A Survey on Utilizing MPLS and Multi-Path Transport Protocols for Power Grid Protection

Name: Jan Tugsbayar
For the Chair of Communication and Distributed Systems (COMSYS)
RWTH Aachen
Email: jan.tugsbayar@rwth-aachen.de

***Abstract*—A variety of communication standards exist in the context of power grids. From the perspective of modern IT technologies, some of these standards can be perceived as outdated, frequently utilizing proprietary technologies that are incompatible with contemporary packet-based communication standards or even incompatible across different vendors. In the context of the modern concept of a "Smart Grid," the International Electrotechnical Commission (IEC) 61850 standard is an emerging standard with the objective of establishing vendor-independent communication for devices within a power grid. The standard specifies a variety of protocols that can be utilized for general communication, management, and control of Intelligent Electronic Devices (IEDs), including protection relays, measurement devices, and controllers. The specified protocols are GOOSE, SV, and MMS. The standard additionally includes two redundancy protocols: PRP and HSR. The goal of the redundancy protocols is to provide resiliency to link failures. The objective of this paper is to provide an overview of the potential for integrating other existing packet-based technologies, such as Multiprotocol Label Switching (MPLS) or multi-path transport protocols MPTCP and MPQUIC, with the IEC 61850 standard. The objective of the integration is to incorporate a new form of redundancy mechanism to provide resiliency to network link failures while maintaining compliance with the rigorous time constraints under which power grid communication must operate.**

I. Introduction

The operation of power grids is of paramount importance to our daily lives. In order for them to function properly and be able to respond to changing demand, faults and other external events such as natural disasters, they require some form of monitoring and communication technologies to detect problems in the system. Natural phenomena such as lightning strikes, landslides, or tsunamis can result in the disconnection of portions of the grid, which may subsequently lead to a power surge or damage to power generation facilities. Another potential scenario is that the grid may become overloaded when the demand exceeds the generation capacity. Such failures can result in physical damage to the grid infrastructure, which is costly to repair and can impair the power distribution until it is repaired. Measures to safeguard the grid are available, but they must be executed promptly to prevent damage. In the absence of dependable and expeditious communication, the grid is unable to respond to such occurrences. In the most extreme scenario, a blackout could occur [1]. A blackout of a significant scale can have a wide-ranging negative impact, with consequences that extend beyond the immediate area affected. This can include the failure of hospital equipment, and the disruption of trading activities resulting in large-scale economical damage. A number of critical facilities and infrastructure have backup power sources, which can provide power for a limited period of time, though a blackout scenario ideally should never occur.

To prevent such occurrences, various grid protection mechanisms exist. These mechanisms must be able to communicate both over long distances between different facilities and short distances locally within a facility. Given the critical role of power grids, it might be assumed that they would all use the newest state-of-the-art technology. However, it is challenging to make such transitions precisely because they have such a vital role and they cannot be simply turned off, or the process of deactivation for maintenance and upgrades is too complicated or costly. Many communication technologies utilized in the power grid can be considered legacy by the modern standard [2] and circuit switching is still employed. Although these legacy systems have the advantage of being purpose-built, they are inefficient and inflexible [3]. A transition is currently being carried out in the industry to transform the conventional grid to the modern *"Smart Grid"* [4]. The fundamental principle of the Smart Grid is to enhance the conventional grid with modern technologies in order to provide automation (Substation Automation System), inter-vendor compatibility and flexibility. These new additions utilize the most recent forms of communication and IT technologies that are packet-based [5].

Nevertheless, even the most recent standards are not without flaws. Conventional IP/TCP-based communication does not meet the high reliability standards that power grids require, necessitating the use of additional protocols to achieve the near-full reliability that is desired for power grids. This paper aims to provide an overview of the newest power grid communication standard, *IEC 61850* [6]. We examine the IEC 61850 standard and how it can be deployed in combination with other packet-based technologies that can be adapted for our use. Section II introduces the IEC 61850 standard and its main components. Then the two included recovery protocols, *Parallel Redundancy Protocol (PRP)* and *Highly-available Seamless Redundancy (HSR)* are presented with their different advantages and disadvantages. In Section III, we examine the potential of using *Multiprotocol Label Switching (MPLS)* as an underlying communication protocol in

power grid communication, which can provide redundancy and conform to the time constraints. Section IV considers an alternative approach to achieving redundancy by using multiple paths, namely the utilization of *multi-path transport* protocols *MPTCP* and *MPQUIC*. Section V presents a comparison of the various approaches presented and assesses which ones could be practically integrated. Finally, Section VI offers a conclusion of our thoughts and recommendations.

