Performance analysis of line differential protection using MPLS networks

Lifan Yang[A], Thomas Rudolph[B], Min Li[C], Motaz Elshafi[C]
[A] Schneider Electric (China) Co., Ltd., Shanghai Shi, China
[B] Schneider Electric GmbH, Dresden, Germany
[C] Cisco, Research Triangle Park, NC, USA

RESUMEN

Este trabajo valida el uso de redes IP/MPLS para cumplir los requerimientos de los esquemas de protección diferencial de líneas, y mostrar el efecto de una red IP/MPLS sobre el comportamiento del relé de protección bajo tres condiciones adversas: retardo asimétrico de canal; alta fluctuación (variación en el retardo de paquetes) y falla sobre el tiempo para cambio de carga. Se observan y registran indicadores clave de comportamiento para cada condición de prueba, incluyendo: retardo extremo-extremo, tiempo de disparo, y medida de corriente diferencial. La alineación de los datos se basa en la medición del viaje redondo de los mensajes de comunicación de los relés. Para el caso de aplicación utilizando un GPS basado en tiempo de muestreo sincronizado, la asimetría del canal no es un reto porque las mediciones tienen referencia de tiempo. Para el fin de la validación, se demuestra que los relé de protección existentes trabajan establemente sobre redes IP/MPLS bajo condiciones adversas.

PALABRAS CLAVE

Redes MPLS, esquemas de protección diferencial

ABSTRACT

This work validates the use of IP/MPLS networks to complay the requirements of digital line differential protection schemes, and shows the effect of an IP/MPLS network over the protection relay behavior under three adverse conditions: asymmetric channel latency; high jitter (packet delay variation) and failure path switchover time. For each test condition, key behavior indicators are observed and recorded, including the end-to-end delay, tripping time, and measurement of differential current. Impairment tools are used to inject an additional and artificial delay in one-direction or both directions of the path to introduce jitter. The data alignment is based on the locally measured round trip for communication messages by the relays. For the application case using a GPS-based time synchronized sampling, the channel asymmetry is not a challenging because the measurements contain absolute timestamps. By the end of the validation, it is demonstrated that existing protection relays works stably over IP/MPLS networks under adverse conditions.

KEYWORDS

MPLS network, schemes of differential protection

INTRODUCTION

Utilities, as operators of critical infrastructure, are responsible for the maintenance and control of the electrical power delivery and control equipment in the electrical grid at all times, regardless of circumstances. To achieve this goal, most distribution and transmission system operators have traditionally relied on private TDM- based solutions such as synchronous optical network (SONET) or synchronous digital hierarchy (SDH). These technologies delivered carrier-class performance, supported the deterministic traffic critical for grid operations, and were relatively straightforward for initial deployment.

However, because of system upgrades and equipment end of life, time division multiplexing (TDM) infrastructures no longer support the long-term needs of utilities. Many were built and operated for specific applications or solutions, creating soloed infrastructures that make it more challenging and complex to integrate new systems and operational processes. This inflexibility necessitates the deployment of ever more specialized overlay networks, creating a spiral of continual increasing complexity. Such overbuilt networks are highly inefficient, require a great deal of manual administration, are more challenging to troubleshoot and increase operating and maintenance costs. As a result, such environments are actually less secure and increase operational risk over time.

With the rapid development of smart grid technologies, the traditional TDM/ SDH communications transmission networks operated by electrical utilities face increasing challenges and cannot accommodate the communication and long-term evolution requirements. MPLS is a proven technology for network operators who need to support diverse legacy systems as well as modernize for next-generation applications. Enabling transparent integration of traditional and smart grid capabilities, MPLS facilitates transport of most forms of traffic.

MPLS technology implements packet switching based on open communication standards widely used by telecommunications carriers and enterprise users. The technology features greater flexibility, efficiency and security. In MPLS networks, the bandwidth is dynamically shared for different services (e. g. video, voice, and intranet). Without additional constraints, the data exchange can be flexibly routed, resulting in variable latency.

