

# Teleprotection Over an MPLS Network

The Need for Deterministic Packet Transport



## Deterministic Packet Transport With MPLS-TP for Teleprotection, SIPS and WAMS

### 1 Introduction

Power companies rely on deterministic, secure, and highly reliable communication networks to operate their mission critical infrastructure. The traditional SDH/SONET networking technologies used to provide this mission critical communications network have reached end of life. In addition, the world is changing rapidly; all modern devices and substations are moving to IP and SDH/SONET is not an efficient way to transport the IP traffic generated by these devices. These two seemingly conflicting demands are causing power companies major challenges.

Power companies must transition to a modern packet transport network (PTN) capable of supporting both the legacy services previously supported by the SDH/SONET networks and new IP based services and infrastructure.

Teleprotection is one of the main challenges operators face when planning to modernize their mission critical communications networks. Teleprotection requires the network to have extremely low, predictable, latency with low latency variation between forward and backward paths. Deterministic packet transport network, using MPLS-TP, provides operators with a solution to this challenge.

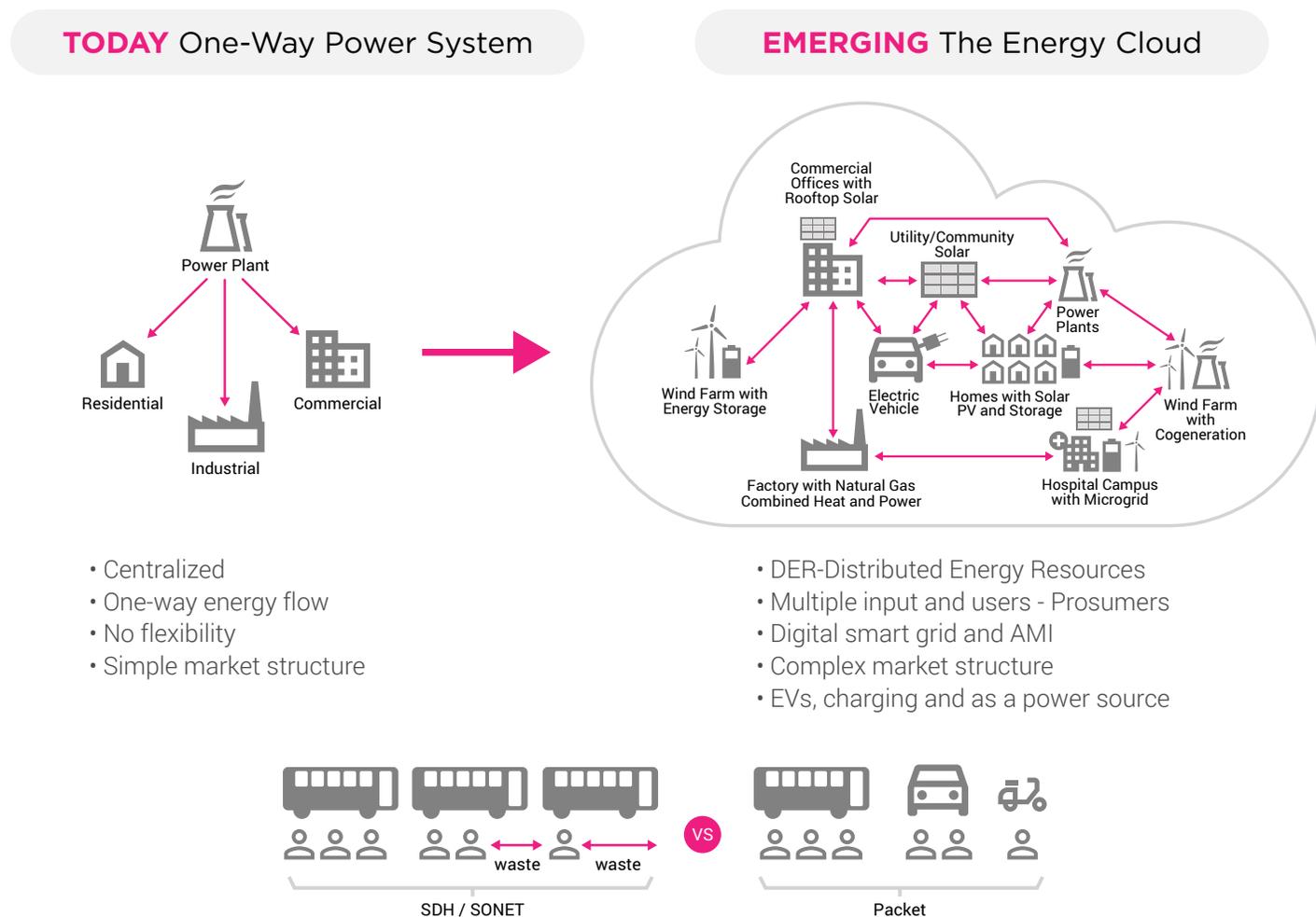


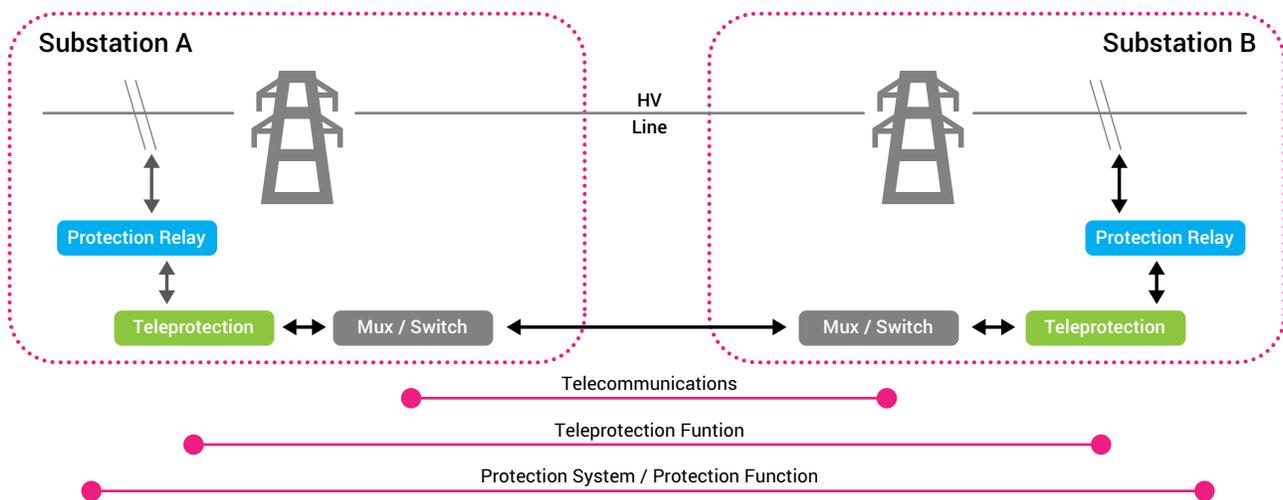
Fig. 1: Evolution of the power grid – topology, services and applications, TDM to packet