II. Power Grid Communication

A. Communication Characteristics

A conventional power grid system is comprised of three principal components: generation, transmission, and distribution. Generation occurs in power plants, which constitute the generation component. The transmission system is responsible for transporting power from power plants over long distances in high quantities, for instance, through overhead high-voltage power lines. Finally, the distribution system is responsible for delivering the power at appropriate voltages to customers. Electrical substations serve as nodes within the grid that connect the transmission and distribution components. Its functionalities include the transformation of voltages, monitoring and controlling the power grid. All of these components must communicate in some form or another. However, our paper focuses on communication within a substation and between substations or facilities. Intra-substation communication is typically implemented as a *Local Area Network (LAN)* using the *Ethernet* over fiber. In contrast, inter-substation communication is realized as a *Wide Area Network (WAN)* using *Synchronous Optical Networking/Synchronous Digital Hierarchy (SONET/SDH)* optical networks, which is a standard for sending data over optical fiber.

The grid must be able to adapt dynamically to current demand, monitor for anomalies and failures. To accomplish these tasks, a *Supervisory Control and Data Acquisition (SCADA)* system and grid protection mechanisms are employed. The primary protection mechanism for transmission and distribution is the *current differential relay*. The fundamental operating principle of relays is to compare measured values on the lines of the grid. Upon the detection of a discrepancy, a trip signal is transmitted to trip a circuit breaker. This action breaks the circuit, preventing damage and enabling the safe examination of the causes. As this process necessitates communication over a network, it is also known as *teleprotection* [7] in the industry. In modern smart grids, the devices responsible for activating circuit breakers are referred to as *Intelligent Electronic Devices (IEDs)*. As this paper addresses the communication aspect of power grids from the perspective of networking, we will not delve into the specifics of how these devices work or into electrical engineering.

Despite that, it should be well known that the speed of propagation of electricity in conductors is high, and thus these protection mechanisms must be able to respond quickly without delays caused by protocol overhead to avoid damage to the grid. Thus, the first main criterion for protection device communication is *low latency*. In other words, the *network delay* caused by the devices processing the messages in the network, such as routers, must be as low as possible.

The second main criterion is *redundancy* [8]. The communication of the protection mechanism must be resilient to network failures, as a simple network failure without any redundancy built in, occurring at the same time as a fault in the grid, can lead to negative consequences. Typical network recovery protocols are too slow, hence redundancy is mostly achieved by provisioning of a redundant backup path.

Finally, it is necessary to consider some general protocol requirements. It should be noted that power grid communication is not bandwidth-intensive [3], [9] and the majority of messages are small in size [10]. In many cases, the data to be transmitted is sufficiently small to fit within a single frame or packet. However, there is often a high frequency of such small messages. Therefore, it is necessary to choose a protocol throughput and network bandwidth that will prevent congestion.

B. IEC 61850

The IEC 61850 standard [6], is an emerging standard that is considered the state-of-the-art technology in the field of power grid communication. The objective of the standard is to provide vendor-independent interoperability between devices and to provide a single standard for message formats. It is based on Ethernet technology and provides several protocols: *Generic Object Oriented Substation Event (GOOSE), Sampled Values (SV) and Manufacturing Message Specification (MMS)* protocols.

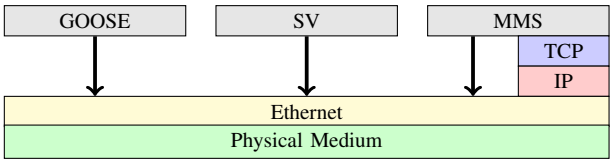

Fig. 1. IEC 61850 network stack. Figure adapted and recreated from [11].

Fig. 1 illustrates the protocol stack of IEC 61850. It is evident that the majority of the protocols function directly upon the Ethernet protocol. Consequently, all the devices must support *Ethernet* in order to form a *Local Area Network (LAN)* within the facility. This approach is adopted in order to avoid the overhead caused by using other higher layer protocols, such as *IP/TCP*, in order to provide low latency communication. The standard employs priority tagging based on *IEEE IEEE 802.1Q* [12] in a *virtual local network (VLAN)* to ensure that time constraints are met. A simplified communication architecture of a substation can be seen in Fig. 2 with devices communicating using the three IEC 61850 protocols. *Merging Unit (MU)* serve as unified digital interface between the digital components of the substation and the analog equipment attached directly to the power lines. It is achieved by converting analog signal from measuring devices and other equipment into a digital signal. Operators of the substation can see and control the devices within the substation from the control stations. We now provide an overview of each

protocol. All of these devices must communicate using the IEC 61850 protocols and we now provide an overview of each one.