One of the most valued features of MPLS is that it allows utilities to perpetuate the use of existing TDM circuits on the same wide- area network (WAN) backbone with next-generation packet-based systems. This is achieved by running these legacy systems over an MPLS network using techniques such as circuit emulation with pseudo wire emulation edge-to-edge (PWE3). Enhanced by MPLS traffic engineering (TE) or MPLS transport profile (TP), networks can integrate virtually all forms of traffic without having to disruptively replace still-functioning older systems. This helps to unify the network management environment, making it significantly more cost-effective to administer. By running new applications alongside older systems on the same network, utilities can protect their current investment while transitioning the business to the smart grid.

Utilities have traditionally accepted SONET/SDH for its ability to deliver high-performance connectivity. By contrast, packet solutions have sometimes been characterized as “best-effort networks,” especially in situations where they are based on T1 or low-bandwidth connectivity. But this not true for well-designed

packet networks, especially not for high-speed MPLS networks designed with quality of service, traffic engineering, fault detection, and fast reroute (FRR) features.

Digital line differential protection affords one of the highest requirements for communication channels in the field of power system protection. The inherent propagation latency, jitter, and asymmetry of an IP network should have no substantive impacts on the behavior of line protection. Moreover, a modern numerical relay keeps working in extreme cases like high jitter or severe asymmetrical latency due to its self-adaptive algorithms. In this paper, the usability of MPLS networks for such applications is evaluated and the results of lab tests are presented.

TELECOMMUNICATION REQUIREMENTS FOR LINE DIFFERENTIAL PROTECTION

Latency

For channel-aided protection schemes, channel delay for transmitting protection messages should meet strict requirements. In North America, maximum of 10 ms latency budget is considered in practice for the communications portion to transport protection relay signals, independently of the distance/path.[1] In China, National Standard[2] defines that digital information one-way channel delay for transmission line teleprotection should be less than 12 ms. IEC/TR 61850-90-12[3] recommends one-way channel transmission time to be ≤ 10 ms. Communication channel delay impacts the time the protection takes to detect a fault and its tripping time.

Latency of communication network channels consists of three parts: the interface delay between relay and communication equipment (including ingress and egress buffering and processing), communications equipment network delay (network nodes forwarding) and network physical medium latency (propagation delay).

The ingress and egress buffering and processing delay depend on the type and speed of communication interface of protection relay. At the ingress of the communications channel, the communication device need to packetize these low-speed (56 kbps or n×64 kbps), synchronous messages of protection relays and transmit them onto high-speed (> 1 Gbit/s) IP communications network. At the egress, the communications device buffers and serializes the high-speed IP packets into the low-speed synchronous serial data referencing a common clock frequency shared with the ingress side. The ingress and egress latencies are generally between 2 ms and 3 ms in total.

The packet transmission latency on a communications network is the total forwarding delay caused by the communications devices that the packets pass through. MPLS packet forwarding is implemented in such a way that the latency is very small, i. e. tens of microseconds per hop.

The network physical medium latency refers particularly to the signal delay in the transmission medium. Modern power systems mostly utilize fiber optic communication networks as the backbone. The transmission delay is determined by the transmission distance, and it is also affected by fiber types, such as single-

mode or multimode fiber and wave length, etc. Based on the propagation speed of an optical signal in the optical fiber, 1 ms delay can be estimated for every 200 km (125 miles) of distance traversed.

Jitter requirements

The average value of the communication network latency is not a sufficient criterion for line differential protection. Delay variation, also called jitter or packet delay variation (PDV), expresses how much the delay can vary. This was not an issue when relays were directly interconnected and wired but it becomes important in a packet switched network (PSN) infrastructure.

Often, jitter is generated by the packet forwarding node waiting randomly for other high-priority traffic. PSN networks utilize quality of service (QoS) mechanisms, and data forwarding is based on priorities. Typically, messages from protective relays are marked as expedited forwarding (EF) which classifies packets as the highest priority. If an EF priority packet arrives while the communication device is processing an earlier packet, then the processing of that EF packet cannot start until earlier packet processing is completed. Waiting time depends on the size of the packet being processed; the larger the packet, the longer the wait time.

