IP/MPLS and MPLS/TP Teleprotection Latencies over High Voltage Power Lines

Kinan Ghanem
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
kinan.ghanem@strath.ac.uk

Stephen Ugwuanyi
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

James Irvine
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—Power utilities dependent on communication networks to deliver critical power services continue to increase. These time-critical networks have evolved to use packet-based technologies such as Internet Protocol Multi-Protocol Label Switching (IP/MPLS) and Multi-Protocol Label Switching Transport Protocol (MPLS/TP). Both packet-based technologies are efficient traffic routing protocols for critical applications like teleprotection with challenging low propagation and asymmetrical latency requirements. This paper presents the findings of IP/MPLS and MPLS/TP hitless teleprotection applications over high voltage power lines. The performance of both technologies is compared based on specific network parameters using test equipment. The major results highlighted include base case tests of propagation and symmetrical latencies following latency injections, event response, bit error, path switching, Quality of Service (QoS), and IEC 61850 proof of concept test. While the result demonstrates that IP/MPLS and MPLS/TP - if configured properly - can meet the strictest requirements of teleprotection latencies over high voltage power lines, their performance varied across the hitless technology test metrics. These findings are not only relevant for unravelling deployment decisions between both packet-based technologies in the energy sector but are also useful for the long-term infrastructural planning of power utilities.**

Keywords—IP/MPLS, Latency, Power Lines, Smart Grid, Teleprotection, MPLS/TP, C37.94, X.21

I. INTRODUCTION

Multi-Protocol Label Switching (MPLS) is a link layer multi-path data forwarding technique which defines packet network latency, resource utilisation, Service Level Agreements (SLA), and Quality of Service (QoS) requirements. MPLS was specified by the Internet Engineering Task Force (IETF) in the 1990s [1] and standardised by the International Telecommunication Union, Telecommunication Standardisation Sector (ITU-T). It is an efficient way of routing packets with high-priority traffic that cannot tolerate latency without services being degraded below a specific SLA threshold. With MPLS, it becomes possible for telecommunication carriers to employ transport technologies to determine IP packet routes by attaching labels to the packets and forwarding the packets based on label inspection rather than the IP header. This packets forwarding technique is contrary to the legacy Synchronous Digital Hierarchy (SDH) operational principles and Synchronous Optical Networks (SONET) that are far less scalable, more expensive, and have lower coverage and capacity. These inefficiencies could be attributed to the lack of Operation, Administration, and Maintenance (OAM), fault localisation, and fast switching function during network failures. Packet-based technology performs better and can be leveraged to improve SDH and SONET performance in utility networks. As shown in Figure 1, paths for packets between network elements (teleprotection relays) are guaranteed via the edge and switching routers before transmission. The connectivity is monitored periodically for path control. The common path control investigated includes protection switching, which recovers the routes of a faulty path, alarm transfer to other network entities, and traffic engineering for dynamic path allocation of bandwidth.

Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) and Multi-Protocol Label Switching Transport Profile (MPLS/PT) network architecture shown in Figure 1 must have sufficient maintenance operation functions as required in transport networks and could disrupt the management of connecting paths between networks entities. At the ingress port of an MPLS network, a label is inserted, and the Forwarding Equivalent Class (FEC) is associated with the label to define the packet priority across the network nodes. The process minimises latency due to the reduced IP address look-up at the switching routers and the use of labels. It also allows tunnelling of multiple traffic types through core networks.

IP/MPLS and MPLS/TP are two variants of MPLS technology that are the subject of debate in the industry for reasons associated with minimising network complexity, Capital Expenditure (CapEx) and Operational Expenditure (OpEx). While MPLS/TP is an improved version of IP/MPLS, they are both designed to meet the network requirements of future applications with stringent SLAs like video and Voice over Internet Protocol (VoIP). However, this paper compares the performance of IP/MPLS and MPLS/TP over a high voltage power line.

