Two of the relays have both 87L line current differential protection and 21L distance element communications based protection which is usually a Permissive Overreaching Transfer Trip (POTT) scheme. These two relays also include time-step backup protection and time delayed overcurrent backup protection. The third relay has 87L protection and time delayed backup overcurrent protection. SDG&E uses two redundant relays for lower voltage than 500 kV transmission line protection.

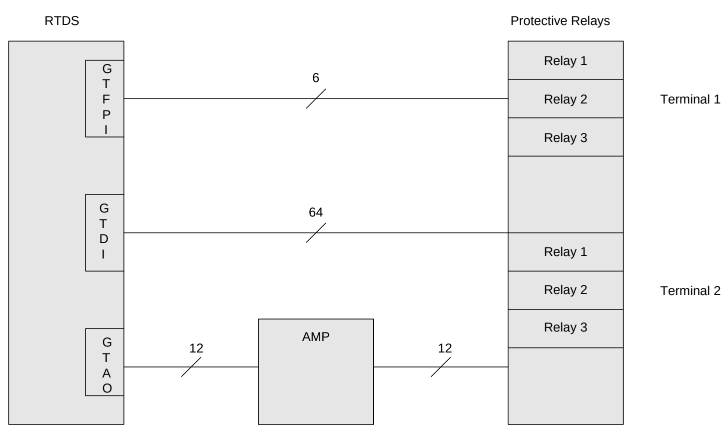


Figure 7: RTDS test setup

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 within SDG&E's transmission line network. The RTDS also provides breaker status outputs (6 digital signals) and receives digital contact output closures (64 digital signals) from the protective relays for such things as trips, permissive signals used in communication based protection schemes and communication channel status. In this fashion, the RTDS and protective relays for each protected transmission line terminal test the protection and communications system in a closed loop method.

Overall, there will be 8-12 different transmission lines' protection systems tested in the lab using the RTDS. Many different fault types, fault locations and operating conditions can be tested using the RTDS to evaluate the performance of the protection system and the communication system before ever implementing the new communication system in the field.

The communications setup in the RTDS lab for testing is shown in Figure 8.

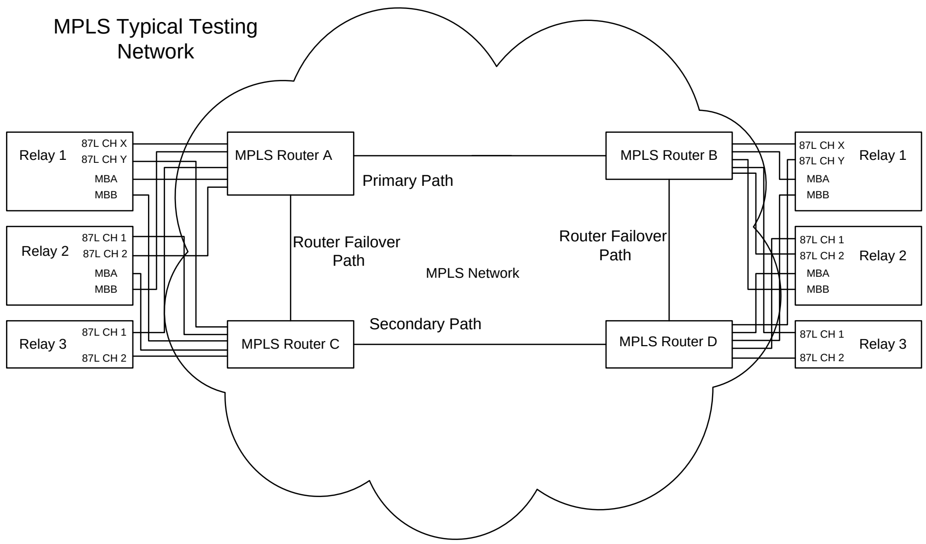


Figure 8: Protective Relay Communications Test Setup

The test set up allowed testing for many different router configurations with respect to speed. This test set up is for two terminal transmission lines. Three-terminal transmission lines were also tested.