Jitter can impact protection behavior, and even cause unpredictable errors in protection ping-pong scheme,[4] an application sensitive to jitter. Therefore, in order to ensure consistency in differential protection performance, the requirement is that jitter must be as small as possible. IEC/TR 61850-90-1[5] defines three message performance classes, and the class TT1 (0.2 ms) providing the highest level of requirement can be used as a reference for current line differential protection.

Symmetry requirements

Line differential protection is usually based on the principle of a "ping-pong" data synchronization algorithm; a prerequisite for this algorithm is the symmetrical latency of forward and reverse paths between two ends. The data alignment for line differential application is based on the locally measured round trip for communication messages. This commonly used method results in high requirements for the communication delay symmetry. When the delay is not equal in both directions, the error introduced in case of high through currents (e. g. external fault currents) can be estimated in the following formula:

$$\delta\% = 2\sin\left(0.5\frac{0.5\Delta t f_0}{1000}\times 360^\circ\right), \quad (1)$$

in which Δt is the difference of propagation delays in ms and f_0 is the nominal system frequency. In case of $\Delta t = 1$ ms and $f_0 = 50$ Hz, a fake differential current appears at a level of 15% of through current. While the pickup current threshold is normally between 15% and 20% based on rating current, an additional asymmetrical latency between forward and reverse paths can lead to unnecessary starting or even mal-operation in case external faults occur.

Similarly, in case of internal fault, the error introduced can be estimated in the following formula:

$$\delta\% = 2\cos\left(0.5\frac{0.5\Delta t f_0}{1000} \times 360^\circ\right) - 1. \quad (2)$$

Notice that here δ% is negative which means differential current measured is smaller than true value. As a result, sensitivity of protection is degraded in this case.

In a meshed network, messages between two ends can take different paths in both directions. In packet-switched networks, MPLS traffic engineering and MPLS-TP guarantee the same path for sending and receiving relay messages In the event of a failure along the communication path, both tunnel endpoints switchover to a backup path simultaneously Proper traffic engineering will ensure that the communication paths are symmetric even in the event of primary communication path failure.

Reconfigurability requirements

Reconfigurability or re-routing is a salient feature of modern communication networks. Fiber failure is one of main reasons for a packet not being received. [5] When a fiber failure occurs, the network must detect the failure and reconfigure to a backup path rapidly, if it is available. For SDH/SONET networks, ITU-T recommends that the switchover time be less than 50 ms. For teleprotection communication systems, there is no defined specifi- cation on switchover time. IEC 60834-1 does specify, however, that the probability of a "command" not being received within 10 ms should be $< 10^{-4}$. The faster the switchover time, the lower the risk of protection relay failure to trip during a coinciding power system fault.

VALIDATION RESULTS

To assess the impact of MPLS communications on protection relay performance and to validate the interoperation of various technologies, a dedicated test bench was set up. The tests were performed using Schneider Electric Easergy MiCOM P545[6] and Cisco ASR 900.[7] In figure 1, the router network is setup with three possible paths between the Easergy MiCOM P545 relays: 1-hop path (green), 5-hop path (blue) and an 8-hop path (orange). Two MPLS-TP tunnels are defined as follows:

1. Tunnel 1 leverages the 1-hop path (green) as the working path, and the 5-hop path (blue) as the protect path.
2. Tunnel 2 leverages the 5-hop path (blue) as the working path, and the 8-hop path (orange) as the protect path.

Test scheme and system configuration

The service model for line differential protection implemented with C37.94 relay interfaces is illustrated in figure 2.

Line differential protection relays connect to the router via an optical/electrical (O/E) interface unit (P-2M-L). The relays send proprietary telegrams to exchange current vectors in terms of use for line current differential protection schemes