The utilities have been in demand to verify the performance of MPLS hitless packet-switched technologies for carrying power system's differential current applications. Tests and research efforts to prove that IP/MPLS and MPLS/TP technology equipment can meet and satisfy the toughest teleproteion requirements of Energy Network Association (ENA's). Technical Specification 48-6-7 Category 1 has always been difficult to show by many vendors. Therefore, it is necessary to have a test platform comprising many IP/MPLS and MPLS/TP nodes to understand the best possible network design to achieve the top network performance outcome.

This paper demonstrates the implementation of IP/MPLS and MPLS/TP technology in transmission networks using two types of test equipment (Equipment Type A – IP/MPLS and Equipment Type B – MPLS/TP) and to validate their suitability in teleprotection service under specific network conditions highlighted in section III. The wider focus of this paper includes evaluating Bit Error Rate (BER), Path Switching, Propagation and Asymmetrical Latency, Error Injection, and Time Synchronisation of high voltage power lines. The results presented cover:

This is a peer reviewed, accepted author manuscript of the following research contribution: Ugwuanyi, S., Ghanem, K., & Irvine, J. (2023). IP/MPLS and MPLS/TP teleprotection latencies over high voltage power lines. Paper presented at International Conference on Wireless and Mobile Computing, Networking and Communications, Montreal, Quebec, Canada.

- A validation test of IP/MPLS and MPLS/TP for line differential services, distance and inter-tripping of IEDs.
- An investigation of IP/MPLS and MLS/TP implementation and latency performance of legacy and new communication interfaces in power transmission networks.
- An investigation of redundant paths and how their outage performance affect teleprotection services.

II. Related Work

Power network protection data has mainly been routed over Synchronous Digital Hierarchy (SDH) Time Division Multiplexing (TDM) with Plesiochronous Digital Hierarchy (PDH) devices deployed at the edge of the network. Nowadays, many power utilities, including those in the UK, have communication interfaces of four-wire systems operating at 64 kbps, X.21 and IEEE 37.94 teleprotection relays in the distribution networks [2]. These interfaces are often accessed through multiplexers with BS IEC 62843, also known as IEEE C37.94 for line differential, aided distance protection schemes and inter-tripping services [3]. This means that the teleprotection relays are either directly connected to the core SDH network or the edge of the PDH network and then the core SDH network. Such traditional private TDM-based solutions are at their end of life as they are costly to operate and manage by the Distribution Network Operators (DNOs). The growing complexity of DNO's network architecture means they will not be able to efficiently support the integration of packet-based Internet Protocol (IP) needed for modern power networks. The benefits of switching to fully IP-based technology are not only to save cost, improve network performance, and meet the requirements of future power networks but because TDM technologies are being considered *"legacy"* in the broader telecommunication industry. They will become expensive to operate, maintain and source network resources [1]. Many power network operators globally are planning to deploy unified packet-switched networks to carry traditional power network services as well as new services like the Generic Object Oriented Substation Event (GOOSE), Sample Values (SVs), and other mission-critical traffics such as teleprotections.

A. IP/MPLS

More recently, packet-based technologies such as Internet Protocol Multi-Protocol Label Switching (IP/MPLS) is being widely introduced to carry network traffic in different critical applications. As a connection-oriented layers 3/2 routing protocol and packet forwarding integrated application [4], IP/MPLS defines specific primary and backup paths for packet traffic with pre-defined paths, low propagation latency and packet prioritisation that is as reliable as TDM technology. It is not only capable of handling much larger communication loads but also is more in-tune with wider telecommunication requirements. However, IP/MPLS in the power networks for critical applications like teleprotection must satisfy existing standards, regulations, and policies to ensure that teleprotection systems remain stable during any protection events. Figure 1 below is a high-level network architecture of teleprotection application over IP/MPLS technology with redundant paths. In this type of network, the impact of relay stability, path switching latency or loss of synchronisation is critical.