# Teleprotection Over an MPLS Network

## 1.1 Teleprotection

Teleprotection is crucial for the reliable and secure operation of electrical power systems, it allows the rapid detection and isolation faults with the aim of:

- **Preventing Widescale Power Outages:** by ensuring local faults do not escalate into widespread power outages.
- **Minimizing Equipment Damage:** by preventing damage to critical equipment such as transformers, circuit breakers, and other components.
- **Ensuring Personnel Safety:** by identifying and switching off faulty segments and installations.
- **Helping Utilities Meet Regulatory Requirements:** by helping utilities comply with regulatory requirements for grid reliability and safety.



**Fig.2:** Schematics of a High Voltage protection relay showing all elements separated. Nowadays, the relay (1) and the teleprotection element (2) and the telecommunications element (3) multiplexer or switch, can be fully integrated into one single element.

Two primary protection schemes are used.

- **Line Distance Protection** is based on the principle that the impedance of a transmission line is proportional to its length. It requires a deterministic, low latency communications network, with very low latency variation to rapidly communicate impedance measurements across the power network.
- **Line Differential Protection** is based on the principle that the current into a point on the network must equal the current exiting from that point. It requires high bandwidth, low-latency communication to exchange analog information between the ends of the line and a common time reference to accommodate delay compensation.