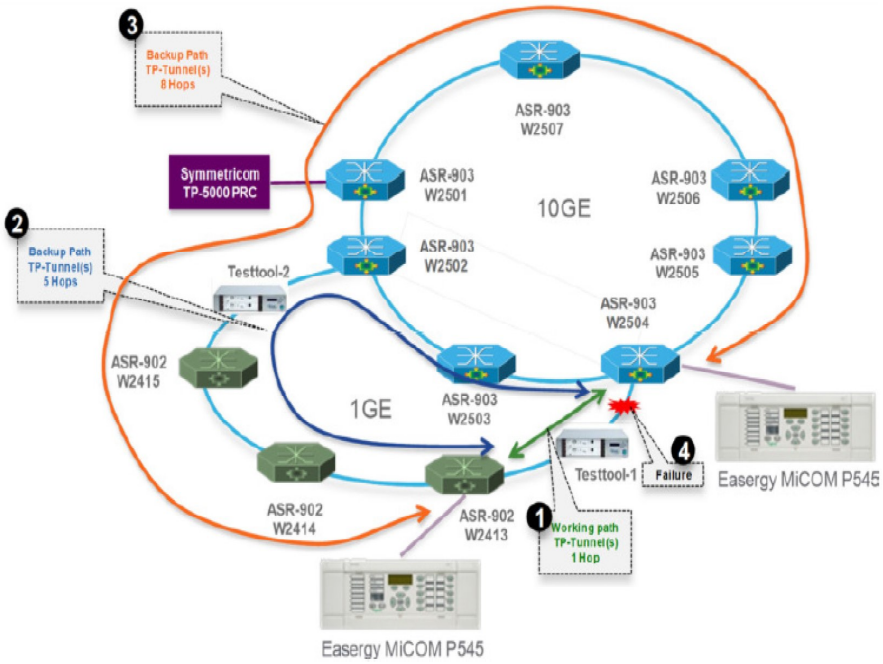

Fig. 1. Validated MPLS network topology.

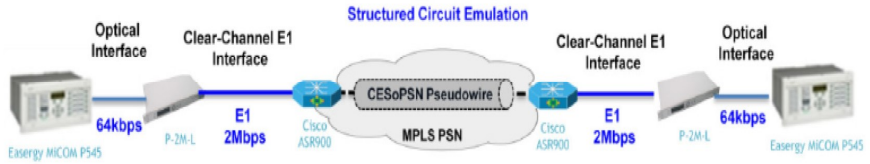

Fig. 2. Connection and service models.

over C37.94, and O/E converters packetize these telegrams into an E1 2 Mbps circuit.

The routers provide Circuit Emulation (CEM) services using TDM-based pseudowires over an MPLS network for transporting the teleprotection data between the two substations. Depending on the relay requirements, the TDM-based pseudowire can be config- ured to perform clear-channel circuits with structure-agnostic TDM over packet (SAToP) or structured circuits using circuit emulation services over packet-switched network (CESoPSN). The Cisco ASR903 router was configured for SAToP transport for P-2M-L

E1 communications. Traffic-engineered forward and reverse paths between substation routers fulfill the pathsymmetry requirement for line current differential protection schemes employing channel-based synchronization.

The substation routers support eight QoS queues per service, including two Priority Queues, and deep buffer sizes capable of accommodating highly bursty traffic in oversubscribed conditions. The TDM pseudowire is mapped to the highest priority queue (PQ1) ensuring that Teleprotection traffic experiences minimal packet delay variation (PDV) when traversing the network over the static tunnel.

High-availability with sub-50 ms recovery against failures in the transport network is supported by MPLS-TP linear path-protection with hardware-based bi-directional forwarding detection (BFD) timers when MPLS-TP tunnels are used.

Test results and analysis

Channel latency

Line differential protection devices continually monitor channel delay, and the measured results are displayed in figure 3. Each section of the figure depicts a one-way measurement calculated from the average of 250 test samples:

- Relay communication latency back-to-back over a short fiber: 2.86 ms one-way.
- Relay communication latency over a 1-hop MPLS network: 4.46 ms one-way.
- Relay communication latency over a 5-hop MPLS network: 4.47 ms one-way.
- Relay communication latency over a 8-hop MPLS network: 4.59 ms one-way.

The network delay excludes the interface delay between relays and communication equipment (2.857 ms). The network delay does include, however, the delay introduced by O/E converters P-2M-L, which is negligible (around 20 μs). The network delay increase caused by traversing more hops is not easily noticeable, and in fact, the increase is almost negligible in the 5-hop case.