This work was funded under the research programme of the University of Strathclyde's Power Networks Demonstration Centre (PNDC)

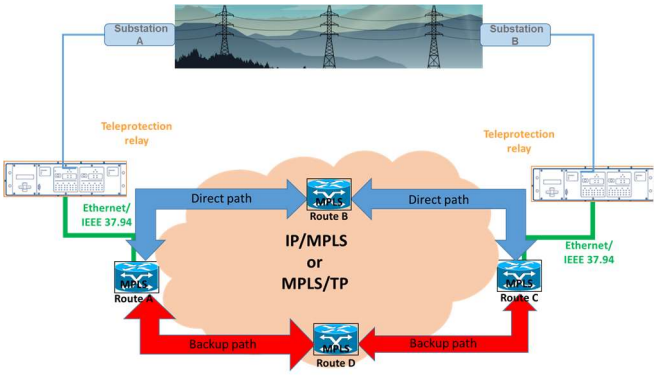

Figure 1. High-Level Network Topology of Teleprotection Service over IP/MPLS and MPLS/TP with Redundant Paths.

The selected teleprotection use case is a current differential protection scheme with the most stringent communication network requirements. The major performance requirements include:

- Steady-state propagation latency not > 6 ms.
- Steady-state asymmetrical latency not > 0.4 ms.
- Relay tripping must be > 30 ms + propagation latency of 6 ms.
- External faults must not trip relays during path switching.

IP/MPLS is connection-oriented traffic where the MPLS packets label changes at every switching node in the network. This implies that traffic rules are implemented at every node with existing knowledge of traffic classes and attributes to achieve distributed network control and intelligence efficiently. IP/MPLS is more suitable in networks with high variation of traffic sources and switching paths that require good transport engineering to manage nodes label replacement and switching decisions. On the negative side, IP/MPLS network's QoS is not guaranteed in large networks even when a dynamic Resource Reservation Protocol (RSVP) is implemented. IP/MPLS is scalable, but the capacity of the network cannot be scaled beyond the allocated bandwidth. It is also very flexible and dynamic in routing traffic because labels are replaced at each switching node [5].

B. MPLS/TP

MPLS Transport Protocol (MPLS/TP), as the name implies, is used to tunnel predetermined transport-types services through network paths. It is a layer 2 connection-oriented and packet-switched transport layer technology developed to satisfy specific requirements of transport networks. It is an adaptation of MPLS to meet SDH/SONET network requirements. It uses pre-defined tunnel with no distributed control plane, and its Operation, Administration and Management (OAM) plane operates without IP functionalities. Separating the control plane from the data plane reduces the impact of failure on the overall network. In addition to supporting large capacity, flexible, reduced CapEx, and secure network, MPLS/TP offers additional opportunities to conduct carrier-grade maintenance, simple network operation and robust and reliable protection services [6]. It is an advancement of IP/MPLS with reduced IP functionality, such as Penultimate Hop Popping (PHP), Label Switched Paths (LSPs), and Equal Cost Multi-Path (ECMP) [7]. The goal is to provide transport functionality of static creation of Label Switching Paths (LSPs) and pseudowires constructs through an external Network Management System

(NMS) while preserving the existing MPLS architecture [8]. MPLS/TP is standardised by the IETF, International Telecommunication Union, and the telecom industry [9] and is suitable to replace SDH/SONET. While MPLS is a matured technology backed by Cisco and Alcatel, as of 2017, MPLS/TP was still considered an in-mature technology [1], but has been accepted as a promising packet switching technology for mission-critical applications in 2019 [10]. In large public networks, the fixed tunnel approach makes MPLS/TP unfit for big Telecom operators covering large customer applications [1], but promising for use in utility-specific applications such as teleprotection. Scalability can still be achieved in MPLS/TP by hierarchical LSPs using label stacking [11]. In terms of security, Virtual Private Networks (VPNs) are effective in securing remote site interconnection in MPLS networks [12].

