Employing Packet Switched Networks for Critical Teleprotection Applications

Tim Phillippe, Ilia Voloh - GE Grid Solutions, LLC

I. Introduction

Protective Relaying has a long history of incorporating communications into various relaying schemes, particularly High Voltage Line protection. As the complexity of the protection schemes evolved, so did the sophistication of and reliance on the communications link. In many utilities, the requirement for communications for the protection application was what justified the deployment of a private Operations Technology (OT) network, which, over time, developed to include other operations applications, such as SCADA, substation voice and security. These networks have evolved to be the central nervous system of the utility. Traditionally, these networks were based on Time Division Multiplexing (TDM) circuit switched technology, such as T1/E1 and SONET/SDH, as these technologies are particularly well suited for the high voltage line protection applications, as well as for traditional serially connected SCADA RTUs.

Lead by the telecommunications industry, today's utility communications networks are experiencing a migration from circuit switched networks to packet switched networks (PSNs). In fact, within the telecommunications industry, this migration is largely completed. The transition, however, is also taking place in utility private fiber optic networks. The PSN technology is intended to leverage the efficiencies of an all packet technology understanding that today's field devices incorporating IP, or other packet interfaces is evolving to include Voice, Video Cameras, RTUs, and other traditional utility IEDs. An all PSN also lends itself for further convergence of the IP centric Information Technologies (IT) network with the OT network.

The suitability of an all PSN to support the growing IP centric applications, such as IT, IP Video cameras, VoIP, SCADA RTUs and other utility IEDs, cannot be argued. However, when addressing the communications requirements of high voltage line protection, generally deemed the most critical application to be carried over a utility private network, special caution is required. We know from experience that the stringent requirements of these services is met by the robust deterministic behavior of the legacy TDM/ SONET networks. We need to be careful that the critical teleprotection communications can be adequately serviced over an all PSN network.

II. Line Protection Communications

The early "Silent Sentinels" were assisted with command transfers, typically over a dedicated link, such as leased or private 4-wire copper lines, or single function power-line carrier. Early electro-mechanical current differential schemes relied on physical copper connections. As the electro-mechanical protection devices evolved to static electronic and eventually all digital IEDs, so did the communications interface, and ultimately the communications channel.

Generally, these protection communications are broken into two types, from a communications point of view, two state and encoded schemes:

-Two State schemes are protection schemes whose input to the communication system represents one of two logic conditions (e.g. on/off for DCB, guard/trip for POTT, etc.). There is no analog or encoded data.

-Encoded Data schemes are protection schemes whose input to the communications system represents some type of time-sensitive, encoded information (e.g. current differential).

Both of these schemes demand various operating parameters of the communications system. However, the critical communications requirements for any protection channel will vary greatly depending upon the asset being protected, its location within the power grid, as well as influence on the stability of the power grid among others. For Two State schemes, the critical communications requirements are typically channel availability, security, dependability and channel latency. The influence of channel delay is fundamental to any protection scheme, as it is a component of the over-all clearing time of the power circuit breaker. However, different types of relaying schemes react differently to channel delays. The most forgiving, are typically distance schemes utilizing permissive or blocking logic, which does not inherently depend upon channel delay in their operations. Utilizing this logic, these schemes often tolerate up to 12 ms of channel delay., often tolerating up to 12 ms of channel delay.

Channel delay is a critical portion of the overall clearing time of a high voltage line fault, as shown in Figure 1. This channel delay is typically made up of three components: ingress and egress processing at the terminal nodes, throughput delay for any intermediate nodes in a network, and fiber cable delay. The ingress and egress processing delay is specific to the relay interface used (i.e. C37.94, wetted contact closure) and the specifications of the communications vendor being used. The throughput delay is specific to the number of hops the relay channel transmits over the network, as well as the specifications of the communications vendor being used. In large networks, the delay caused by the light traveling in the fiber cable must also be accounted for. Typical 1300nm single mode glass fiber has a refractive index of 1.4677, that yields a signal propagation delay of approximately 8 micro-seconds per mile.

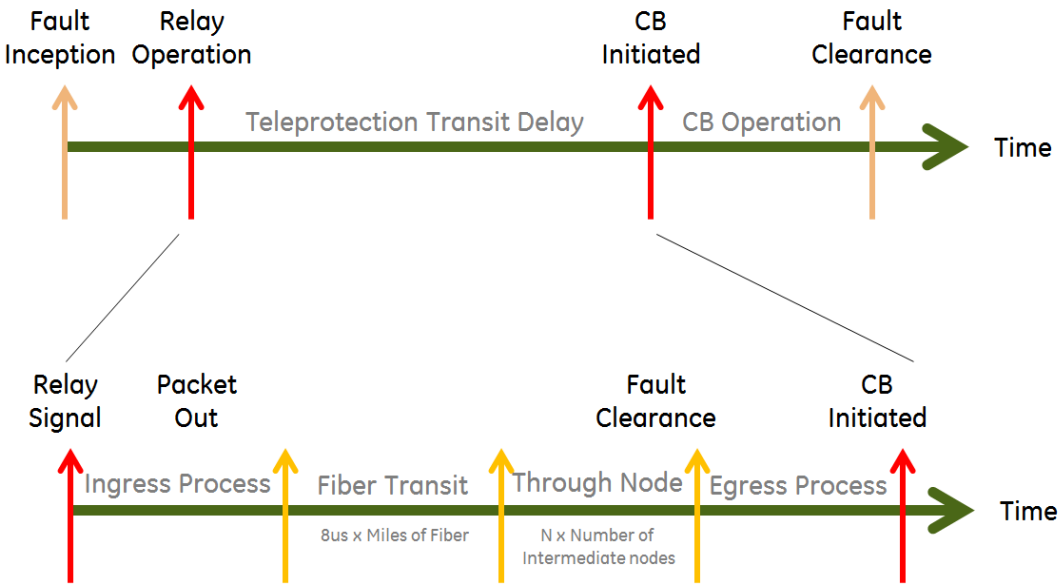

Figure 1. Channel Delay Components

For line differential protection, on the other hand, the influence of channel performance is far more profound, in part due to the higher information content being transmitted. Line differential schemes require the streaming bi-directional transmission of the measured quantities of line currebt, both in amplitude and phase. The values being sent are not a change of state, as for command systems, but represent the measured analogue values of an electrical quantity at one terminal for the purpose of comparing amplitude and phase angle between the two terminals of the line being protected. In current

differential relaying, the communications is a fundamental element of the overall protection scheme, and the performance of the channel is critical to the performance of the relaying scheme. Overall channel latency needs to be kept to a minimum as in the command schemes, as it adds to the overall fault clearing time. However, it is not just the over-all delay that is important, but the asymmetry of the channel delay can have a significant impact on the operating characteristics of the schemes.