Even while taking into account the network physical hediuh latency (propagation delay), and assuming signal transmission speed on an optical fiber is about 200 km/ms, (generating additional 2.5 ms delay on a distance of 500 km/310 miles), the overall channel delay easily falls within the 10 ms target.

Asymmetric channel latency

Impairment tools are used to inject a slowly increasing delay in one direction of the path. In case of internal fault, the differential currents measured become smaller than theoretical value as asymmetry increases. In figure 4a the difference of time delays of sending and receiving (X axis) increase from 0.1 to 5 ms, while the differential current deviation negatively reaches more than 6%. In another word, protection sensitivity becomes worse in this case.

In case of throughout flow or external fault, a slight asymmetry will cause a significant error of differential current. As an example figure 4b shows that a 2 ms of asymmetric delay results in the 26% error of flowing current. If the current is significant enough, the artificial differential current will cause a mal-operation.

However, modern protection relay can be immune to asymmetric latency when GPS-time stamped sampling and data alignment is enabled at all line ends. The latency of TX and RX can be estimated respectively and current vectors can be aligned correctly.

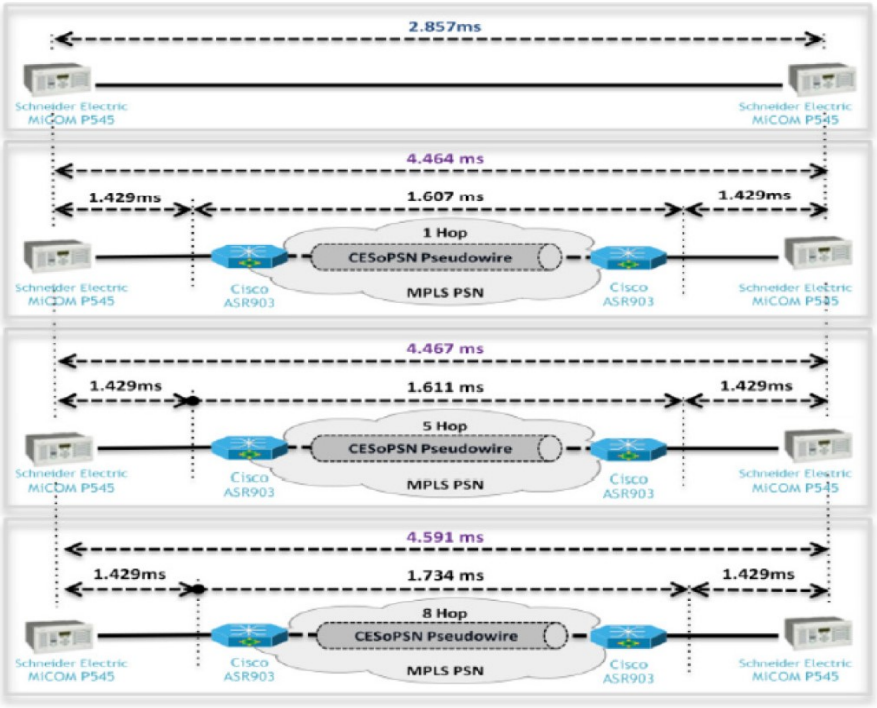

Fig. 3. Channel latencies of different paths.