The speed of the router was controlled by MPLS router settings called Jitter Buffer and Payload. The faster the speed, the lower the Jitter Buffer, the smaller the Payload size of Ethernet packets and the higher the bandwidth of the communications channel. Conversely, the slower the speed, the higher the Jitter Buffer, the larger the Payload size of Ethernet packets and the lower the bandwidth of the communications channel.

The communication paths from the relays through the MPLS network are shown in Table 2.

Table 2: Teleprotection communications paths

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)

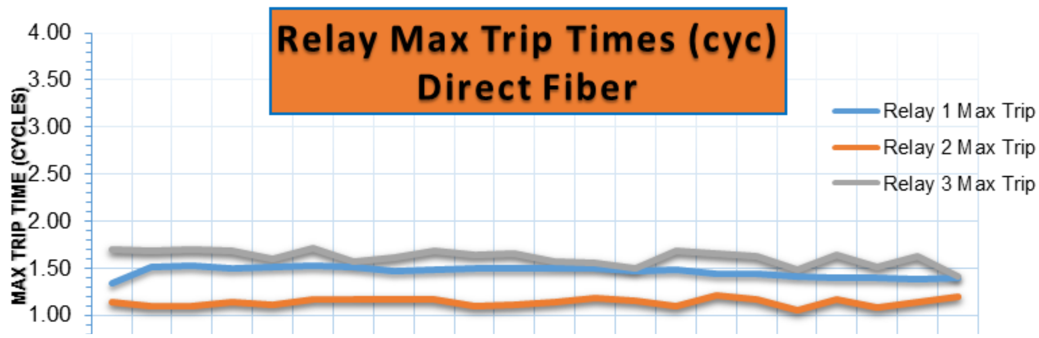
For redundancy, not all 87L primary channels are routed through the same MPLS path. Similarly, not all 21L POTT scheme channels are routed through the same MPLS path.

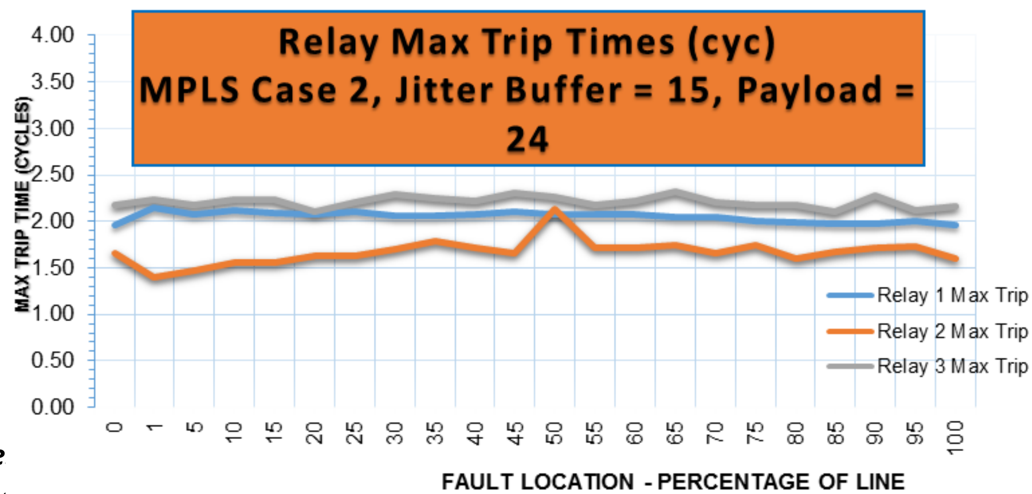
Latency Tests

Latency tests were performed by using measurements from the protective relays to determine the communications channel latency from the protective relay communications report. Baseline latency and jitter/variance tests were also performed by using a benchmark of back-to-back fiber connections between the relay communications channels (no MPLS Ethernet routers). These tests were conducted by determining the tripping speeds of the 87L line current differential and 21L distance POTT scheme, then comparing these trip times to various tests run with the MPLS routers in the communications path run at different Jitter Buffer and Payload router settings.

The latency tests applied internal faults along the line and trip times were compared with the benchmark back-to-back trip times. This data has helped determine several opportunities for improvement in both the communications channel setup as well as protection scheme settings in the relays. The data along with communications channel reports from the relays have helped determine the Ethernet MPLS router settings needed to meet the latency requirement for teleprotection traffic in the MPLS routers.