# Teleprotection Over an MPLS Network

## 1.2 SIPS (System Integrity Protection Schemes)

These schemes are designed to prevent severe systems disturbances which could lead to widespread blackouts, ensuring local issues do not impact the rest of the network. SIPS closely monitor the power system and take corrective actions to maintain its integrity.

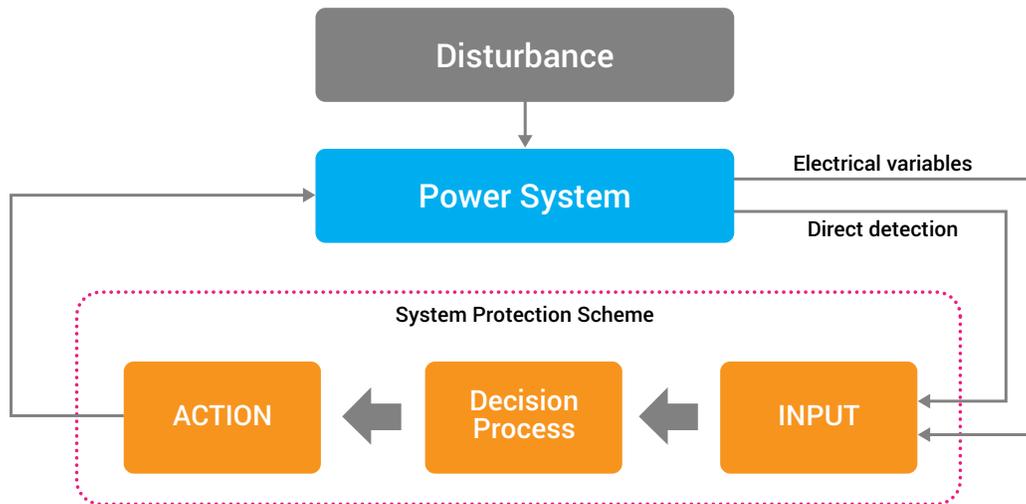


Fig. 3: General structure of a system protection scheme

There are two categories of SIPS:

- **Response-based SIPS** operates by measuring a set of electrical variables such as voltage phasors, frequency. It requires accurate synchronization and a fast exchange of huge volumes of data. It requires a highly reliable, high bandwidth communication network.
- **Event-based SIPS:** operates by detecting a combination of events (loss of several lines for example), it is faster to act than response-based systems as it does not need to wait for out-of-tolerance variables to be measured. It requires a reliable, fast, time-constrained and fully predictable communications network

## 1.3 WAMS (Wide-Area Monitoring System)

WAMS is a monitoring and control system that uses real-time data from multiple locations across the network to assess the overall health and stability of the power grid. WAMS collects synchronized data from Phasor Measurement Units (PMUs) located at various substations. These measurements include voltage, current, and frequency phasors, providing a comprehensive view of the network. Control systems detect and respond to disturbances quickly. WAMS use a variety of analytics and algorithms such as; post-incident analysis, static modeling, visualization and situational awareness monitoring and decision support systems. WAMS require a lossless, highly synchronized communications network.

## 1.4 Other Elements to Consider – Network Interfaces and Devices

The interfaces used by the relays and sensors in the power system network, provide n x 64 kbps up to 2 Mbps capacity and include RS232/ITU-T V.24, RS422/423/ITU-T V11/V10, G.703 co-directional and contra-directional, X.21, V.35, E1, T1, E&M and C37.94. As networks digitize and standardize around IEC 61850-based substation architectures we are starting to see IP devices gradually replacing the legacy devices used in the OT network. However, this is a long-term complex task that will take many years if not decades for the majority of network to move to IP. This means the communications network will need to provide network connectivity with the reliability, latency, and security required by both legacy and packet-based devices and systems.

## 2 Modernizing to a Deterministic Packet Transport Network

### 2.1 Historical Overview of OT Communication Networks

The evolution of communication networks used for teleprotection is traced from Power Line Carrier Communications (PLCC) to the SDH/SONET networks used for the last 30 years. The emergence of digital technology such as packet-based sensors, IEDs, RTUs, CCTV, digital substations, and the end-of-life of SDH/SONET equipment has driven the need for power network operators to urgently evaluate how to evolve their OT communications network to packet.

