# Case Study Protective Relaying over IP/MPLS

Myth to Facts

Michael A. Nunez, P.E. and James Denman, *Lower Colorado River Authority*

Genardo T. Corpuz, P.E. and Joey B. Melton Jr., *Lower Colorado River Authority*

Hansen Chan and Ivan Schonwald, *Nokia*

**Abstract:**

The Lower Colorado River Authority (LCRA) is a public utility that operates in central Texas to manage the water supply in the Lower Colorado River basin and both generates and supplies electric power. LCRA Transmission Services Corporation (TSC) owns and operates more than 4,800 miles of transmission lines and 330 substations.

IP/MPLS (Internet Protocol/Multi-protocol Label Switching) utilized primarily by the larger telecommunications service providers but has recently developed a presence in the public utility market. LCRA TSC has its own mission critical communications network supported by an 80-node SONET ring including over 170 IP/MPLS nodes. We have been migrating systems to IP/MPLS over the last 5 years. The MPLS network supports services that include SCADA, voice, security video, metering, and enterprise data. LCRA TSC is currently in the process of testing protective relay communications on its IP/MPLS network.

In this paper, we will discuss the implementation of IP/MPLS technology for protective relaying. We will publish our test results using relays with DCB and LCD pilot schemes transported over the IP/MPLS network. Our IP/MPLS network is multivendor and uses various types of communication transport including microwave radio, direct fiber, SONET, and DWDM.

**Discussion Points**

1. The overall advantages of MPLS over older technologies such as SONET.
2. Test results for communication and relay delays.
3. Strategies for protecting and monitoring the communication paths to provide maximum reliability.
4. Potential risks and important considerations.

## I. History of LCRA TSC Communications

LCRA TSC utilizes a communication network that consists of both legacy TDM (Time-division multiplexing) and IP/MPLS (Internet Protocol/Multi-protocol Label Switching) backbone technologies. It contains over 1100 miles of OPGW (optical ground wire) fiber and by over 500 miles of 3rd party fiber. This also includes over 280 microwave paths supporting both TDM and Ethernet for IP/MPLS and TDM transport. The migration from legacy TDM to Ethernet services over MPLS began slowly but the transition has occurred rapidly over the last couple of years.

## II. TDM Communications

TDM is a legacy transport used by LCRA TSC for nearly 25 years. The network transition initially began by migrating from legacy analog networks to implementing a digital network consisting of SONET (synchronous optical networking) nodes with T1 communication lines and channel banks. The digital TDM network operates using a high-speed SONET utilizing fiber for speeds as high as OC-192 down to OC-3 microwave. The overall TDM network supports customers with speeds of one gigabit per second to as low as 1200 bps for an EIA-232 serial communications signal.

TDM communication has its advantages in that it is synchronous or time-based. It utilizes a source clock to ensure transmission of data bits is isochronous, where the time between two consecutive data bits is always the same. This ensures data arrives when expected and helps to reduce jitter where an individual communications device will adjust its own transmission clock rate to match the master source clock.

TDM can provide guaranteed bandwidth. Each customer circuit has a specified amount of bandwidth to transmit data on a given set of timeslots. However, TDM does not provide statistical multiplexing; therefore, when a customer is not transmitting any data during its assigned timeslot, the bandwidth is wasted and is unavailable to other customers.

TDM is also inherently secure since each customer connection has its own end-to-end circuit. With multiple TDM services at the same location, each customer will not be able to view or modify each other's network data.

Most importantly, TDM is deterministic. This allows the network administrators to know exactly where customer data travels around the network. This helps to provide faster support in case of any network link failures and can provide direct paths to support time-sensitive applications such as teleprotection.

## III. What is IP/MPLS?

IP/MPLS is a method of transporting multi-protocol data including TDM and Ethernet across an IP network using a pre-engineered tunnel or path. Because the tunnel is already established by signaling protocols, the MPLS frames can be directed (traffic engineered) across the network using labels. Customer applications are converged into one network infrastructure allowing the network to transport a wide range of applications ranging from the most latency sensitive one such as teleprotection to best-effort Internet traffic.

Initially, there was significant resistance to bringing Ethernet/IP into the substation. The high bandwidth nature of Ethernet was not required for applications such as metering, SCADA (supervisory control and data acquisition), protective relaying, and phone circuits. SCADA and protective relaying circuits require reliable and deterministic communications, which is not always the case for IP networks.