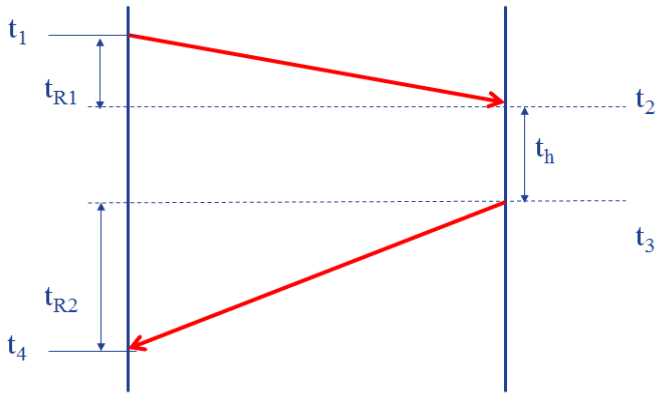

Figure 2. Channel Delay Measurement Using Ping-Pong

Current differential channels are bi-directional. Most digital current differential relay designs measure the channel delay and compensate for it. The prevalent method of channel delay estimation uses a ping-pong measurement. One end sends out a special message that is echoed back from the remote end. The loop time (less the turn-around) time is divided by two to calculate the one-way delay, as shown in Figure 2.

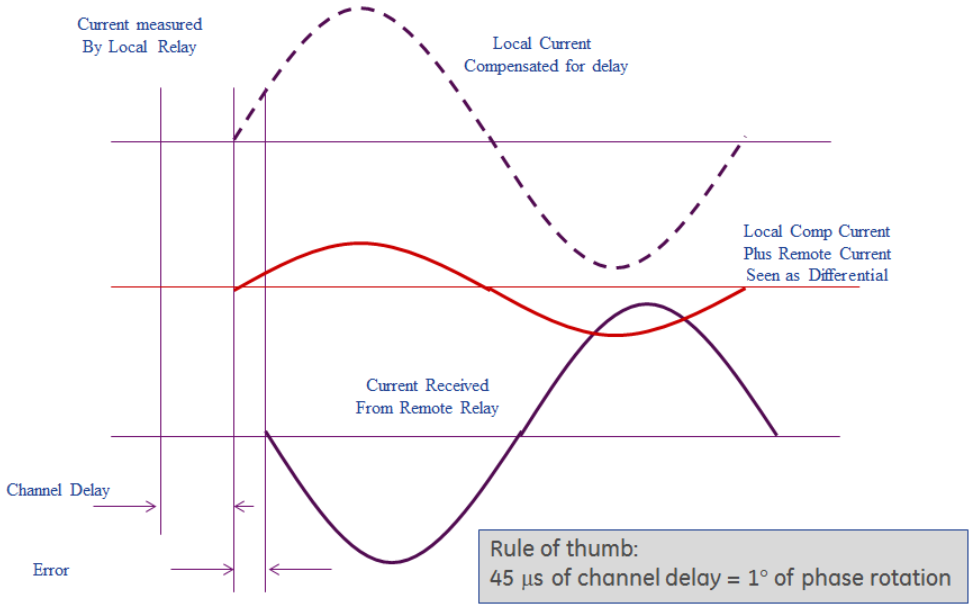

Figure 3. Impact of Asymmetrical Delay

When there is asymmetry in the channel delay, such that the channel delay differs in the direction from terminal 1 to terminal 2 than the channel delay in the direction from terminal 2 to terminal 1, the calculation of channel time off-set to apply to the measurement datagram for current comparison is incorrect. This can result in a false differential being detected, desensitizing the relay, or perhaps causing

a false trip to occur. For reference, every 45 microseconds of error results in 1^0 of phase error, as shown in Figure 3.

Figure 4 shows various options for transmitting teleprotection signals between remote line protection relays. One set of options to choose from is the physical layer, copper cable, wireless, fiber optic cable, or even the high voltage line itself. Additional determinations include whether the channel is shared or dedicated, as well as the behavior of the channel (i.e. audio tones, serial, 64 kbps, circulating current). The choice of these blocks often was a complex choice weighing the communications media available, the cost and the overall relaying scheme's bias toward dependability or security.