### 2.2 Circuit Emulation Services (CES)

Circuit Emulation Services (CES) is a method by legacy SDH/SONET services are “tunneled” across a packet transport network (PTN). The TDM data is encapsulated for transport across the PTN, creating packets on ingress and reversing the process on egress. As a result, the TDM equipment on either end of the PTN perceives a direct connection to the opposite end and is unaware of the intermediary network that is being used to emulate the behavior of a TDM circuit. Different CES protocols are used to cater for different operational scenarios:

- **SAToP (Structure-Agnostic TDM over Packet)**, encapsulates TDM frames into IP packets the underlying TDM frames are transported agnostically.
- **CESoPSN (Circuit Emulation Service over Packet Switched Network)**, preserves structure of the original TDM frames during encapsulation.

### 2.3 Deterministic Packet Transport

Over the last decade, IP/MPLS has become the ubiquitous transport technology for networking packet technology and devices. However, as described previously, the modernized OT communications network must support Teleprotection, SIPS, WAMS and legacy and packet-based sensors/actuators. To achieve this, it must provide the traffic engineered, deterministic, circuit switched, transport provided by the SDH/SONET transport network, along with the ability to natively transport packet-based devices. Whilst IP/MPLS is perfect for packet transport, either native packet from packet-based devices or circuit emulated packet traffic from legacy devices, it was not architected and by itself, it is not able to provide the traffic engineered, deterministic, circuit switched transport required to support Teleprotection, SIPS and WAMs.

Over the years a number of approaches have been used;

- **RSVP-TE:** Designed to add traffic engineering capabilities to IP/MPLS by allowing for the explicit setup of LSPs through the network and a way to reserve resources along a specified route. It is complex to set-up and does not guarantee latency or the bidirectional paths required for accurate synchronization.
- **SR-TE:** A centralized path computation engine calculates the path a packet should take and encodes it in the packet header. Not widely field proven in mission critical networks.
- **MPLS-TP:** Extends IP/MPLS to specifically provide capabilities provided by legacy SDH/SONET network. Can not perform layer 3 routing.

### 2.4 Why MPLS-TP is Ideal for Teleprotection, SIPS and WAMS

MPLS-TP extends IP/MPLS by adding transport specific features to the IP/MPLS protocol and removing some of the IP/MPLS routing protocols. The capabilities provided by MPLS-TP include:

- Deterministic transport:
  - MPLS-TP uses a centralized NMS to create pre-determined paths across the network, making the performance of the network entirely predictable. In addition, the transport network can be monitored to ensure the design requirements and service level agreements (SLAs) are met over the lifetime of the connection.
- Consistent predictable behavior:
  - MPLS-TP and IP/MPLS use the same data-plane mechanisms. However, MPLS-TP uses bidirectional Pseudowires (PW) and Label Switching Paths (LSP), while IP/MPLS uses unidirectional PWs and LSPs. This ensures the forward and return paths always follow the same route, which is essential for accurate, reliable synchronization.
- Improved resilience:
  - Pre-determined alternative paths ensure rapid protection switching, well within 50ms, provided by SDH/SONET for all network topologies. For mission-critical applications such as SCADA and teleprotection, it is mandatory that the protecting paths guarantee the same low latency, jitter, and round-trip delay as the working path. Pre determined paths provide this guarantee.
- Full-centralized control:
  - A centralized NMS maintains ensures services are always functioning, even if there is a failure in the network control plane. MPLS-TP management “look and feels” like SONET / SDH, making migration from SDH SONET transport to IP transport less complex and far less prone to human error.
- Mission critical grade OAM:
  - MPLS-TP supports extensive Operation, Administration, and Maintenance (OAM) functions, similar to those available in the traditional SONET/SDH transport networks. These include enhanced Fault Management, Performance Monitoring, and in-band PW/LSP/Section OAM levels. The OAM functions are an integral part of the MPLS-TP data plane and are independent of the control plane.

With the above capabilities MPLS-TP can provide a communications network able to support Teleprotection, SIPS and WAMS.