The pressure to introduce IP into the substation has increased due the introduction of smart grid technologies and higher bandwidth applications such as surveillance video, causing TDM and serial equipment to become obsolete. Additionally, advances in routing architecture have allowed manufacturers the ability to provide low latency, increased reliability, and deterministic services.

Security is also one of the biggest concerns when using IP. Utilizing IP/MPLS technologies such as L2 (Layer 2) and L3 (Layer 3) VPNs (Virtual Private Networks) keeps all customers and services separate and secure. Each customer cannot see other each other's networks or data. See Fig 1.

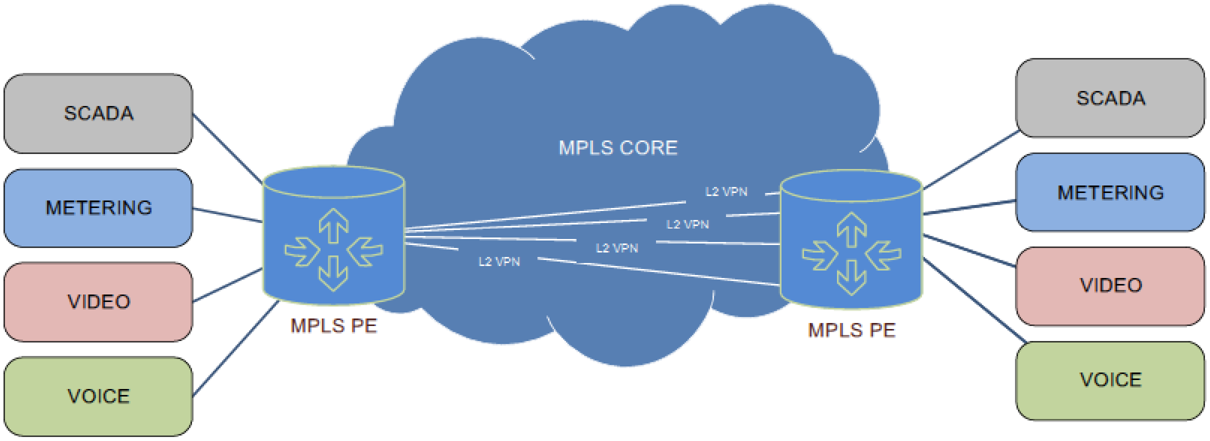

Figure 1. Using L2 VPNs for Secure Services

Traditionally, using IP as a transport required the router to perform a "lookup" of the destination address when it received a packet prior to sending data packets to the best path based on least cost following the routing protocol. This would inherently cause jitter issues with unpredictable latency and does not provide explicit route control of traffic. When deploying protective relaying applications such as line differential protection, it is critical for the network to provide reliable communications so that data bits constantly arrive at predictable intervals. Therefore, network engineers have been wary to adopt IP, until the advent of routing architecture advances such as IP/MPLS.

IP/MPLS allows the transportation of many types of data, from IP to TDM and Ethernet frames, across an IP network using a pre-engineered tunnel or path (label switched path, or LSP) setup by the Resource Reservation Protocol – Traffic Engineering (RSVP-TE). With IP/MPLS and RSVP-TE, network engineers can have complete route control when provisioning a critical network path for a specific application. This is achieved by provisioning a LSP with a strict, explicit route to specify a series of hops that the LSP must take. Coupled with Quality of Service (QoS), this ensures the traffic flow will be constantly symmetric and latency determinable even during congestion, crucial to satisfy the most latency-sensitive applications.

## IV. Why Move to IP/MPLS?

IP/MPLS coupled with the use of RSVP-TE allows LCRA TSC to operate in a similar manner to the existing SONET network while moving forward with new technology, providing better services and support, eventually reducing costs, and freeing up network resources.

SONET offers automatic protection with redundant paths commonly known as ring protection. If a failure occurs on a single path, the SONET node will switch to the alternate path typically within 50 ms.

IP/MPLS with RSVP-TE allows us to steer traffic flows in the network and provides multiple path protection and switching times comparable to SONET.  This deterministic behavior using Traffic Engineering and strict explicitly routed LSP hops allows an operator to provide the necessary connectivity to their critical customers, optimize under-utilized links in the network, and provide the most robust routes while meeting latency, protection, and bandwidth requirements.  IP/MPLS also provides QoS by prioritizing critical customer traffic.