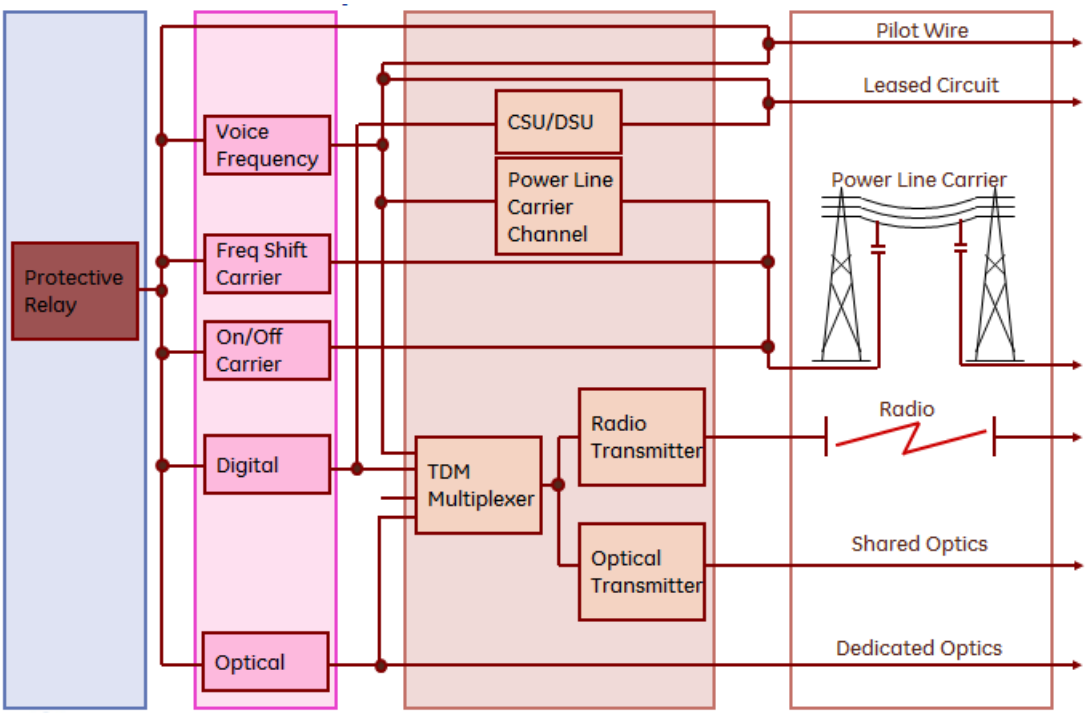

Figure 4. Traditional protective relaying communications blocks

Over the decades, with Telco companies abandoning leased copper connections into substations, dedicated fiber becoming more economically unfeasible and additional OT traffic requirements growing, many utilities began deploying private operational networks to meet their communications needs. With the explosive growth in IEDs, security video traffic and sophisticated business IP services and applications, there is a growing desire for these private networks to evolve to pure PSN technology. It is imperative that the network designer understand this technology, and be comfortable with it to support the utility- specific services requirements.

III. Packet Switched Networks

PSN technology is fundamentally different than TDM technology. The time division of Time Division Multiplexing dictates that for every circuit in a TDM network, there is a guaranteed circuit, with a guaranteed connection with guaranteed bandwidth. PSN technology, on the other hand, is based on statistical multiplexing. In its purest form, with statistical multiplexing, a packet is inserted into a network element which sends the packet along based upon "best effort." However, PSN technology has evolved significantly from the simple LANs for which PSN that the technology was initially developed to be able to better handle the packet collisions and congestion that might be expected in a large utility wide OT or IT/OT converged network.

A. MPLS

One of the widest deployed technologies in the telecommunications industry, and gaining acceptance for utility networks, is Multi-Protocol Label Switching (MPLS). MPLS was designed for high-performance data centric telecommunications networks that direct packets from one node element to the next based on a short outer label, inserted by the network, rather than a long network address. As the work "Multiprotocol" implies, a wide suite of network protocols can be encapsulated within MPLS packets. The access technologies supported by MPLS include T1/E1, Ethernet, ATM, Frame Relay, and DSL. When properly configured, MPLS presents itself essentially as a collection of "Virtual" Switches and Routers presented on a "Real" Layer 3 Infrastructure, such that every defined service perceives the MPLS architecture as a single Layer 2 Switch or Layer 3 Router dedicated to its use. There is no concern for VLAN or IP address/reputability conflict.

For services transmitted over an MPLS network, Label Switched Paths (LSP)s are first established The LSP is a path through an MPLS network, either manually configured or set up by a signaling protocol, providing connectivity between the switches and routers in the network. Pseudo wires (PW) are defined to connect services in switches and routers to the LSPs, providing connectivity between the end points of the service. The services utilizing these paths can be Layer 2, Layer 3 or emulated TDM services, as shown in Figure 5. A service enters the MPLS network at a label edge router (LER), where the data packets are assigned labels identifying both the PW and LSP to be used to forward the packet to the intended remote end point of the service. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself, and are based upon the specific label-switched path (LSP) rules. The LER makes a decision on what labels (PW + LSP) to prefix to a packet. It then forwards the packet along to the adjacent node in the path. The adjacent node, a label switch router (LSR), swaps the packet's outer (LSP) label for another label, and forwards it to the next node, again based upon predefined LSP associated with the service. The last node in the path, again a LER, removes the (LSP) label from the packet and forwards the packet to the correct service based on the next inner (PW) label.

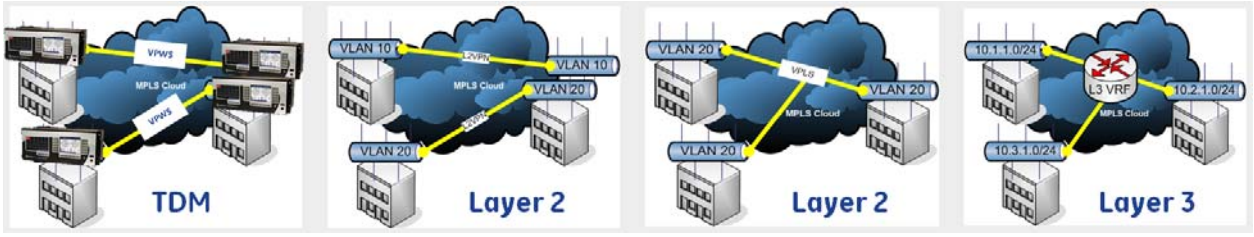

Figure 5. Services carried over MPLS Network

Services transported over the Utility network can range from full Layer 3 data communications, Multi-point Layer 2 data communications, point-to-point Layer 2 data communications, and point-to- point emulated (packetized) TDM streaming services.

Virtual Routing and Forwarding (VRF) describes the technology used to allow multiple instances of Layer 3 (IP Routing) that can to co-exist within the physical MPLS infrastructure. Because the routing instances are independent, multiple virtual routing networks can be implemented without conflicting with each other. Individual Layer 3 instances essentially look like a large Layer 3 router. The MPLS cloud provides the routing functionality between the defined end-points. Within each MPLS VRF service, advanced routing protocols can be enabled, so that the MPLS routing functionality can interact with local routing protocols running at the local sites.

Virtual Private LAN Service (VPLS) describes the technology used to allow multiple instances of Layer 2 (switching) that co-exist within the physical MPLS infrastructure. The switching instances are separate and they do not conflict with each other. Each instance provides multipoint-to-multipoint service connectivity between endpoints, acting like a large layer 2 switch with the MPLS cloud providing the switch functionality. In a VPLS, the LAN at each site is extended to the edge of the MPLS network, which emulates a switch to connect all remote LANs, creating a single distributed bridged LAN.

Where full multipoint-to-multipoint connectivity is not required, simple point-to-point Layer 2 connectivity can be accomplished by establishing a Layer 2 Virtual Private network (L2VPN). The L2VPN is easier to construct and manage, as it does not require the full mesh connectivity of the VPLS.