1) GOOSE: Generic Object Oriented Substation Event (GOOSE) is an event-based messaging protocol that transmits mission-critical information with strict time constraints. The data contained in GOOSE messages may include status updates, error messages, and control commands [13]. The principal objective of GOOSE is to facilitate the transmission of event-based data between Intelligent Electronic Devices (IEDs) and between IED and MUs. as seen in Fig. 2. These messages are given a high priority within the network, ensuring that IEDs are able to react in a timely manner. GOOSE was originally intended for communication within a substation. However, the latest addition to the standard, IEC 61850-90-1 [14] , enables the usage of GOOSE for communication between substations [15] [16]. As GOOSE messages are embedded directly into Ethernet packets and the standard does not include network and transport layer protocols, two workarounds are recommended in IEC 61850-90-1: tunneling or proxy gateway [14].

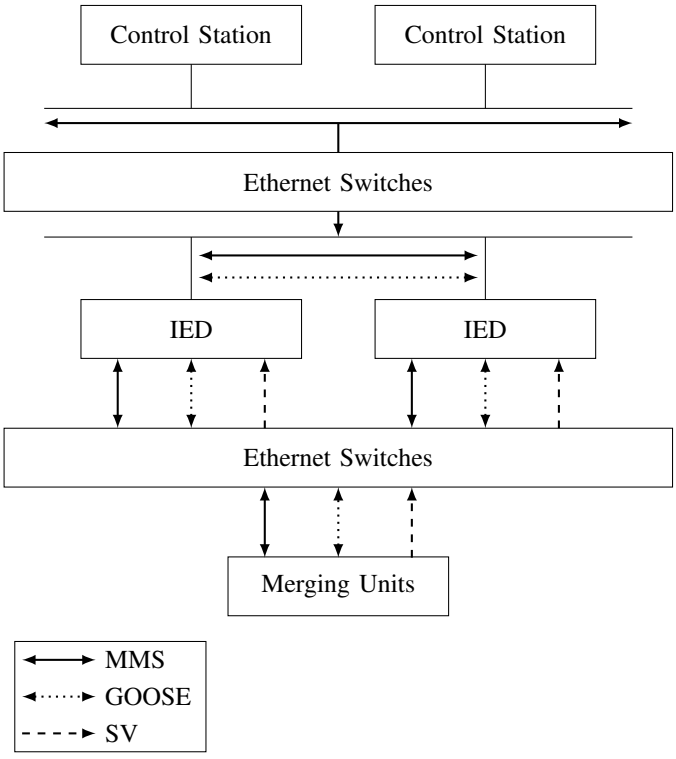

Fig. 2. Typical substation communication architecture. Figure adapted and recreated from [17].

2) SV: In contrast to GOOSE, Sampled Values (SV) transmits messages at regular intervals. As the name suggests, these messages contain sampled measurements of current and voltage. Measurement values must be sampled at different points of the power line and transmitted from a MUs to an IEDs as visible in Fig 2. If discrepancies are detected in the values by the IEDs, they can trip a circuit breaker. The sampling rate is typically either 80 Hz or 256 Hz, which results in a high-bandwidth stream of periodic SV messages. Consequently, the communication needs to have high throughput, low delay, and highly reliable, as these sampled values are used to detect an electrical fault.

3) MMS: Finally, MMS serves as a control protocol and can be directly mapped to Ethernet or used with IP/TCP. Initially, it was not developed for power grids, but its capabilities led to its adaptation into IEC 61850. It serves as a SCADA protocol, so it is primarily used for monitoring and management of devices and has a lower priority than GOOSE or SV messages. As MMS messages are not as critical, they can also be used for long-distance communication between substations or facilities. For this purpose, MMS can be used with IP/TCP. Fig 2 illustrates how MMS messages are sent from the control room computers into the lower layers of the station to control the devices.