III. Test Configuration

The test network is a hardware-in-the-loop shown in Figure 2 and based on C37.94 and X.21 interfaces. Three types of connection schemes exist among the current protection relays and the MPLS hitless network. Relays are connected via fibre optic MPLS Node carrying C37.94 signal and X2 cable for the X.21 interface. It consists of Real Time Digital Simulator (RTDS) for electrical faults generation and relay trip time measurement and an Apposite Netropy network emulator for the delay, jitter and BER injections. Netropy was assessed through a dedicated management port from a PC with a standard web browser using HTTPS to inject faults. The electrical current signals from the RTDS are fed to the teleprotection relays through secondary injection amplifiers. Upon detecting power line faults, the teleptotection relay issues a trip signal. The end-to-end latency, delay, and jitter results are presented for each of the interface test scenarios. The first approach is to inject the latency in both directions and check the stability of the MPLS and protection system, whereas the second approach is to inject in one direction only. The device specified that the mean value must be at least 3 times the standard deviation for a normal distribution (i.e., in order to avoid negative latencies, the normal (Gaussian) distribution, with a specified mean and standard deviation (jitter) must be at least 3 times the Standard Deviation)

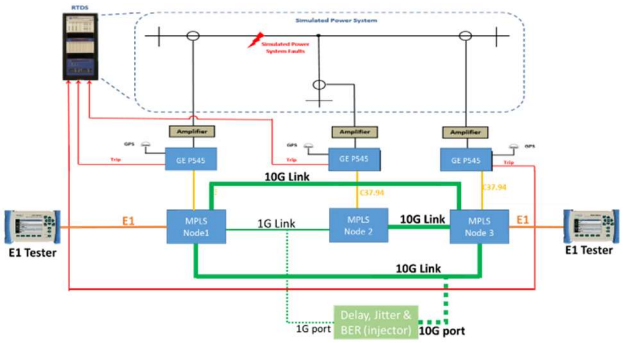

Figure 2. Overview of Hardware-in-the-Loop Testbed at PNDC

A. IP/MPLS

The IP/MPLS test network consists of four MPLS routers/nodes with dual CPUs and 6 interface slots for network integration. The hitless test is only activated on C37.94 and X.21 interfaces. The possible router configuration of the interfaces is shown in Figure 3. Teleprotection schemes over packet-switched networks must meet the requirements for different communication service categories in terms of latency, communication re-routing and BER as defined in the ENA Technical Specification 48-6-7. Specifically, end-to-end latency and symmetrical latency must be < 6 ms and 0.4 ms, respectively.

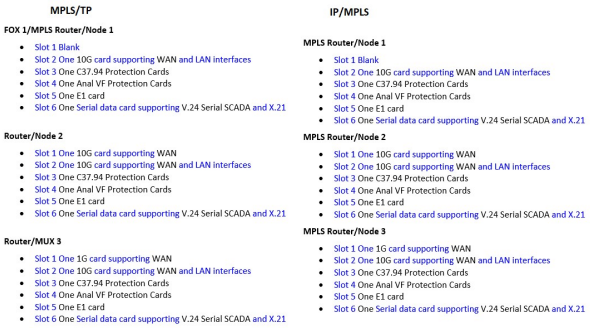

Figure 3. IP/MPLS and MPLS/TP Routers/Nodes Main Interfaces

B. MPLS/TP

Similarly, the MPLS/TP test network also consists of four MPLS routers/nodes with dual CPUs and 6 interface slots for network integration. The possible configuration of the interfaces includes using one slot for either of the configurations shown in Figure 3. In order to comply with the critical capabilities and ensure deployment flexibility, for each interface, the teleprotection services are configured as hitless path redundancy via different WAN cards.

IV. Results and Discussions

A. Base Case Test

In IP/MPLS, the relays communicate with each other using the main path, and IP/MPLS network operated without artificial bit error and latency. In this test, the measurements of the end-to-end latency from the relay show an average value of 4.56 ms for a buffer size of 1 ms. Table 1Table 1 shows the propagation delay obtained by the relays and the calculated asymmetrical latency of the optical interface. The propagation delays and the asymmetrical latencies of the X.21 communication interface obtained by the relays are also shown in Table 1. The internal buffer size for the base testing of C37.94 and X.21 interfaces was configured and setup with a fixed value of 2 ms. By injecting different values of delays and jitter, end-to-end latencies were measured by the relays and a network tester.