Support for the LCRA TSC SONET network is approaching end-of-life in the next several years. Protective relaying is the last major customer requiring the performance abilities of SONET and other TDM technologies.  With IP/MPLS, we have the ability to provide communication service with SONET-like performance.  Support for IP/MPLS allows us to provide improved network performance monitoring and diagnostic support.  The number of services provided to our internal and external customers continues to grow and we now have the capabilities to monitor them more granularly to ensure their performance and reliability.  With the large transition of customers over to IP/MPLS, this requires us to support two backbone networks for the next several years but with higher operation costs including increasing TDM backbone equipment support costs.

By allowing us to aggregate services onto a single converged transport network, LCRA TSC can free up fiber, optimize microwave radio bandwidth usage, offer other high bandwidth services, and take advantage of direct fiber for protective relaying.

## V. MPLS Network Setup

The approach of our network setup was to provide scenarios relevant to the LCRA TSC IP/MPLS network.  The provider edge routers (PE) connected directly to the protection relays while adapting relay traffic from EIA-232, EIA-422, and C37.94 interfaces onto IP/MPLS using TDM pseudowire.  The two PE routers connected through a multi-vendor IP/MPLS core network consisting of label switching routers (LSRs) and various combinations of Ethernet fiber, DWDM, and SONET transport.  Our primary network test was using a single IP/MPLS vendor with Gigabit Ethernet interfaces over fiber and SONET.  Our secondary network test utilized a multi-vendor IP/MPLS core network over Gigabit Ethernet interfaces over direct fiber and SONET.  For the purposes of this paper, we chose to include results of these two network types while other network components such as MW transport are still in testing.  Additionally, we also included a synchronization network to provide the necessary clock distribution for synchronous data transfer.

Synchronization is a critical component of a synchronous communication circuit.  In particular, line current differential requires low latency with synchronized data while directional comparison blocking requires low jitter with low latency.  As shown in Fig. 2, one PE (Lab 1) recovered timing from the reference clock of a SONET node timed off a Stratum 1 clock and distributed to the other PE (Lab 2) using IEEE 1588v2 technology [1].

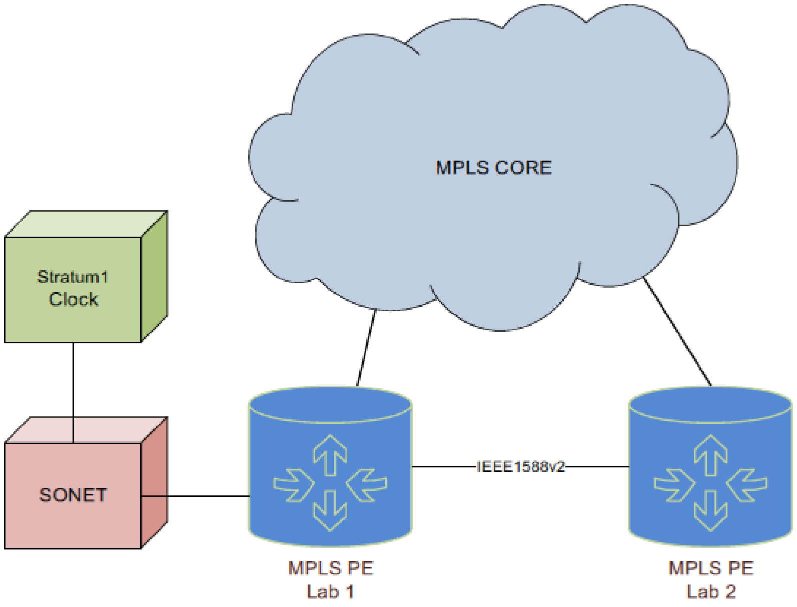

Figure 2. MPLS Timing Network

In the first test, two PEs connected to a single vendor IP/MPLS core consisting of approximately 100 fiber miles with Ethernet over SONET connections in and out of the core. There were eight SONET nodes providing Ethernet services along with 13 end-to-end IP/MPLS nodes. At the time of our testing, the network latency average was 4.06 ms, therefore providing enough buffer time well within latency budgets. See Fig 3.