For emulated streaming TDM services, two common formats exist: Circuit Emulation Service over Packet Switched Network (CESoPSN) and Structure Agnostic TDM over Packet (SAToP). CESoPSN adapts the TDM frame to a packet stream while maintaining the payload organization. This allows for individual DS0 data to be visible to intermediate nodes, to be tracked and mapped as it crossed the packet network. SAToP adapts the entire TDM frame to packet, agnostic to the individual DS0 payload within. SAToP assumes the entire TDM frame will be reassembled for playback at the destination (i.e. a complete T1 or E1 frame)

B. IP/MPLS

In an IP/MPLS network, a high degree of flexibility and dynamic routing capability exists. To accomplish this, the IP/MPLS network requires complete system wide knowledge of the network, which involves a continuous exchange of control information between all nodes in the network, or a distributed Control Plane. The distributed Control Plane, using the network intelligence along with advanced routing protocols, such as Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP) will configure PWs and LSPs required for the traffic requirements of the network. Within IP/MPLS, PWs and LSPs are built in a single direction. If bi-directional communications are required, as in current differential relaying communications, a separate PW and LSP are built both to and from the far end back to the local end. Traffic enters the IP/MPLS network at the ingress LER, where the initial MPLS labels are assigned, and the packet is then forwarded on to the next LSR in the pre-defined LSP. At each LSR, the outer label is swapped according to the LSP designation, and the packet is forwarded out the appropriate port to the ensuing LSR. At the penultimate LSR to the end of the LSP, the outer (LSP) lavel I removed, in accordance to penultimate hop popping (PHP) prior to forwarding to the LER At the LER, the (PW) label is stripped off of the data packet, and the traffic exits the network, as shown in Figure 6.

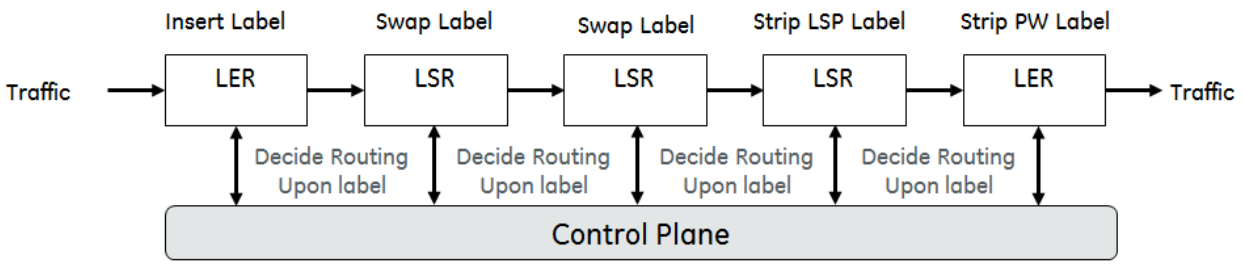

Figure 6. Label assignment and switching in an IP/MPLS Network

IP/MPLS, in its simplest form, uses no traffic engineering, but simple Priority Assignment as in native Ethernet. The most time sensitive traffic, such as differential protection circuits, will have only a better delay variation than lower priority traffic. Such a system provides traffic isolation advantages of MPLS along with dynamic routing through a distributed Control Plane; but no guarantee on resource allocation to each service without the advanced Traffic Engineering via control plane exchanges using protocols such as RSVP. It is also important to understand that this methodology for assigning LSPs is completely non-deterministic, as it is totally based on the underlying Layer 3 routing protocols. If parameters within the network change, so does the nature of the forwarding for LDP LSPs.

The Data Plane uses the LSPs established by the routing protocols in the Control Plane to decide what to do with the packets arriving on an inbound interface; i.e. swap or remove the forwarding label and egress the packet out the proper outgoing interface. In the case of a failure of the Control Plane and the routing protocols are lost, there is a direct impact on the Data Plane's capability to forward incoming packets, affecting the performance of the network.

IP/MPLS has a well-defined suite of Operations, Administration and Management (OAM) processes and tools. These tools provide MPLS Fault, Configuration, Accounting, Provisioning and Security (FCAPS) A significant tool within the MPLS OAM is the Bi-directional Fault Detection (BFD), which is with the links between IP/MPLS nodes. The BFD provides Connectivity Check (CC), Connectivity Verification (CV), while the Generic Associated Channel (G-ACh) enables frame Loss Measurement (LM) and Delay Measurement (DM). To maintain the scalability required for IP/MPLS large scale networks, this OAM is out of band. To get measurement and performance statistics of a particular service, since within IP/MPLS the OAM is not associated with the service, one of two popular methods are used. Using a manufacturer's proprietary protocol, a parallel service is built, that approximates the same connectivity as the service being measured. This gives a good approximation of the CC, CV, DM and LM but, as the measurement packets are not guaranteed to follow the same paths or experience the same traffic management features, such as QoS, the results are not assured to accurately reflect how the target service measures against its SLA. If more accurate statistics are required, the services client can inject probes (packets), to ride along with the services traffic. This method requires additional hardware or software in the client environment, which is outside of IP/MPLS.

This technology is well suited for multi-site, large scale, ever-changing Enterprise networks, Telecommunications Providers, or utility core business (Non-operational) networks. However, is it well suited for the utility OT networks, with their requirement for tight time, determinism and utility grade Quality of Service imperatives?

C. MPLS-TP

The Transport Profile of MPLS (MPLS-TP) is a variant of the MPLS technology which is both simplified and optimized for transport-type traffic, as depicted in Figure 7. MPLS-TP shares the label-based forwarding functions of IP/MPLS and the MPLS-TP Data Plane utilizes and builds upon a subset of the MPLS Data Plane. This means that MPLS-TP must be built on the core components of MPLS and be interoperable with it. There are, however, some very specific differences that are specifically important for a utility operation, particularly teleprotection circuits.

One of the key elements of MPLS-TP is that the Control Plane must be physically separate from the Management and Data Planes. Therefore, it is possible to establish services that have no reliance on the Control Plane, which eliminates the reliance on the associated complexity of Layer 3 routing tables or control protocols. The Transport Profile allows LSPs to be set by the management plane in an approach that is similar to SONET/SDH. This centralized management allows the network operator to statically set up pre-determined end-to-end paths, as well as static pre-determined end-to-end alternate paths with very simple resource allocation. This type of service configuration is appropriate for a utility network's most critical circuits, as they are a known quantity of circuits, with well-defined end points and bandwidth requirements that rarely require adds, moves or changes. The Transport Profile also dictates that restoration of services, in times of failure, not rely on the Control Plane. This means that routing protocols are not required to restore services in times of failure, resulting in more robust and faster failure recovery.