Figure 9 shows 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 graphs illustrate the added delay due to the latency over the communications link, which is expected. What is also important is that the graph verifies that the relay settings provide practically constant operating times for internal faults, and that the MPLS channel is not introducing trip speed variations.





Failover Te

Figure 10 shows the test setup for testing of failover from primary communication channel to backup relay communications channel. The primary communication channel could be broken at specific times using a switch controlled by the RTDS simulation. Notice that the failover can be done two ways, one by failing over from the primary Ethernet router path to the secondary Ethernet path by the routers themselves; the second is the protective relays failing over from the primary path to the secondary path because there were redundant 87L line current differential channels for each relay and two of the relays using 21L distance element protection schemes had redundant communications channels also used for POTT schemes.

87L Channel Link Break
Test Setup

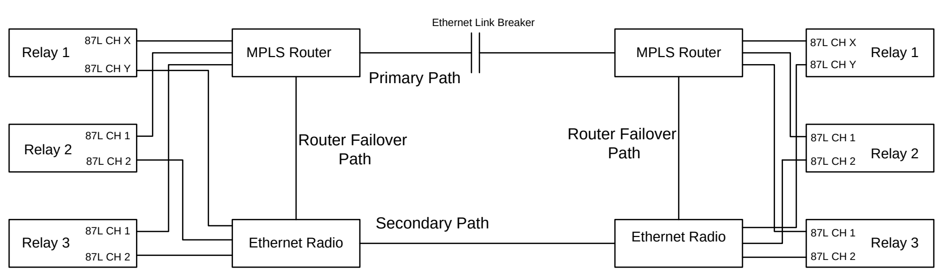


Figure 10 Communications Channel Failover Test Setup

The primary protection channel of the MPLS Ethernet routers was broken at a specific time by the RTDS simulation controlling a fiber optic switch. Times were then measured by relay event reports for healing or failover times for the MPLS routers and also for 87L line current differential channel failover in the protective relays from the primary channel to the backup 87L channel. The MPLS routers failover time ranged between 35 and 50 ms which was slower than the specified time of 3 ms. Two of the three protective relays could switch between the primary 87L channel to a backup "hot standby" channel within 2 ms which did meet the SDG&E failover requirement. One protective relay's failover time from primary to backup 87L channel was in the range of 50 ms which did not meet the failover requirement. Overall, the protection system as implemented met the failover requirement with 2 of the 3 protective relays.

Asymmetry Testing

Asymmetry is the difference in the transmitted data latency versus the received data latency. Asymmetry can cause errors in protective relay protection elements, especially in 87L line current differential elements. The asymmetry looks like a phase error in the received currents from the remote terminal as compared to the measured currents in the local terminal. This can cause 87L line current differential protection to false trip for out of section faults and a failure to trip for in section faults.

Figure 11 shows the test setup for testing the asymmetry tolerance of the protection system. Asymmetry was introduced by creating delay in the communications channel in one direction only. These tests focused on checking that the 87L line current differential elements in each relay did not misoperate by tripping for out of section faults or fail to trip for in section faults.

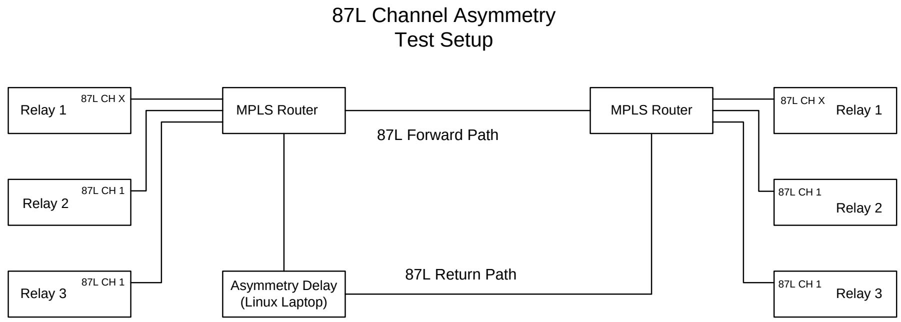


Figure 11 Asymmetry Test Setup

It should be noted that some of the tested 87L relays have the ability of using time based synchronization, taking their time source from a station GPS rather than using channel based synchronization. The time based synchronization have much higher asymmetry tolerance as the actual one-way channel delay is used for compensation. While SDG&E's present standard is to use channel based synchronization due to potentially unreliable GPS sources, some field test relays will be set to use time based synchronization for evaluation purposes.