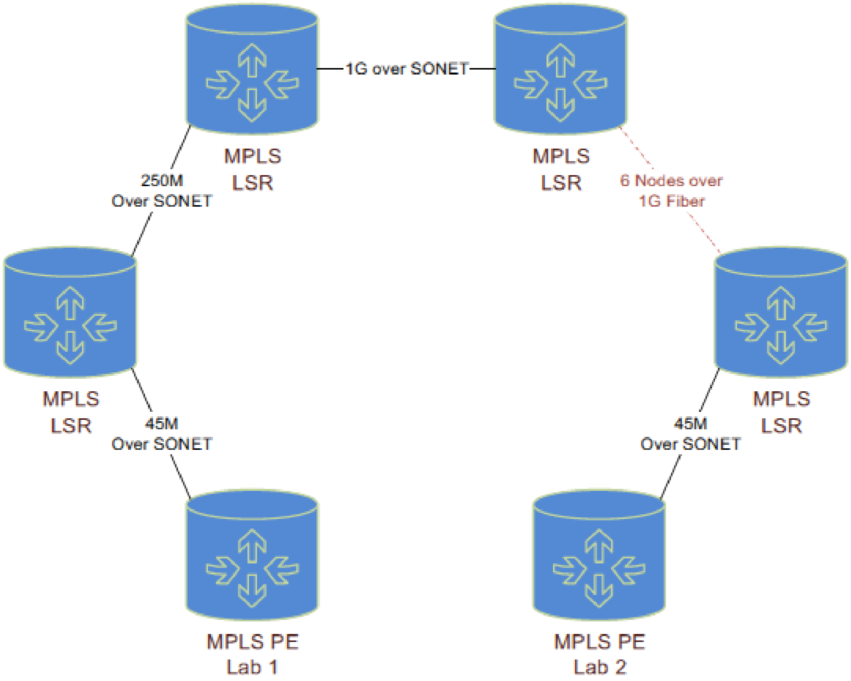

Figure 3. Long Path: Single-Vendor over Fiber

| | |
|---|---|
| Fiber Mileage | ~ 100 miles |
| # of SONET Nodes | 8 nodes |
| # of MPLS Nodes | 13 nodes |
| Network Latency (One-way) | 4.06 ms avg. |

In the second test, two PEs connected to a multi-vendor IP/MPLS fiber network that consists of two IP/MPLS vendors. As in the primary test, the two PEs provided protective relay data packetization and connected to each other through a multi-vendor core. See Fig. 4.

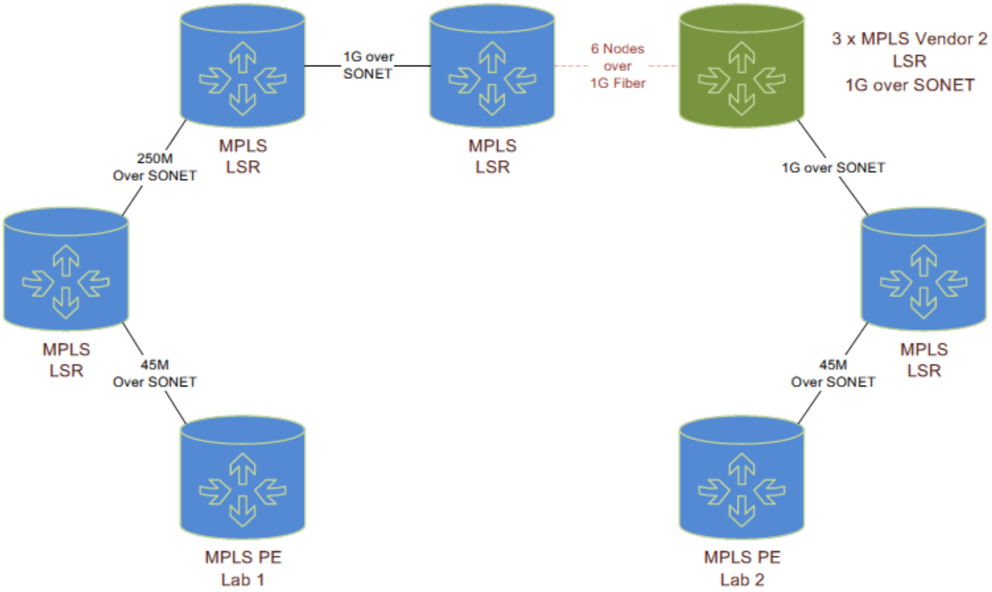

Figure 4. Long Path: Multi-Vendor over Fiber

| | |
|---|---|
| Fiber Mileage | ~ 172 miles |
| # of SONET Nodes | 14 nodes |
| # of IP/MPLS Nodes | 16 nodes |
| Network Latency (One-way) | 5.97 ms avg. |

The network in Fig. 5 below compared latency with a smaller number of nodes. It also provided a baseline test for RS-422 back-to-back testing discussed in Section VII.