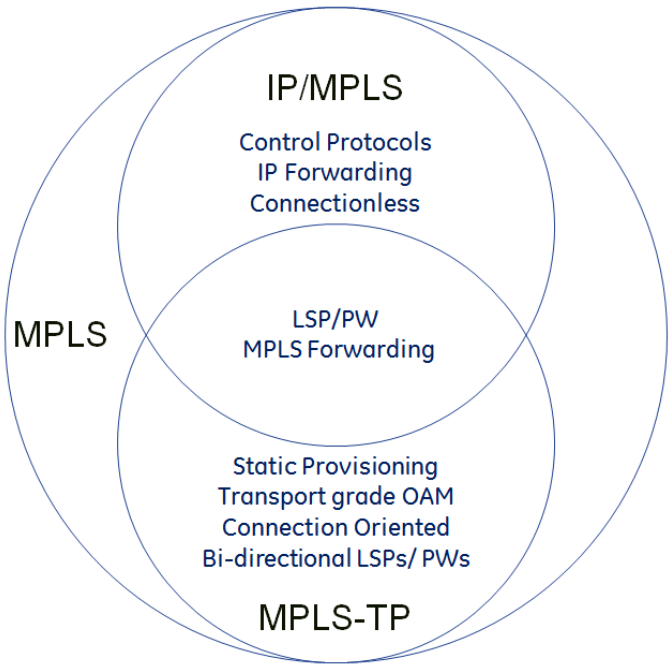

Figure 7. IP/MPLS and MPLS-TP Feature sets

To provide a more transport optimized network, the overhead Operations, Administration and Maintenance (OAM) traffic has been specifically designed to provide capabilities more like SONET/SDH OAM. The transport oriented overhead reduces the network operational complexity associated with network performance monitoring and management, fault management and protection switching. This allows the network to be operated without any IP Layer functionality. One of the primary differences in how MPLS-TP treats OAM is that the OAM traffic is associated with a specific PW or LSP, such that the OAM packets for a specific PW or LSP must follow the same exact path as the service for that PW or LSP**.** This is called "in band OAM", or "fate-sharing". One of the clear advantages of in-band OAM design is how Bi-directional Fault Detection (BFD) and Generic Associated Channel (G-Ach) are utilized. As opposed to the link based OAM of IP/MPLS, the BFD and G-Ach packets in MPLS-TP are associated with the service. This gives the network operator service connectivity verification between endpoints, as well as highly accurate delay and latency measurements. Service based BFD is used to speed any fault

detection and restoration of the end-to-end service. It should also be noted that the OAM will be uniquely associated with each PW or LSP, so that each service can be monitored and measured independently. For critical circuits, in-band OAM is also important because the OAM/ BFD can be associated with the protection path of a service as well as the primary path, so the operator will know the health and performance of the protection path even when it is not in use.

MPLS-TP is a deterministic connection-oriented packet-switching technology with traffic-engineering capabilities to support point-to-point, point-to-multipoint and multipoint-to-multipoint transport paths. In IP/MPLS, there is no guaranteed determinism on where packets will flow as they are affected by the dynamic state of the network at any one point in time. The capability for IP/MPLS to build LSPs across multiple links allowing the use of Equal Cost Multipoint (ECMP) and Weighted Round Robin is not deterministic, as there is no way to know which path, or which link, is being used for any given packet within that service which is not allowed in MPLS-TP. Guaranteed determinism of packet flow is particularly important when transporting emulated TDM circuits; DS0 (64kbps), T1 (1.5Mbps) or E1 (2Mbps), which is required for most critical teleprotection services. In order to re-build and re-frame the TDM service at the egress point of the PSN a jitter buffer is required to allow for the variable time it takes packets to transit the network. If there are multiple paths allowed for packets of a service to transit the network, the variability of the packet latency can be significant. The size of the jitter buffer must be sized to accommodate the overall variance of the packet latency. A large buffer allows for the absorption of a large delay variation at the cost of a large absolute delay of the TDM service. It is therefore essential to control delay variation in the packet network if it is to be used to emulate circuits for time critical circuits, and the path determinism of MPLS-TP is a critical component of controlling this variability.

Within MPLS, LSPs are inherently unidirectional. One LSP is for transmit between the two end points and a second independent LSP is for receive. MPLS-TP introduces the concept of bidirectional paths, which associates the transmit LSP and the receive LSPs to each other. With IP/MPLS, the Tx LSP and the Rx LSP are conceived and configured independently, with no guarantee that they will traverse the same physical links and nodes. With no Tx/Rx association packets could transit across the PSN on completely different paths, experiencing different channel delay. MPLS-TP allows bidirectional LSPs (Tunnels) to be defined using identical paths (Bidirectional CoRouted) or diverse paths (Bidirectional Associated). The Tx & Rx association of Bidirectional CoRouted, provided by MPLS-TP ensures that delay symmetry is maintained. Eliminating symmetrical delay is essential for applications (i.e. operational protection and control traffic) that can be sensitive to asymmetrical delays.

Although MPLS-TP was designed for Telecom Operators as a means of service assurance and measurement in strategic areas of their networks, it's use for end-customer (access aggregation) parts of the telecom network is limited due to the very large numbers of end points and services encountered in the public networks. However, in this context, it is the more appropriate technology for the utility traffic containing mission critical, performance sensitive traffic.

IV. TESTING

A. Test Objective

The objective of this test plan is to verify the performance of line current differential protection relays over an MPLS-TP communications network. Both protective relays and MPLS-TP diagnostics are used to monitor the channel performance, such as CRC fail, lost packet, PFLL fail and channel switching or fail. The data recorded in relays are used to determine the performance scheme and effect of channel status.

The test results shall include (1) the effect of channel on 87L (line current differential) performance, and (2) the channel statistical data. The primary objective is to verify security and dependability of the line current differential relay over an MPLS-TP communications network during line internal and external faults with or without channel impairments.