- Low deterministic latency:
  - Fiber transmission latency: approximately 200 ms/km, negligible when compared to other factors.
  - Interface latency: high-speed interfaces produce a shorter transmission delay than low-speed interfaces with interface converters.
  - Network Element Latency: packet buffers result in latency in the ingress and egress ports. Pre-determined paths make these delays totally deterministic
  - Packet forwarding latency: very small, tens of microseconds for each device.
  - Transmission latency: the fiber transmission introduces latency of approximately 200 ms/km. This is negligible when compared with the other factors.
- Packet delay variation (PDV):
  - MPLS-TP provides a PDV prevention superior to IP/MPLS QoS mechanisms, this ensures the stability and reliability of the teleprotection service
- Communications Channel Symmetry
  - MPLS-TP ensures channel symmetry by transmitting data on bi-directional LSPs and predetermined traffic paths and traffic priorities
- Rapid protection switching (sub 50ms):
  - MPLS-TP guarantees loss, sub 50ms, protection switching, regardless of network topology.

# Teleprotection Over an MPLS Network

Cigre Green Books state the advantage of MPLS-TP for power utilities:

**“...transition to packet for power utility network having extensive SONET/SDH TDM infrastructure, management tools and skills is almost smooth for MPLS-TP because of its SDH-like behavior... (while) IP/MPLS is a jump into another type of network operation”**

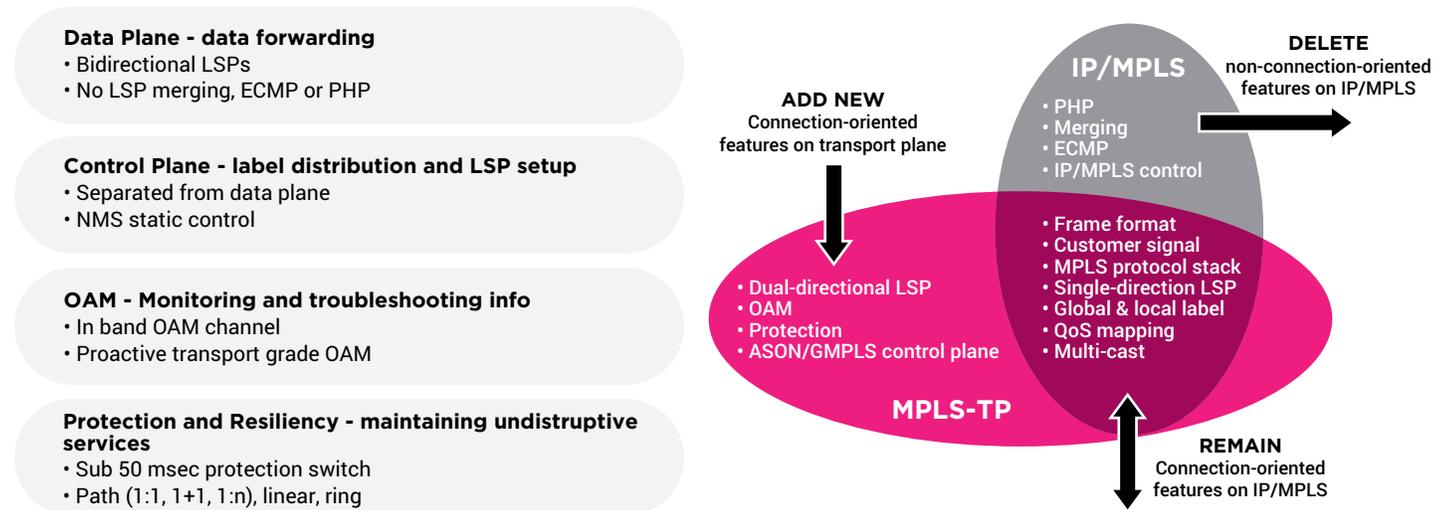


Fig. 4: MPLS-TP and IP/MPLS compared – MPLS-TP main advantages

## 2.5 Conclusions

With MPLS-TP and circuit emulation, power companies now have the tools they require to confidentially transition from their legacy SDH/SONET OT communications network to a modern packet-based OT communication infrastructure.

Circuit emulation ensures seamless support for legacy services and devices on the packet network, while MPLS-TP provides the deterministic packet transport crucial for successfully supporting the teleprotection, SIPS, and WAMS applications.

## Example Case Study

Transmission of teleprotection signals over a MPLS-TP network Ribbon NPT-1200 platform and ZIV DIMAT TPU-1 protection relay.