Table 1. IP/MPLS Propagation and Asymmetrical Latency Measured by the Relays for C37.94 and X.21 Interfaces

X.21 (ms)		**C.37.94 (ms)**	
Propagation	Asymmetrical	Propagation	Asymmetrical
4.61	0.05	5.00	0.01
4.60	0.005	5.02	0.09
5.07	0.02	5.07	0.02

For the MPLS/TP, The configuration without bit error or latency enabled relays to communicate with each other using the main path via MPLS/TP network. Average end-to-end latency of 9.6 ms was obtained with a buffer value of 6 ms. Table 2 shows the measured values obtained by the relays of the propagation delay and the calculated asymmetrical latency of the X.21 and C37.94 interfaces.

B. Teleprotection Latency over IP/MPLS Network

Table 2 below summarises the test findings for IP/MPLS equipment providing teleprotection services over a high voltage line.

Table 2. Teleprotection Requirements and Latency over IP/MPLS Network

Test case	Requirements	Note
Propagation and Asymmetrical Latency	Propagation Latency < 6ms and Asymmetrical Latency < 400 µs	C37.94 and X.21 interfaces should normally have stable IP/MPLS network supporting teleprotection with unchanged delay.
Fault and Trip Time	Teleprotection relays should trip successfully	Stable and functioning IP/MPLS network providing teleprotection services
Network Stability upon Path Switching	No connectivity loss and communication interruption	Stable IP/MPLS supporting teleprotection services
Incident Test: Power failure or Network Outage	No maloperation and communication interruption	Stable IP/MPLS supporting teleprotection services
Bit Error Rate	No maloperation and communication interruption	Stable IP/MPLS supporting teleprotection services
Synchronisation Loss	No maloperation and communication interruption	No maloperation and communication interruption
QoS Test	Highest teleprotection priority service not affected by flooded traffics	Flooding non-critical services should not affect critical services
IEC 61850 Support	No dropped packets	This should apply to non-critical services

The delay and jitter over IP/MPLS due to constant delay and asymmetrical BER impairment injections from network emulator via HTTPS into the network showed normal distribution where mean and standard deviation values of delay and jitter were 4 ms and ±250 µs, respectively. The injections took two different approaches (uni and bi directions) in which the stability and protection of IP/MPLS network were investigated to check the hitless technology.

C. Propagation and Asymmetrical Latency via X.21 and C37.94 Interfaces

The average delay of propagation and asymmetrical latencies between channels is shown in Table 3 for MPLS/TP. The round trip propagation latency measured by the relays via C37.94 interface is shown in Table 4. The relays communicate using the main path via an MPLS/TP network without bit error or latency above the recommended value for the base case test. End-to-end latency averaged 9.6 ms for a buffer size set to 6 ms. The asymmetrical latency for C37.94 and X.21 interfaces are shown in Table 3 for average propagation latencies between relay channels.

Table 3. MPLS/TP Propagation and Asymmetrical Latency Measured by the Relays for C37.94 and X.21 Interfaces

X.21 (ms)		C.37.94 (ms)	
Propagation	Asymmetrical	Propagation	Asymmetrical
9.67	0.01	8.98	0.02
9.64	0.08	8.88	0.03
9.74	0.13	8.90	0.07

In terms of delay injections, following different injected values into the MPLS network along with various jitter values, a path of the two teleprotection services was affected by the injected delay over X.21 and C37.94. The end-to-end delay and associated asymmetrical latency remained unchanged when the network emulator was configured with latency and jitter values of 1ms and 0.25 ms; 2 ms and 0 ms; 2 ms and 0.5 ms; and 4 ms and 0.5 ms. For these injection measurements, no trip occurred within the network and MPLS hitless communication between relays of MPLS/TP was still operational. For the teleprotection relay with an end-to-end delay of 4 ms for an internal buffer set to 4 ms, within an MPLS/TP network maintained an end-to-end delay of 6 ms.