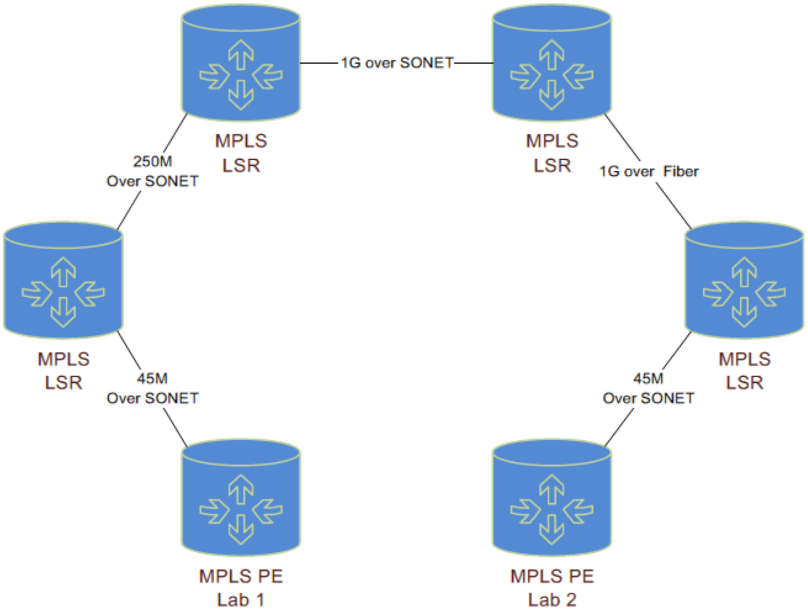

Figure 5. Short Path: Single-vendor over Fiber

| | |
|---:|:---:|
| Fiber Mileage | ~ 100 miles |
| # of SONET Nodes | 6 nodes |
| # of IP/MPLS Nodes | 6 nodes |
| Network Latency (One-way) | 3.91 ms avg. |

In addition to network delays in the IP/MPLS core, packetization and buffer delays factor into total latency consideration in the end-to-end TDM pseudowire transport. At the ingress PE, the payload size will determine the packetization delay. At the egress PE, based on the playout buffer settings, the TDM data is held in the buffer and then played out when the buffer is half-full. The changes in the buffer can affect the overall communication latency. The test buffer settings used were jitter-buffer = 4 bytes and payload-size of 2 ms. The packetizing IP/MPLS vendor provided ports to support C37.94 and EIA-422 for line current differential applications and EIA-232 for directional comparison blocking schemes.

For IP/MPLS to provide the same type of bandwidth and data delivery guarantee as SONET, QoS policies place protective relaying communications data in the highest priority over other customers. This ensures guaranteed data delivery in times of bandwidth congestion especially when competing with other bandwidth intensive customers such as video and enterprise traffic.

Line current differential communications requires symmetric, constant communication delays in both transmit and receive directions [2]. Exceeding the asymmetry delay budget can result in relay synchronization errors, causing possible false trips. While advanced IP/MPLS traffic engineering and QoS capability can allow network engineers tightly control jitter to ensure constant delay, overcoming delay asymmetry is not as straightforward as one would think. It is more than just using traffic-engineering capability to ensure packets in both directions are on the same physical path with strict QoS. The random nature of core network jitter can cause the delays in both directions to be asymmetrical but also constant, thus causing possible false trips in the relays. Asymmetric delay control (ADC) is a new QoS capability that is useful to ensure that path delays adaptively adjust despite core network delays. ADC helped to stabilize communication delays for both EIA-422 and C37.94 for LCD communications.