Measuring performance with a healthy comm's channel and artificially AFFECTING the channel are the primary objective of this test plan. Specific to the MPLS-TP network, the following performance characteristics will be monitored

- 87L channel latency (1-hop, 7-hops, asymmetrical)
- Asymmetry
- Jitter (variability in delay)
- Accumulated CRC errors, packet loss (measured availability), channel failure, relays re-synchronization
- Line current differential operate time for the line faults (dependability)
- Line differential restrain during external faults (security)

A broad set of disturbances will be introduced in an attempt to measure the differentials recorded by the relay.

Test Disturbances (test scenarios)

- Noise interference (Introduce random Bit Errors)
- Channel interruptions affecting the primary communications paths.
- Errors (Inject and recover) with duration: 50ms, 100ms, 1 s.
- MPLS-TP network synchronization
- MPLS-TP network congestions
- Measured asymmetry (during single-fiber break, categorize asymmetric avoidance)
- Over-allocation (flood client services affecting H/M/L Traffic classes)
- Scaling up (expanding the network by adding nodes, via optical loops)

B. Test Set up

Figure 8 shows a current differential scheme between two MPLS-TP routers. The primary path between the two substation LERs (MPLS-TP Node 1 and Node 2) is a 1-hop 10 G link, and the backup path between the two substation LERs is 7 hops at 10G through 6 LSRs (MPLS-TP Nodes 3 through 7). The current differential line relays Relay-1 and Relay-2 are connected their LERs respectively via a G.703 64kbps electrical link. A protection test set is used to energize the three-phase CT inputs of the relays

with secondary current, as well as to simulate line faults. The breaker signal from Relay-1 is fed back to the analog input to the protection test set for time measurement purposes.

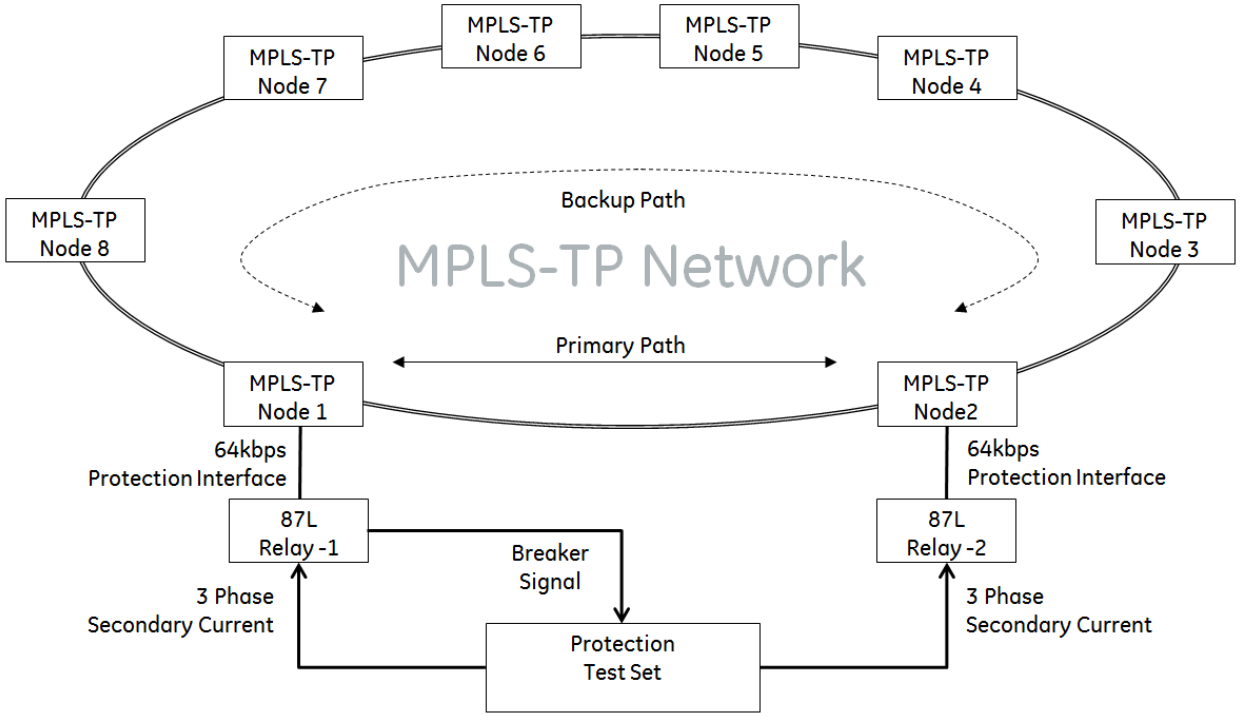

Figure 8. MPLS Network Carrying 87L traffic Test Setup

In the test set-up, the relays are connected to the LER by an electrical G.703 64kpbs connection. This PDH signal is packetized by the LER, and then mapped to a PW. The PW is then configured to be carried over a dedicated LSP between the two edge LERs. All configurations are accomplished utilizing the static configuration capability of the Transport Profile of MPLS, as shown n Figure 9.

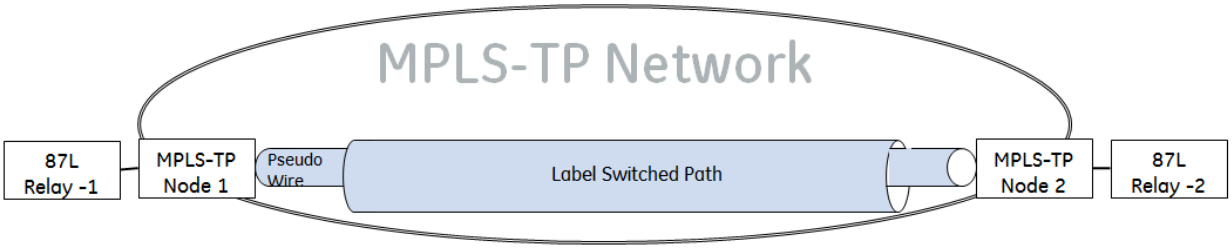

Figure 9. Circuit Emulation over MPLS-TP for 64kpbs channel

For dependability tests the line current differential operating point was just 10% within operate characteristics (internal line fault), while for security tests the line current differential operating point was just 10% outside operate characteristics (external fault). This means that for line internal faults relays have to operate 100% within published time with small margin, while for line external faults relays have to restrain 100% during all channel impairments.