C. Network Faults

The protocols in IEC 61850 function directly over Ethernet, with only MMS being capable to function over IP/TCP. In the event of network faults, traditional Ethernet recovery mechanisms are insufficient for our purposes [18]. IEC 61850 specifies delay tolerances, for example, the *SV* protocol requires *"bumpless"* recovery time, meaning there should be no downtime during recovery. For IED to IED communication when performing a reserve block (blocking of reverse current flow), the tolerated recovery delay is *4ms*. Traditional recovery method of Ethernet, such as *Spanning Tree Protocol (STP)*, the network reconfiguration process can take up to a minute [18]. In contrast, the *Rapid Spanning Tree Protocol (RSTP)*, defined in *IEE 802.1w* [19], can reduce the recovery time to a few seconds. However, this is still in the order of magnitude longer than the specified recovery time in IEC 61850. Even more rapid recovery methods, such as *Fast Failure Handling in Ethernet Networks* [20], can achieve recovery times of approximately *50ms*. However, this is still not sufficiently rapid for our bumpless requirement. Consequently, additional protocols or methods are required. The standard therefore includes two recovery methods, which will be presented next.

D. PRP and HSR

In order to achieve the strict recovery tolerances, IEC 61850 stipulates the usage of the IEC 62439-3 standard [21] to achieve zero recovery time communication. The standard specifies two redundancy protocols, namely the *Parallel Redundancy Protocol (PRP)* and *Highly-available Seamless Redundancy (HSR)*. An overview of these protocols will be provided in the following section.

1) PRP: The basic concept of PRP is to achieve redundancy by using two independent networks. This effectively converts zero recovery time to zero packet loss because all messages are duplicated. The figure 3) illustrates the basic principle of PRP. Devices that do not have dual interfaces are called *Single Attached Node (SAN)*. To achieve duplication capacity, they are then connected to the PRP network through *Redundancy Boxes (RedBoxes)*, which have dual interfaces for redundancy.

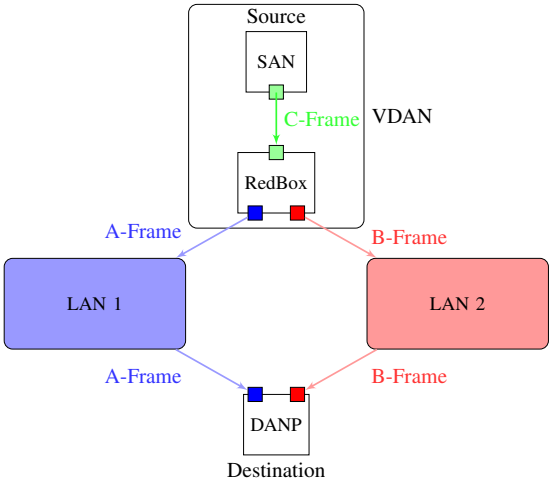

Fig. 3. PRP Network. Figure adapted and recreated from [18].

Such a configuration is called a *Virtual Doubly Attached Node (VDAN)*. The original C-frame from the publishing source is duplicated by the RedBox into an A-frame and a B-frame, which are sent independently over two separate LAN networks A and B. Devices that are natively PRP-enabled with dual interfaces are called *Double Attached Node Implementing PRP (DANP)*, hence such devices do not require a RedBox. The destination device in the example figure is a DANP and it receives both frames, with the one received later being discarded as it is a duplicate.

PRP embeds its protocol-specific information into standard Ethernet frames, specifically into the payload part of the frame. This simplicity enables PRP-enabled networks to use standard Ethernet LAN networks and switches within the networks, with the exception of DANP, SAN, and RedBoxes. For PRP to function properly, the two networks must be separately identifiable, and in the event of failures, each network's failure must be independent of the other. In the event that one of the networks experiences a fault, it must be able to recover quickly enough, as otherwise the redundancy is lost during the downtime period. Furthermore, the travel time of frames over the networks must be approximately equivalent.

2) HSR: HSR also achieves redundancy by duplicating packets, thus preventing any packet loss. However, the method by which this is achieved differs from that of PRP. Unlike PRP, HSR uses its own specified frames, which are incompatible with Ethernet frames and switches, although Ethernet ports and cables are utilized. Consequently, all the devices in HSR networks need to be specialized HSR devices. Similarly to PRP, there are three types of devices: *Double Attached Node Implementing HSR (DANH)*, *RedBoxes* and *SANs*. The main concept is to use a ring network and send frames in both directions. The source device publishes two frames, an A-Frame and a B-Frame, which are sent in both directions of the ring network. Similarly to PRP, the receiving subscribed device discards the duplicate frame. As with PRP, it is necessary for the network to be able to recover quickly in the event of a failure occurring in one part of the ring.