## VI. Relay Schemes

Two communications assisted tripping schemes used in testing protective relays in the LCRA TSC IP/MPLS network are Directional Comparison Blocking (DCB) and Line Current Differential (LCD). The protective relays in a DCB scheme relies on the direction of the fault during a system disturbance to determine if the event is an external or internal fault. During an external fault, one terminal will see it as a forward fault and the other terminal will view it as a reverse fault. The relay that sees the reverse fault will transmit a block signal to prevent a trip operation from the other end. For an internal fault, the relays sent no-block signals and both terminals can trip to isolate the fault. DCB is widely used in LCRA TSC since it is more reliable but less secure when relay communications is lost during a fault condition. The LCD protection scheme responds to the sum of all the currents in the protected zone to determine if an internal fault is present. This scheme requires digital communications and time synchronization to perform the differential calculation, as each terminal of the protected line needs to communicate their current values from one end to the other. LCD is the preferred relay scheme for LCRA TSC since it is less susceptible to dynamic system conditions, and provides better performance in terms of faster relay operation and increased sensitivity for low System faults.

## VII. Relay Setup

The relay communications test setup comprised of two transmission line relays, two power system simulation devices, and one GPS clock.

The test scenarios used relays capable of performing both LCD and DCB schemes. The relays were mounted in two different rack units adjacent to the IP/MPLS equipment rack. The GPS clock mounted in one of the relay racks provided synchronization to the relays and power system simulators. See Fig. 6.

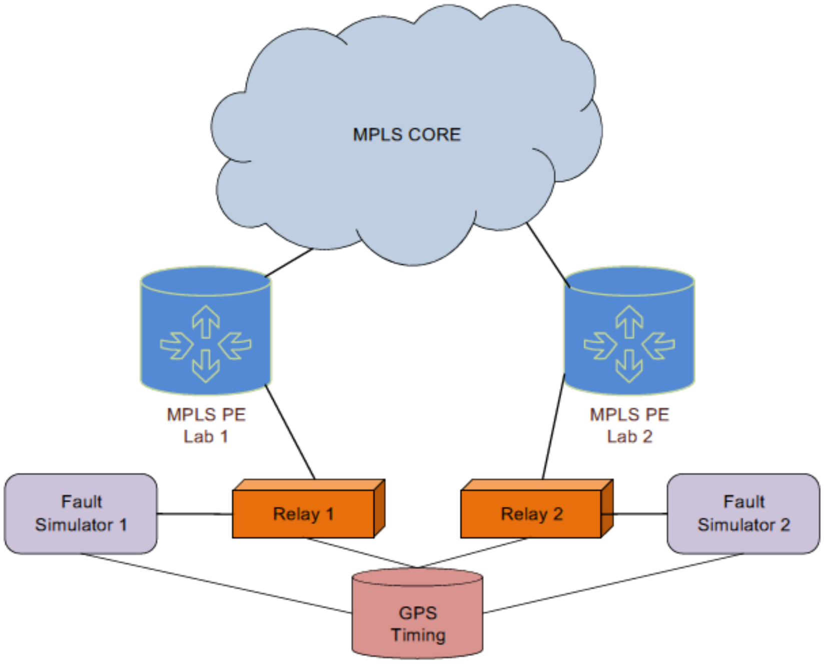

Figure 6. Relay Synchronization Setup

To ensure the fault reports and sequence of events (SER) data from each relay would show the same information at the same precise time both relays were time-synched through the GPS clock. The clock signal was distributed to each relay via either an IRIG-B connection or a hard wire connection to an EIA-485 port on each relay. Once the clock signal was established, data bits transmitted from relay to relay and a log of each relay's SER data was obtained to verify relay communication channel delays. The channel timing determined how well each communication channel scenario would perform in comparison to LCRA TSC's requirement, which states, "for protective relaying, the longest route shall have a latency not to exceed 15 ms" [3].

Another component of the relay communication test setup was the power system simulators. These devices provided the ability to connect the required power system fault quantities (three-phase voltage and three-phase current sources) into both relays. These devices simulated the system faults at a specified time using GPS synchronization via an IRIG-B connection from the aforementioned GPS clock. To ensure proper operation of the LCD and DCB schemes, both relays must see their respective faults at the same time (on the microsecond level). Without GPS synchronized fault equipment, a power system fault cannot be simulated effectively to verify proper relay operation over the IP/MPLS network.