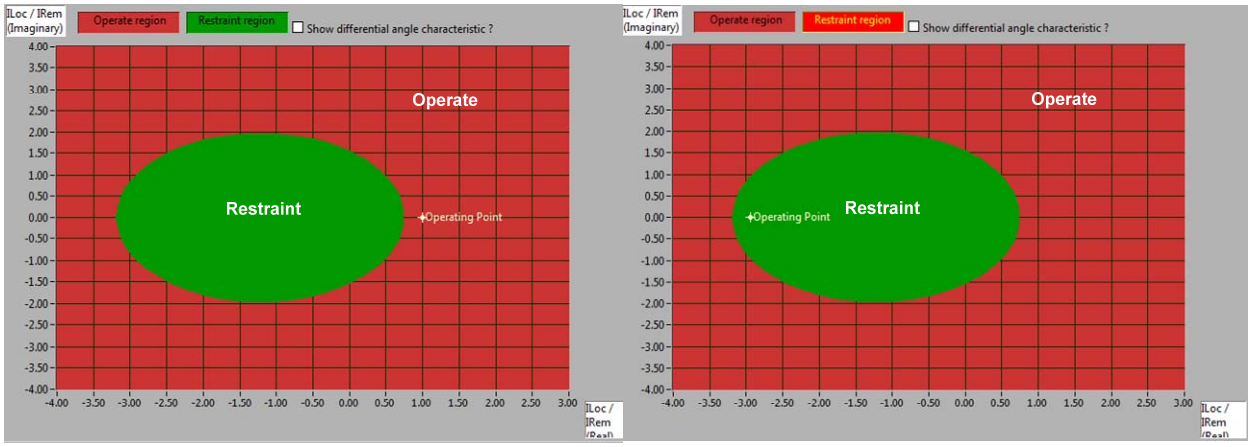

Figure 10. Security and dependability tests line differential operate and restraint points

C. Test Benchmark

In order to determine a baseline for channel characteristics for evaluating the current differential communications channel, following benchmark tests were performed:

- Healthy channel round trip delay measurement.
- Line differential operate time measurement for internal line fault
- Verify absence of 87L channel impairments, such as packets loss or corruption, no asymmetry, no channel failures for a long observation time.

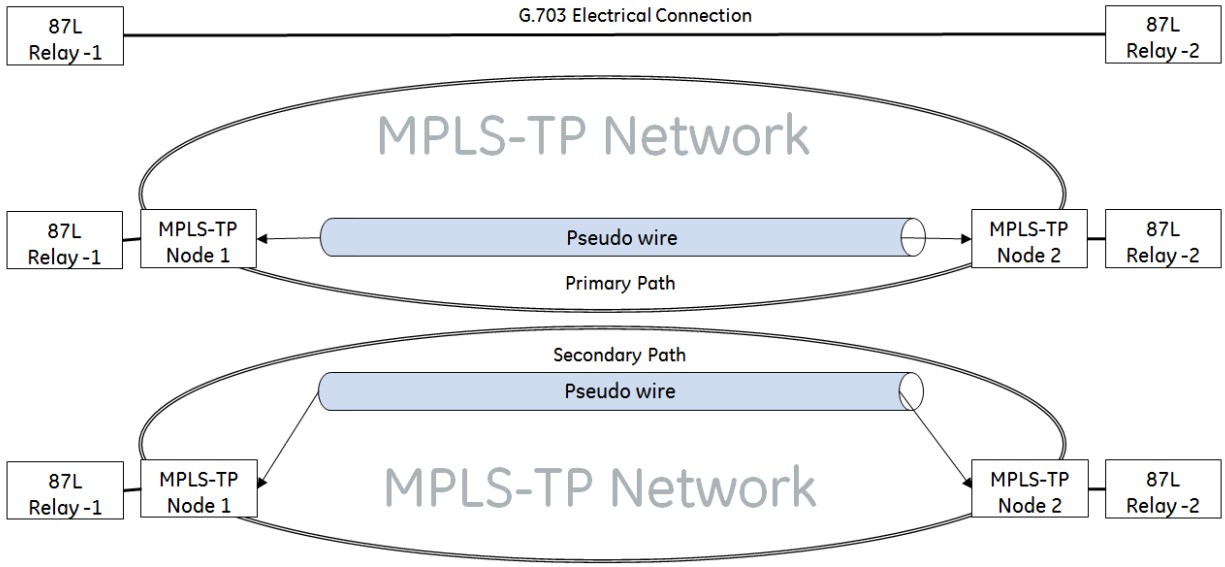

Figure 11. Benchmark tests arrangement

D. Results

- **Latency tests** were carried out to observe the effect of the short-long-asymmetrical communications paths on the line current differential performance. For each communications path there were 5 tests performed with a operate time averaged.

Table 1. Latency measurement tests

Test	Round Trip Delay	Asymmetry	Lost/Corrupted Packets	Channel Fail, Loss of 87L synch	Trip Time (average of 5 shots)	Pass/Fail
Relay channel delay back-back	9.5ms	0ms	No	No	N/A	Pass
Relay end-end delay over G.703 normal path	14.9	0ms	No	No	N/A	Pass
Relay trip time over G.703 normal path	14.9	0ms	No	No	18.5ms	Pass
Relay trip time over G.703 single fiber break	15.1	0.2ms	No	No	19.5ms	Pass
Relay trip time over G.703 dual fiber break	15.3	0ms	No	No	20.0ms	Pass

All tests yielded positive results with a major conclusion that MPLS-TP network gives only 0.2ms channel asymmetry for the 7 hops↔1 hop asymmetrical path. This is an important positive MPLS-TP channel performance for the line current differential.

- **Primary fiber break and restoration** were carried out to first measure effect on the line current differential performance by monitoring packets loss, CRC failures, asymmetry, channel failures and secondly to verify relay dependability and security, if fiber breaks happen during internal or external faults. There were carried out 15 tests for single primary fiber breaker and dual primary fiber break in both direction at Nodes 1 and 2.

Table 2. Dual primary fibers break impact on 87L availability

Test #	Break				Restore			
	Packets Lost	Errors			Packets Lost	Errors		
		LOST	CRC	ASYM		LOST	CRC	ASYM
1	2				1			
2	1				2			
3	2	x			2			
4	2				2			
6	1				2			
7	1				2			
8	2	x			2			
9	1				3	x	x	

10	1				2			
11	2				2			x
12	2	x			2			
13	2	x			3			x x x
14	2			x	1			
15	1				2			

As expected, fiber breaks are causing all 87L impairments. The faster the fiber connection is broken/restored, the less 87L packets are lost

- **Network traffic congestions** were carried out to measure effect on the line current differential performance when network traffic is high. There were tested different network frame sizes 64 (minimum), 128, 256, 1815 (maximum) bytes with a different line congestions rates varying from 0% to 100%. All tests were performed in the presences of the external or internal faults to verify line differential security and dependability during these conditions.