Table 4. MPLS/TP Round Trip Propagation Latency for C37.94 Interface

Delay (ms)	Jitter (ms)	Propagation Latency (ms)	Buffer Size (ms)
1	0.25	4.69 to 4.51	2
2	0	6.8 to 6.81	4
2	0.5	6.8 to 6.81	4

For the X.21 interface, an end-to-end delay of 6.67 ms is maintained for the forward path and 6.86 ms for the return path for an internal buffer configuration of 6 ms. When the end-to-end latency is reduced to a constant value of 4.86 ms, the latency for the forward and return paths was 4.86 ms and 4.80 ms, respectively. The asymmetrical delays for the two 6 ms and 4 ms internal buffer configurations were constant values of 185 µs and 63 µs, respectively. The asymmetrical delay is due to the PDH Backplane Bus and data processing.

D. Event Response Time

Understanding the event time response is essential as it introduces power events, out-zone faults and in-zone disturbances. The network propagation latency measurements from the relays showed a stable MPLS/TP network during faults event response test under injection and jitter values of 1 ms and 0.25 ms; 2 ms and 0 ms; and 2 ms and 0.5 ms, respectively. The average network propagation latency for optical interface (C37.94) is between 8.77 ms to 8.99 ms when injecting the above delay and jitter values for an internal buffer configuration of 6 ms. Based on the event response time measurements by RTDS, the in-zone trip time is between 27.95 ms to 31.45 ms, while the remote inter-tripping time is between 43.40 ms to 51.10 ms.

For IP/MPLS, The average round trip of network propagation latency for optical interface (C37.94) is between (4.69 ms to 4.51 ms when injecting a delay value of 1 ms and jitter of 0.25 ms). While the network propagation delay is between 6.8 ms to 6.81 ms when injecting a delay value of 2 ms and jitter of 0.25 ms. The change caused by the measured value is due to the change in the buffer size, which is reconfigured and changed from 2 ms to 4 ms. The difference in the obtained values for the optical interface was caused by changing of the internal buffer size values which were configured and setup with two values (2 ms and 4 ms). The event response time measured by the RTDS shows that the inzone trip time is between 23.40 to 30.3 ms while the remote inter-tripping time is between 35.8ms to 45.9 ms

E. Bit Error Test

The Bit Error (BER) test is important as it covers propagation and asymmetrical latency, relay tripping time, monitor communication, and protection stability. By injecting BER into the 10 Gbps and 1 Gbps traffics of MPLS hitless test setup, packet loss and corruption rate is determined; see Table

5 for IP/MPLS and MPLS/TP test scenarios. These results are based on each of the paths being broken during tests. One important observation is that channel failing becomes persistent on the relays only when BER is applied to the 10 Gbps path.

Table 5. IP/MPLS and MPLS/TP Packet Loss and Corruption Rate

BER		Notes
Corruption	**Loss**	
10^{-6}	10^{-6}	No impact on the traffic, the relays tripped correctly for all fault events, and there was no communication alarm on the relays or the MPLS nodes.
10^{-5}	10^{-5}	Relay channels flashing that indicates BER threshold.
10^{-4}	10^{-4}	No communication between channels

Similar to MPLS/TP, several BER values were injected into the traffic in the IP/MPLS hitless test setup based on the packet's corruption and lass rate, as shown in Table 5. Two test scenarios also apply in IP/MPLS, which involves both paths remaining available, and in the other, one path is broken.

In summary, the test results for IP/MPLS and MPLS/TP test scenarios show that applying any value of BER in any mode had no impact on the traffic and the communication relay-to-relay remained 100% available. There was no communication alarm on the relays when BER was lower than $10^{-5,}$ and the MPLS hitless technology successfully maintained the protection service during the implemented test. Both networks failed when BER greater than 10^{-4} was applied to the 10G link, and the main path was broken; see Figure 4.

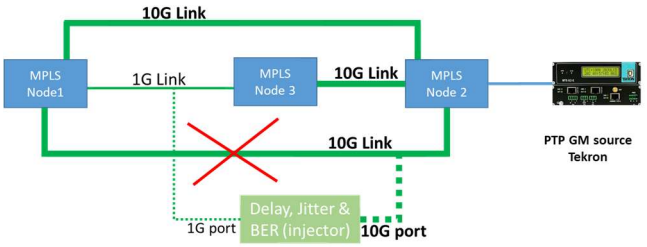

Figure 4. BER Injection: 10 G Link Broken and Delay and Jitter Injected into the 1G Link.