Summary of Test Results

The summary of lab test data versus the SDG&E defined requirements is listed in Table 3.

Table 3: Summary of Test Results

Communication Requirement	Specification	Results
Latency	< 5 ms	Pass[1]
Asymmetry	< 2 ms	Pass[2]
Failover	< 3 ms	Pass[3]
Availability	> 99.95%	N/A

[1] Latency < 5 ms achieved with specific Jitter Buffer and Payload MPLS router settings.
[2]Asymmetry < 2 ms achievable with specific network design. Laboratory tests show protection operates correctly at 2 ms asymmetry specification limit.
[3]Failover < 3 ms achievable with 2 of 3 relays meeting specification. Protection system with designed failover paths and protective relay failover meets failover specification. MPLS routers do not meet failover specification failing over to backup Ethernet router path.

Field Relay Test Methodology

As the project moves from lab testing to field test where test relays will be commissioned in live substations with a new MPLS Ethernet communications network, communications channel monitoring functions will be utilized from both in the protective relays and from the network equipment into a SDG&E non-operational data warehouse for post analysis and trending.

Field test relays will be commissioned in the field alongside of production relays using the existing TDM communications network. The MPLS field test relays will not trip breakers nor do any circuit breaker control as they are evaluated in parallel with the production relays.

The communications channel monitoring functions include alarms in the Sequence of Event Recorders (SERs) and Event Reports of the protective relays. These alarms include loss of communications channels, high latency, high asymmetry and noise bursts in the communications channels. SER, communication reports and event reports will be archived and the alarm data will be monitored by SDG&E personnel through the SDG&E Condition Based Maintenance (CBM) system that handles non-operational data. These alarms will help to quickly troubleshoot issues and problems that can arise in the new communications network as the field test relay evaluation period progresses.

The event reports and SERs of the MPLS field test relays will also help to evaluate their protection system performance as compared to the existing production relays. Proper tripping, trip speeds, and restraint of tripping for out of section faults will all be evaluated using the field test relays.

Conclusions and Lessons Learned

1. Laboratory testing to this point has shown that MPLS networks are a viable communications medium for protective relay telecommunication traffic if designed properly by considering latency, asymmetry, failover and availability.
2. A potential improvement of teleprotection with MPLS communications is the increased network monitoring and diagnostics functions. It is expected that this will enable better correlations between relay channel monitoring functions and network monitoring tools to be able to determine where errors or failure are located in the communications chain from relay to relay. This is an important function that will be further enhanced during field relay testing.
3. While the MPLS network compares favorably with a TDM network with regards to performance, it could not meet the <3 ms fail-over requirement. However, the comparatively long failover times for MPLS channels (>50 ms) were overcome by using the relay channel redundancy. One advantage with MPLS is that more teleprotection communications channels with diverse paths (where available) can be applied to the protection schemes.
4. The RTDS testing has helped to prove SDG&E performance requirements of the MPLS communications system by allowing configurations, transmission line protection systems of SDG&E lines and many other scenarios to be tested.
5. While the RTDS testing is utilizing MPLS communications channels, it is not possible to emulate the production MPLS network conditions in a lab environment. To ensure that any issues that may arise during the field relay test period are related to the communications network, and are not due to a protection scheme deficiency, the schemes and relay settings are thoroughly tested in the RTDS lab on a model that accurately simulates the Tie Line circuit they will be installed on. In this way, root cause analysis of any protection misoperations during field relay testing does not need to involve extensive protection scheme evaluation and testing as the schemes and settings have been fully verified.
6. Laboratory testing of the new MPLS communications system using the RTDS has allowed many real-world types of tests to be completed before implementing an actual network design. This testing in conjunction with field relay testing will help to validate the new MPLS communications system and has promoted the learning about the new MPLS communications system for SDG&E engineers, technicians and operations personnel.