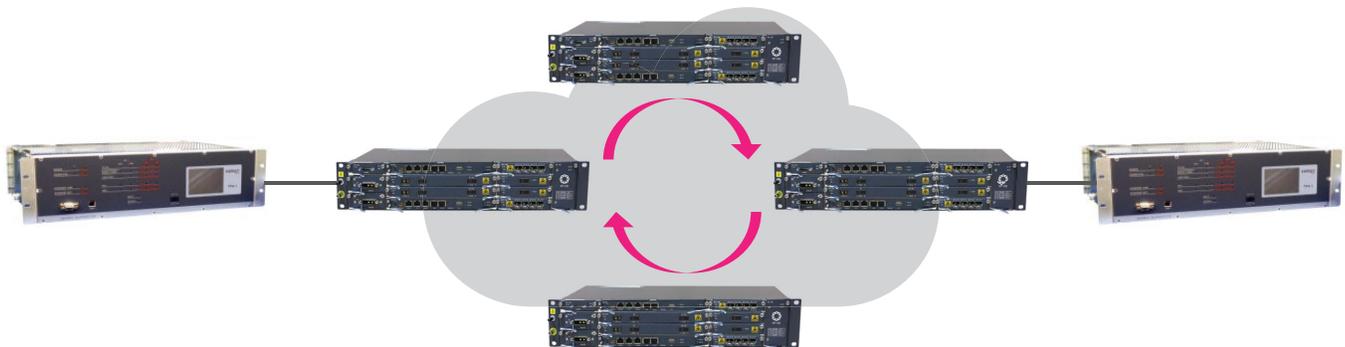


**Benchmark:** IEC 834-1 performance figures for teleprotection systems

Protection scheme	Maximum actual transmission time $T_{ac}$ ms		Channel quality		Noise duration $T_a$ ms	Security $P_{uc}$		Dependability $P_{uc}$
	Analog	Digital	Analog S/N dB	Digital BER		Analog	Digital	
Blocking	15	10	6	$10^{-6}$	Continuous	N/A	N/A	$<10^{-3}$
Blocking	15	10	Worst case		200	$<10^{-3}$	$<10^{-4}$	N/A
Permissive underreach	20	10	6	$10^{-6}$	Continuous or pulsed	N/A	N/A	$<10^{-2}$
Permissive underreach	20	10	Worst case		200	$<10^{-4}$	$<10^{-7}$	N/A
Permissive overreach	20	10	6	$<10^{-6}$	Continuous or pulsed	N/A	N/A	$<10^{-3}$
Permissive overreach	20	10	Worst case		200	$<10^{-3}$	$<10^{-7}$	N/A
Intertripping	40	10	6	$<10^{-6}$	Continuous or pulsed	N/A	N/A	$<10^{-6}$
INtertripping	40	10	Worst case		200	$<10^{-6}$	$<10^{-8}$	N/A

NOTE - The maximum actual transmission times quoted refer to applications for EHV systems. Longer times may be allowable for lower voltage systems. Longer times may also occur at reduced bandwidths. (See 3.3.1).  
N/A: Not applicable.

### Network Topology:



# Teleprotection Over an MPLS Network

## Test Results:

	Latency Results Blocking Applications	Latency Results Direct Trip
TPU-1 to TPU-1 direct connection	2,48 ... 3,29 ms (E1) 15 ms (E&M)	13,4 ... 14,2 ms (E1) 22 ms (E&M)
Communications over MPLS-TP with Digital E1 interfaces	4 ... 5,12 (No congestion) 7,92 ... 8,72 (Network congested)	20 ... 20,6 ms (No congestion) 20,8 ... 21,2 ms (Network congested)
Communications over MPLS-TP with Analogue (E&M) interfaces	18 ... 18,6 ms (No congestion) 26,2 ms (Network congestion)	22 ms (No congestion) 26,2 ms (Network congestion)

## Conclusions:

- Effect of MPLS-TP network on dependability and security – path rerouting
  - No alarms during switching to alternative path
  - No losses of guard messages during switchover process
  - No interruptions of command state during switchover process
  - No false commands were observed
- Transmission of teleprotection signals over MPLS-TP is approved
- Jitter buffer configuration has an impact on transmission time
- Digital interfaces, as expected, delivers better performance

## About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit [ribbon.com](https://www.ribbon.com).

**Contact Us**

Contact us to learn more about Ribbon solutions.