F. *Path Switching Test*

Path switching test involves disconnecting the fibre link, and an external fault applied. No communication or trip alarms were captured during the test for the many test scenarios, and the network latency remained stable after path switching. When one path is broken, the performance of the network remains unchanged. MPLS/TP linear protection switching standard guarantees a switchover time of less than 50 ms. MPLS hitless WAN redundancy and linear protection are needed for smart grid capabilities and deployment flexibility.

G. *Time Sychronisation Test*

The synchronisation loss test allowed the monitoring of changes in the performance of both the MPLS communication network and the protection services covering the main source of synchronisation from the grandmaster. The absence of external time synchronisation (i.e., the main external source of synchronisation) has not caused any alarms on the relays and does not affect the operation of the MPLS teleprotection service in both IP/MPLS and MPLS/TP networks. The relays switched from one priority to another without any traffic interruption. Note that the tests were performed without relay synchronisation (i.e., the GPS synchronisation signal was disconnected to reflect the current status of the operated relays in DNO's networks).

H. *Incident Test*

An incident test is performed to monitor changes in the MPLS communication network or the protection service when the controller card and redundant power units are removed or MPLS routers rebooted. This way, the incidents' effects on the communication and protection services are identified and analysed.

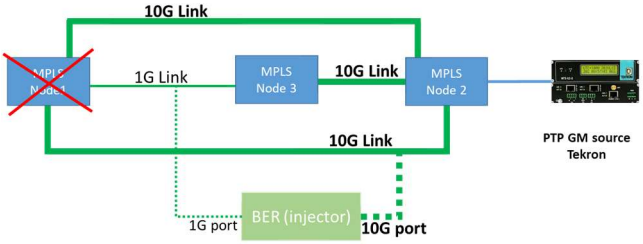

Figure 5. High-Level Testbed for Incident Test: MPLS Node 1 Controller Card Removed.

As shown in Figure 5, when the redundant power unit is removed on MPLS Node 1, the system functioned without power supply failure that would have resulted in communication alarm trips from the relays. When the active core unit (CESM3) responsible for increasing packet switched capability and synchronisation in MPLS/TP network was removed, the network switched to another slot of CESM3 without communication alarms and trip signals from relays. In both IP/MPLS and MPLS/TP incident tests, communication alarms were observed when the test equipment was rebooted. While it took 280 s for the alarm to be cleared and the full IP/MPLS communication service restored, MPLS/TP achieved the same network recovery process in 220 s.

I. *QoS Test*

The test network is flooded with Ethernet traffic from critical and non-critical service, and the impact on the teleprotection services are examined. An alternative source of SCADA and ANM traffic is used; E1 tester for IP/MPLS and Albedo tester for MPLS/TP. As shown in Figure 1, a separate service pipe for Teleprotection critical services (10% of available WAN capacity) was setup to represent the critical teleprotection service, whereas SCADA services of 90% of the available WAN capacity have been configured (90% of available WAN capacity). In this test, two Ethernet services were created over a 1Gb/s link (MPLS Node1 to MPLS Node3). Ethernet service 1 was created as a 100Mbit/s critical service (Highest priority (i.e.Traffic Class 6)), whereas Ethernet service 2 was created as a 1Gbit/s non-critical service (Best effort Traffic (i.e., Traffic Class 0)). The services included both priority and best efforts traffic over 100 Mbps and 1 Gbps links. The result showed that for both IP/MPLS and MPLS/TP, the allocated bandwidth for critical teleprotection services with the highest priority was maintained and had no impact on the traffic. The performance remained unchanged with non-critical service of Class 5 configuration. When the allocated bandwidth

exceeded the available bandwidth, packets of non-critical type of service were dropped for the critical teleprotection type of service.