References

[1] Inside the Cloud – Communications Basics for the Relay Engineer, S. Ward et al, WPRC 2007

[2] Pilot Protection Communication Channel Requirements, S. Ward et al, WPRC 2004

Acknowledgements

A special “Thank You” to those who contributed to the creation and completion of this paper:

- Mike Mahoney – Burns & McDonnel
- Clint Struth and Cory Struth – SCI Networks
- Terry Wright – GDC Consulting

Biographies

Tariq Rahman is a Principal Engineer in the Electrical Transmission & Distribution Engineering Department at San Diego Gas & Electric Company (SDG&E), California. Prior to joining SDG&E Tariq worked with Long Island Lighting Co. in New York, and Sunflower Electric Coop. in Garden City, Kansas. He obtained his BSEE in 1980 and MSEE in 1985. Tariq has 30+ years' experience in working in the electric utility industry. During this time he has worked in Electric Operations, Generation Planning, and System Protection and Control Engineering. In addition to his system protection engineering functions he is leading the Transmission Synchrophasor Project at SDG&E. He is a licensed Professional Engineer in the states of New York and California, and is a member of IEEE.

James Moralez James Moralez received his Bachelor of Electrical Engineering degree in the area of Power Systems, Power Devices, and Power Design from Georgia Institute of Technology, and is a Principal Engineer working in the System Protection and Controls Engineering group at San Diego Gas & Electric Company. James currently works within SDG&E as a Project Engineer working on several projects involved with integrating new or network based equipment with existing controls equipment within the substation environment.

Solveig Ward has over 40 years' experience working in a variety of managerial, product management and marketing roles in the protective relaying and relaying communications area, and presently is Executive Advisor for Quanta Technology; Protection and Automation group. Combining relay expertise with communications knowledge, she provides leadership in the area of communication systems for power system protection and control including IEC 61850, wide area protection, and cyber security issues. Solveig is an IEEE Fellow and past Chairman of the IEEE PSRC System Protection subcommittee.

Eric A. Udren has a 48-year career in design and application of protective relaying, substation control, communications systems, and remedial action schemes based on embedded computing platforms, Ethernet, IEC 61850, and synchrophasor techniques. Eric is Life Fellow of IEEE, and twice served as chair of the Relaying Communications Subcommittee of the IEEE Power System Relaying Committee. He is US Technical Lead for IEC TC 95 relay standards; and is a charter member of IEC TC 57 WG 10 that develops IEC 61850. Eric serves as SME on the NERC System Protection and Control Subcommittee (SPCS) and the NERC Relay Maintenance Standard Drafting Team (PRC-005-6). Eric appeared as Sept. 2016 PACworld Magazine Guru, with over 90 technical papers and 12 patents. Since 2008 he has served as Executive Advisor with Quanta Technology LLC, with his office in Pittsburgh, PA.

Michael “Mike” Bryson received his Bachelor of Science in Electrical Engineering (BSEE) from the University of Idaho. Mike is a power system protection engineer with 28 years of experience at Schweitzer Engineering Laboratories (SEL) in Pullman, WA. He has experience in power system protection, protective relay development, modeling, simulation and testing. Mike has used RTDS systems at SEL to develop protection algorithms in SEL relays and to model, simulate and test unique and challenging customer protection and control systems. He is a member of IEEE, author of several technical papers and presentations, a recipient of several patents and a registered PE.

Kamal Garg is a senior protection engineer in the engineering services division of Schweitzer Engineering Laboratories, Inc. (SEL). He received his M.S.E.E. from Florida International University and India Institute of Technology, Roorkee, India, and his B.S.E.E. from Kamla Nehru Institute of Technology, Avadh University, India. Kamal worked for POWERGRID India and Black & Veatch for several years at various positions before joining SEL in 2006. Kamal has experience in protection system design, system planning, substation design, operation, remedial action schemes, synchrophasors, testing, and maintenance. Kamal is a licensed professional engineer in the United States and Canada.