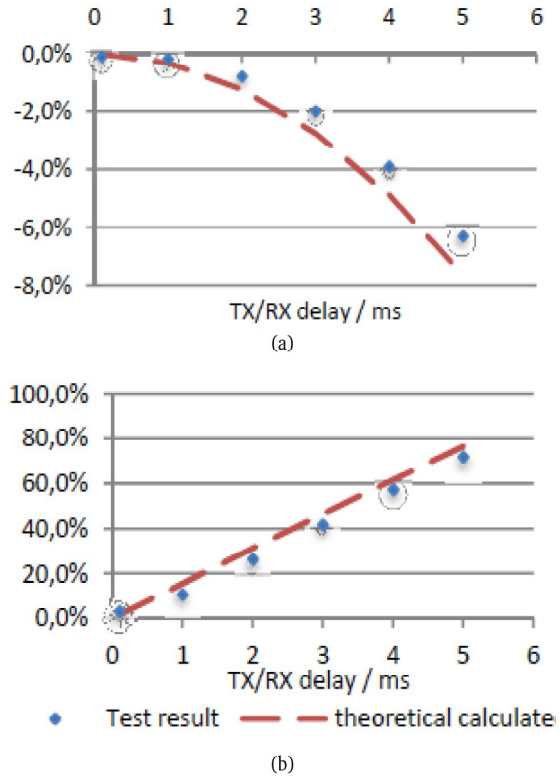

Fig. 4. Differential current deviation: (a) internal fault case, and (b) external fault case.

High jitter

A configurable de-jitter buffer is implemented on routers to compensate for the network delay variation. A larger de-jitter buffer effectively mitigates the risk of network jitter. However, increasing the de-jitter buffer also increases overall channel delay and tripping time as a side-effect.

Artificial jitter is introduced by test tool using a Gaussian model, and the jitter is applied along with a baseline delay of 3 ms. This means at an instant in time where no jitter is applied, the channel latency will increase by 3 ms when compared to channel latency results tabulated in *Channel latency*.

The applied jitter in the communication channel is observed by monitoring the channel delay variation. For each test scenario, 50 test samples of latency are recorded and statistical values are presented in the table I. The values show no obvious effect of network jitter on channel latency within certain limits when buffer mechanism works.

The average values are portrayed in figure 5. When the de-jitter buffer is set to 2 ms, protection relays start reporting error messages when the jitter increases to 350 μs; When the de-jitter buffer is set to 3 ms, protection relays start reporting error message when the jitter increases to 950 μs; When the de-jitter buffer is 5 ms, no error messages are reported by the protection relays, even when the jitter increases to 2 ms.

Failure path switchover

The primary path (green path in figure 2) for teleprotection relay (TPR) traffic is protected with MPLS-TP 1:1 protection. When the link on the primary path failed, the convergence time is measured for the emulated bi-directional TPR traffic flow. When the link on the primary path recovered, the convergence time is also measured for the emulated bi-directional TPR traffic flow. MPLS-TP is provisioned to use BFD as its detection mechanism to quickly determine link/path failure.

As shown in figure 6, the primary path is broken at T1 and recovers at T2; and repeated at T3 and T4. The channel delay change is perceived (blue curve), jump from 4.5 to 6.6 ms when primary path failure; restore when primary path recover. Two error messages (orange curve) are reported at each moment of change.

During the switchover, current is injected and make it outside of tripping zone but very close to the boundary. Obviously, differential current is calculated correctly because relay can detect the change of channel delay and use the new delay time for data alignment.

The Ixia traffic tool indicates the time changeover is 6.74 ms, which is shorter than 25 ms, the threshold of trigger degraded mode of the protection relay.

However modern line differential relays are able to master this situation. When the change of propagation time on communication channel is detected and exceeds a configurable value, the relay will upraise the threshold of differential function temporally to ensure the stability during channel switching or other abnormal conditions.

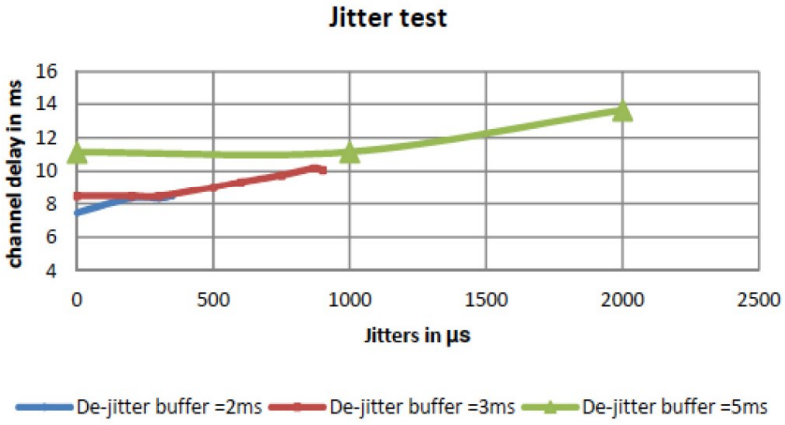

Fig. 5. Result of jitter test.