J. *Proof of Concept IEC 61850 Test*

In the proof of concept IEC 61850 test, the RTDS is configured to generate and receive the IEC 61850 Generic Object Oriented Substation Event (GOOSE) messages with precise timestamps. Without BER injections, latency and device incidents, IP/MPLS and MPLS/TP hitless networks successfully passed the traffic without errors.

V. CONCLUSION

The paper shows that MPLS hitless technology can meet latency and asymmetrical requirements over communication interfaces for teleprotection systems with adequate network design and test configurations. Hitless technology uses active MPLS paths simultaneously to ensure the arrival of packets under tough network conditions. As the packets move between relays, they are duplicated over different active paths, which can guarantee the arrival of the packets to their destination. End-to-end latency and asymmetrical requirements of teleprotection services via MPLS network are critical for energy network restoration in the case of black start. QoS prioritisation ensures that teleportection packets are not queued under network congestion, reducing end-to-end and asymmetrical latency. Under severe network congestions for both IP/MPLS and MPLS/TP test equipment, MPLS hitless technology is verified based on the hardware-on-the-loop principle by applying MPLS network monitoring tools and diagnostics on latencies, synchronisation, packet loss and jitter buffers. The RTDS testing has been configured to verify the performance requirements and the functionality of the MPLS communications service via applying different types of faults to the simulated high voltage power line. The study verified that teleprotection service is stable, and no mal-operation has been observed in any of the tested use cases for both IP/MPLS and MPLS/TP.

VI. REFERENCES

[1] C. Samitier. Books, Utility Communication Networks and Services - Specification, Deployment and Operation, Paris, France: Springer & Cigré, 2017.

[2] IEEE Standard Association, "IEEE Standard for N times 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment," IEEE, NY, USA, 2017.

[3] S. M. Blair, F. Coffele, C. Booth, B. De Valck, and D. Verhulst, "Demonstration and analysis of IP/MPLS communications for delivering power system protection solutions using IEEE C37. 94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols," CIGRE, CIGRE Session, 2014.

[4] F. Rambach, B. Konrad, L. Dembeck, U. Gebhard, M. Gunkel, M. Quagliotti, L. Serra, and V. López, "A Multilayer Cost Model for Metro/Core Networks," *Journal of Optical Network,* vol. 5, pp. 210-225, 2013.

[5] S. M. Blair, C. D. Booth, J. Michielsen, and N. Joshi, "Application of MPLS-TP for transporting power system protection data," in *IEEE International Conference on Smart Grid Communications*, Sydney, Australia, 2016.

[6] M. Murakami, and Y. Koike, "Highly Reliable and Large-Capacity Packet Transport Networks: Technologies, Perspectives, and Standardization," *Journal of Lightwave Technology,* vol. 32, no. 4, pp. 805-816, 2014.

[7] Cisco, "Understanding MPLS-TP and Its Benefits," *MPLS,* 05 May 2013.

[8] M. Ina and L. Julian, "MPLS Transport Profile (MPLS-TP)," in *MPLS-Enabled Applications*, John Wiley & Sons Ltd, 2011, pp. 509-529.

[9] S. M. Blair, C. D. Booth, J. Michielsen and a. N. Joshi, "Application of MPLS-TP for transporting power system protection data," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Sydney, NSW, Australia, 2016.

[10] F. Kamoun, and F. Outay, "IP/MPLS networks with hardened pipes: service concepts, traffic engineering and design considerations," *Journal of Ambient Intelligence and Humanized Computing,* vol. 10, p. 2577–2584, 2019.

[11] M. A. Ridwan, N. A. Radzi, W. S. Wan Ahmad, F. Abdullah, M. Z. Jamaludin, and M. N. Zakaria, "Recent trends in MPLS networks: technologies, applications and challenges," *IET Communications,* vol. 14, no. 2, pp. 177-185, 2020.

[12] A. Bahnasse, M. Talea, A. Badri, F. E. Louhab, and S. Laafar, "Smart hybrid SDN approach for MPLS VPN management on digital environment," *Telecommunication Systems,* vol. 73, pp. 155-169, 2019.