## VIII. Test Cases – Relay Testing over IP/MPLS

Fault simulations files were developed for testing the line relays over the IP/MPLS network. The 2016 ERCOT short circuit case model was used to produce five sets of the following fault types:

1. Phase to Ground Fault: A-G
2. Phase to Phase Fault: AB
3. Phase to Phase to Ground Fault: AB-G
4. Three-Phase Fault: ABC

Three sets of internal faults were simulated at 10%, 50%, and 90% of the protected line and at 10% behind each line terminal. See Fig. 7.

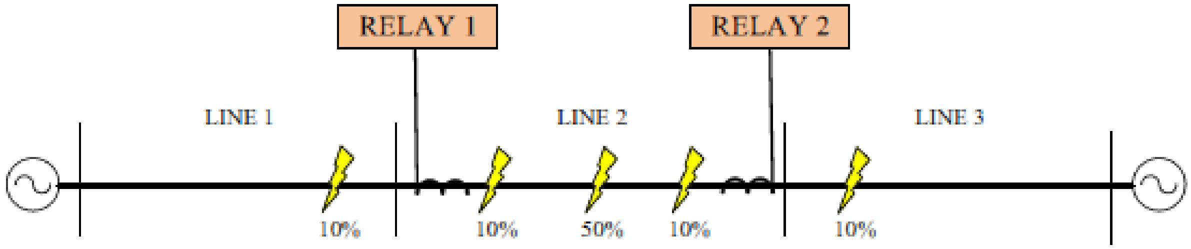

Figure 7. Fault Locations

The GPS synchronized fault simulations were performed on the following relaying schemes:

1. LCD with IEEE C37.94 Optical Interface
2. LCD with EIA-422 Serial Interface
3. DCB with EIA-232 Serial Interface

Each of the relaying schemes traversed the following IP/MPLS networks below. Details on the different networks are described in Section V. In addition, a direct path or back-to-back connection was established between relays to obtain the base operating times for each relay scheme.

1. Short Path: Single-Vendor over Fiber
2. Long Path: Single-Vendor over Fiber
3. Long Path: Multi-Vendor over Fiber

A total of 240 fault simulations were conducted to verify relay performance. Relay event reports and SER data from each fault simulation were obtained and reviewed. Analysis of the fault events found no unintended operations. The relays operated correctly for all internal faults and restrained appropriately from tripping for all external faults. In the table below are the average relay operating times for the LCD and DCB relay schemes. The operating time for the LCD relay scheme was calculated from fault inception to the assertion of the differential trip element. For the DCB scheme, the operating time was calculated from fault inception to the assertion of the block receive element. The base operating time was subtracted from these values to determine the added delay from the IP/MPLS networks.

| | **Average Relay Operating Times (ms)** | | |
|---|---|---|---|
| **Relay Schemes** | **Short Path (Single-Vendor)** | **Long Path (Single-Vendor)** | **Long Path (Multi-Vendor)** |
| LCD C37.94 | 3.8 | 6.3 | 9.2 |
| LCD EIA-422 | 1.6 | 4.3 | 4.9 |
| DCB EIA-232 | 7.8 | 9.0 | 10.8 |

Other testing included channel delays obtained from the relays. The round-trip channel delays for each relay schemes over the IP/MPLS network are shown in the table below. The base channel delay for the LCD EIA-422 was obtained with a lab-to-lab IP/MPLS node setup since the back-to-back connection was unavailable. In addition, the communication report for the DCB EIA-232 was not automatically calculated by the relay. A test was manually programmed in the relays to transmit data bits from relay to relay and the channel delay was calculated from the SER data.

| | **Average Relay Channel Round-Trip Times (ms)** | | |
|---|---|---|---|
| **Relay Schemes** | **Short Path (Single-Vendor)** | **Long Path (Single-Vendor)** | **Long Path (Multi-Vendor)** |
| LCD C37.94 | 10.7 | 11.2 | 15.1 |
| LCD EIA-422 | 6.4 | 6.8 | 10.8 |
| DCB EIA-232 | 9.0 | 15.7 | 19.7 |

Lastly, during a test on a portion of the network, a burst of traffic was injected into one of the lab nodes. This immediately triggered relay errors. This high burst of best-effort traffic competed with the protective relay data and caused the MPLS node to drop MPLS frames indiscriminately, impacting relay communications. This occurred on all rings. Further investigation will be required to isolate any QoS inconsistencies. As a quick test, an IP/MPLS node back-to-back lab test was performed with a burst of traffic to utilize all available bandwidth in a lower queue injected between lab nodes while utilizing C37.94, EIA-232, and EIA-485 communication channels simultaneously. Each relay communications channel remained error-free despite the competing bandwidth. Overall, due to limited time, bandwidth congestion was not fully tested in time for this paper authorship. Further QoS and bandwidth contention testing is planned for future testing in preparation for piloting.