  Packets loss was observed in the network explorer, while relays diagnostics was used to monitor 87L channel performance and correct operation of the line current differential. Line current differential traffic was set as the highest priority; injected traffic was set to a lower priority.

Table 3. 128 bytes frame size with

Line Rate	Packet Loss in 87L diagnostic (Packet/sec)	Packet Loss % in Network Explorer	87L Loop Delay (in ms)	87L Trip Time Delay (in ms)
86.047%	0.050	1.435%	14.9ms	14.845ms
90.244%	1.533	6.232%	15.9ms	19.259ms
94.872%	3.483	11.295%	15.9ms	23.434ms
100%	4.300	16.147%	15.9ms	21.614ms

Traffic congestions tests are considered one of most importance because they would address the major concern of the protection engineers to provide secure and deterministic communications channel for the line primary protection, which is line current differential. These tests allowed us to come to the following important conclusions:

1) 87L channel loop delay stays consistent for ‘low’ congestions but jumps around +1ms in ‘higher’ congestions. Oversubscribing ports and injecting maximum traffic does not affect Trip Time Delay
2) Higher congestions may cause occasional packets loss, which may slightly delay (1/2 cycles) differential operation.
3) It is important to set 87L traffic to then highest priority – setting it to normal priority is causing packets loss at the higher rate.
4) Higher frame sizes and higher traffic is not causing CRC fail, this is important for 87L security that no excessive data corruption generated in the MPLS-TP network.

There were 15 tests generated at nodes 1 and 2 both directions for bot external and internal faults for each frame size with a 960 total number of tests. It demonstrated high degree of security and dependability for the 87L application over packet switched network.

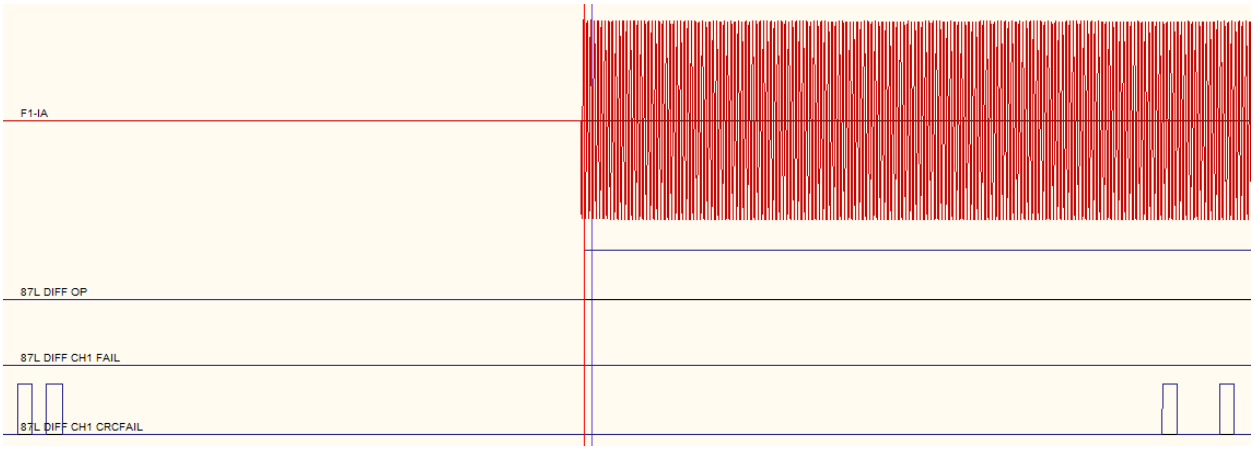

Figure 12. Line differential operation in the presence of noise

V. CONCLUSIONS

Telecommunications industry is rapidly migrating from circuit switched networks to packet switched networks (PSNs). The PSN technology is intended to leverage the efficiencies of an all packet technology understanding that today's field devices incorporating IP, or other packet interfaces is growing, such as Voice, Video Cameras, RTUs, and other traditional utility services.

Critical teleprotection applications have special requirements and need special attention, because they ensure power grid reliability and stability. These requirements are;

- minimum and stable channel delay
- highest priority designation for the teleprotection applications
- minimum or no channel asymmetry
- paths redundancy
- low jitter, typically less than 200µs
- fast paths switching in the case of the primary fiber failure or hardware failure
- minimum data corruption as a result of the switching or network overloading
- ensuring compatibility with a legacy teleprotection terminal devices protocols and rates, G.703, RS-422, X.21, V.35, IEEE C37.94 etc

When looking at how new PSNs are able to support existing utility services, the core service architecture is the same – connection-oriented communications. The fact that the terminal devices have not changed often requires that the service interfaces cannot change either. Only the method by which communication is provided from source to destination may change. This means that if a service was a point-to-point TDM service in the TDM world, it will remain a point-to-point service in the packet environment – they continue to require connection oriented transport protocols.

Technological migration cannot be driven by supplier pressure- it must be planned and performed by the utility for enhanced operational benefits (i.e. maintaining present capability and enabling new applications). Technologies cannot be compared or assessed without knowing what we want to do with them. Therefore P&C and communications communities have to work together to educate each other and let both benefit from the new PSN technology.

Tests described above proved that MPLS-TP provides the required channel performance for the critical teleprotection applications, in most cases meeting or exceeding performance requirements, as in the legacy TDM networks. It demonstrated that security, dependability, availability, quality of service are preserved or exceeded.

Many new applications in today's environment require Ethernet connectivity such as synchrophasors, IEC61850 substation-to-substation tunneling, time synchronization via IEEE 1588 and others. It seems to be natural that all utility applications in the future will be packet based to ensure standardization, cyber security, simplification, easy migration, cost reduction, uniform maintenance and management.

Therefore it is beneficial for the legacy teleprotection applications to be migrated into new transport optimized PSN technology sooner rather than later.

VI. REFERENCES

1. GE publication GEA-31950(E) JPAX Technical Practices and Installation manual, 2016
2. GE publication GEK- 119623A, L90 Line Current Differential System- Instruction Manual, 2015.