Table I. Channel latency during jitter test.

Jitter (ms)		0	0.2	0.3	0.5	0.6	0.75	0.87	0.9	1	2
De-jitter buffer = 2 ms	Max	7.55	8.41	8.42							
	Average	7.47	8.35	8.34							
	Min	7.41	8.28	8.27							
De-jitter buffer = 3 ms	Max	8.55	8.55	8.53	9.08	9.39	9.82	10.34	10.2		
	Average	8.47	8.47	8.47	9.02	9.34	9.77	10.24	10.09		
	Min	8.41	8.40	8.42	8.96	9.29	9.72	9.89	9.73		
De-jitter buffer = 5 ms	Max	11.21							10.32	11.22	13.71
	Average	11.16							10.17	11.16	13.66
	Min	11.09							9.75	11.09	13.6

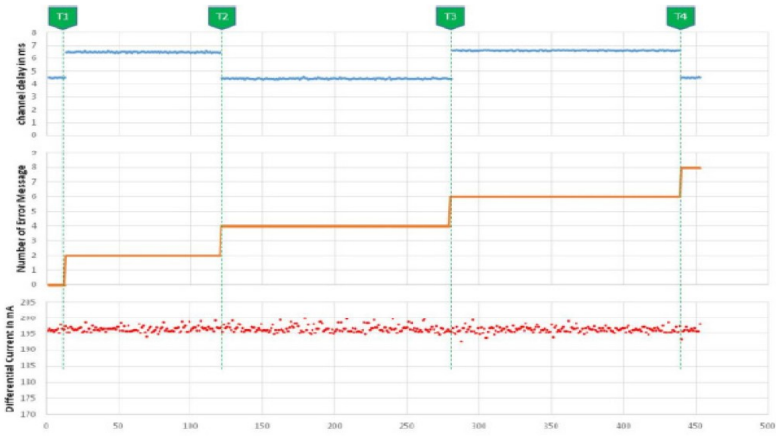

Fig. 6. Protection relay performance during path change over.

CONCLUSION AND SUGGESTIONS FOR IMPROVEMENT

Based on intense tests connecting line differential protection with MPLS networks, it could be demonstrated that critical performance requirements of line differential protection applications are met by using the excellent communication infrastructure provided by MPLS networks. Also from protection relay perspective, commercial solutions already available are suitable to be used in this kind of communication networks.

As seen from the test results presented in this paper, these main concerns from protection engineer point of view, like channel delay, traffic load, jitters and asymmetry are considered during the tests by using commercially available products and the results demonstrated a full mastering of these concerns.

As technology is continuously evolving, lifecycle management is vital. Modular approaches based on existing standards applied on protection equipment provide the benefit of supporting existing traditional teleprotection communication technologies as well as migration paths towards an MPLS based communication. From customer side, one big benefit is that the relays do not have to be changed once it is decided to migrate the communication network to the new technology. This paper will serve as a reference for using MPLS networks for line differential protection applications allowing all kind of migration strategies.

IP technology is also pushing the development of protection relay, especially protection traditional communication interface would be gradually IP-based, more efficient, more flexible, more reliable, and further enhance the overall performance of protective relay.

REFERENCES

1. S. V. Achanta, R. Bradetich, and K. Fodero, "Speed and security considerations for protection channels," Proceedings of the 42th Annual Western Protective Relay Conference, Oct. 2015.
2. GB/T 14285-2006, Technical code for relaying protection and security automatic equipment, Chinese Standard.
3. IEC/TR 61850-90-12, Communication networks and systems for power utility automation— Part 90-12: Wide Area Network Engineering Guidelines.
4. Network Protection & Automation Guide, Technical Report, Schneid-Electric, 2016
5. IEC/TR 61850-90-1, Communication networks and systems for power utility automation — Part 90-1: Use of IEC 61850 for the communica- tion between substations.
6. Easergy MiCOM P54x – User Manual, Technical Report, Schneider Electric, 2016.
7. ASR 903 data sheet, Technical Report, Cisco, 2016.