## IX. Conclusion – Summary of Recommendations

We can conclude that with the proper QoS profiling & clock synchronization, IP/MPLS is capable of carrying teleprotection traffic to support LCD, and DCB relay schemes.

Throughout the testing exercise, we have observed that a proper QoS profile is key for the protective relay services. The QoS profile must reflect the criticality of protection relay traffic and be consistently applied across all MPLS nodes, including a multi-vendor network environment. This will ensure protective relay services obtain the highest priority and guarantees bandwidth end-to-end throughout the network.

It is also good practice to provide master and backup clock sources to ensure timing is propagated throughout the network in case of link or node failures. While there were no clock failures in our testing, we did notice that the initial lack of synchronization settings did cause data errors and buffering issues. Once the synchronization settings were updated, the errors and issues disappeared as all relay traffic passed properly.

Although the fast re-route feature of IP/MPLS is available to sustain a protective relay communication path, due to the latency sensitive nature, LCRA TSC plans to let the relay decide on the reliable communications channel while utilizing direct fiber on the primary channel. The speed of IP/MPLS allows us to transmit data with low latency of over 16 IP/MPLS nodes. LCRA TSC expects to achieve even lower latency when testing with a lower number of nodes. Due to limited time, we were not able to utilize any network management features to test end-to-end service latency assurance as planned, but we are optimistic it will help with planning future IP/MPLS services for protective relaying. With plans to implement a protective relaying pilot test, LCRA TSC will look forward to validating results and deploy protective relaying over IP/MPLS networks.

## X. REFERENCES

[1] IEEE 1588-2008 – Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

[2] Test Report - Teleprotection over IP/MPLS Networks, Isometric 2011

[3] Telecommunications System Performance and Expansion Criteria Rev. C, Lower Colorado River Authority, 2016

## XI. BIOGRAPHIES

**Michael A. Nunez** received his BS in Electrical Engineering from the University of Texas at Austin in 2000. He is a licensed professional engineer (PE) in the state of Texas and currently is a Senior Engineer at the Lower Colorado River Authority (LCRA) in Austin, Texas. His work experience includes cellular network RF & application validation and telecommunications design for substation and enterprise applications including network, fiber, and microwave design.

**James Denman** graduated with an AAS in Electronics from Texas State Technical College in Waco, Texas in 1997. He has 4 years of experience as a relay technician commissioning substation protection equipment and 14 years of experience operating telecommunication networks. His work experience includes turning up networks from the initial installation to daily operations of SONET, DWDM and IP/MPLS routed networks. He is currently working on network certifications with Nokia, NRS I completed.

**Joey B. Melton Jr** graduated with an AAS in Electrical Systems from Texas State Technical College in Waco, Texas in August of 1999. He was hired by LCRA-TSC as a Relay Technician I in August of 1999. Currently he holds the position of Lead Technician in the System Protection and Control group. His work experience includes construction, testing, and commissioning of substation protection equipment.

**Genardo T. Corpuz** received his BSE in Electrical Engineering from the University of Texas at, Austin in 2005. He is a licensed professional engineer (PE) in the state of Texas and currently works at the Lower Colorado River Authority (LCRA) in Austin, Texas. His work experience includes substation design and system protection.

**Hansen Chan** is an IP routing and transport product-marketing manager at Nokia with a special focus on the industries segment. He has more than 25 years of network consulting and product management experience in the telecommunications industry and is a frequent speaker at international industry conferences.

**Ivan Schonwald** started his career with a Silicon Valley startup more than 20 years ago at Ungermann-Bass, a Pioneer of Ethernet technology for the Local and Wide Area Network. He ended up at Alcatel-Lucent through four acquisitions responsible for architecting the evolution technology path for both the wireless and wireline major services providers. Ivan has also led Bell Labs on new technology start-ups responsible for the Americas and most recently moved his focused to the utility/oil & gas sector, architecting and consulting on designing mission critical networks.