E. Evaluation of PRP and HSR

Based on evaluations from [22] [23] [18], it can be concluded that both protocols achieve good redundancy and permit interoperability between vendors. In terms of performance, PRP appears to be the superior protocol [23]. PRP can utilize standard switches within the LAN network itself, while requiring RedBoxes or dual interface DANP devices to attach critical devices, the necessity of having two independent networks increases the associated cost of switches and Ethernet cabling. In contrast, HSR necessitates a single ring network and the use of specialized devices that support HSR custom frames, while the amount of Ethernet cabling is less. All three evaluations conclude that HSR is a more cost-effective option [22] [23] [18]. On the other hand PRP is more suitable for larger applications, as it offers greater flexibility and enables traffic shaping, which is not possible in a ring network [18].

PRP and HSR are primarily designed for use within a substation. PRP employs Ethernet, which is well-suited to the IEC 61850 standard, where the protocols can be mapped to Ethernet. The protocols can be even combined, for example in Fig. 2 the lower layer network consisting of IEDs and Merging Units can be implemented as a ring network utilizing HSR. Then this ring network can be connected to the control station layer station using a dual LAN connection of PRP.

For longer distance communication between substations, both protocols are can be reduced down to the same concept, a dual independent connection. Creating a long range dual LAN using PRP would require Ethernet over fiber [24]. As standard copper copper cables have a limited transmission range [24]. The same would apply to HSR, as it also uses Ethernet cables. While it is theoretically possible, we do not deem it as a good solution for long distance communication, as it lacks the flexibility and scaling. Therefore we have a look at alternatives to PRP and HSR, which can offer more flexibility.

III. MPLS

An alternative to achieve the redundancy and time constraints desired for power grid protection over long distances would be to utilize or adapt other existing packet based protocols. One of the potential protocols is *Multi-Protocol Label Switching (MPLS)* [25], sometimes also refereed to as *IP/MPLS*. MPLS is protocol that functions between the link and network layer and provides its own form of routing based on labels.

A. MPLS Principles

MPLS is a routing technique utilized for the forwarding of packets within an MPLS network. For MPLS to function, the devices within the network must be MPLS-compatible. The principal objective of MPLS is to diminish network latency, ensure dependable communication, and provide a framework for Quality of Service (QoS).

Packets entering a MPLS network are assigned a label, which is contained in an *MPLS header*. The header determines the *Forwarding Equivalence Class (FEC)* of a packet.

Packets with the same characteristics, such as same destination address, are assigned the same FEC. This process is conducted at the edge routers of the network, which are designated as *Label Edge Routers (LER)*. Subsequently, routers in the MPLS network ignore the IP header, as all the requisite information is contained within the MPLS header. Routers within the network designated as *Label Switch Routers (LSR)* and forward the packets through a designated *Label Switched Path (LSP)*. These paths are calculated upon entry into the network, hence these paths are predetermined. The LSR routers themselves function simply as switches in a circuit-switching network. A crucial aspect of path predetermination is the capacity to create a backup path in the event of a link failure, which provides redundancy aspect of MPLS. Furthermore, FECs can contain *Quality of Service (QoS)* data, which can be utilized to determine the priority of the packet [25]. The benefits of MPLS is its ability to provide reliable, and if desired, low latency communication. Furthermore it is protocol-agnostic, as it can encapsulate Ethernet packets [26] and has been used to create virtual private LANs [27], [28]. This makes it suitable for our type of communications, as it can operate with IEC 61850 protocols, which are mapped to Ethernet. Research has been conducted to utilize MPLS for power grid networks as a way to provide redundancy and low latency communication. A selection of four papers will be presented next.

B. Application of MPLS for Teleprotection

1) Paper 1 [3], by Blair et al.: The paper explores the usage of MPLS with IEC 61850 GOOSE and SV messages. The objective of the paper is to validate the applicability of MPLS with IEC 61850 and considerations on how to achieve full redundancy. A MPLS network is created using MPLS routers. The MPLS routers were connected directly via a full duplex optical link. The power lines are simulated using a *Real-Time Digital Simulator (RTDS)* using the hardware-in-loop method, which enables the simulation and testing the behavior of equipment. Various scenarios were tested to validate the application of MPLS for protection schemes using different payload sizes and number of routers. Electric faults were simulated on the relays and the delays of the trip times caused by network propagation were measured.

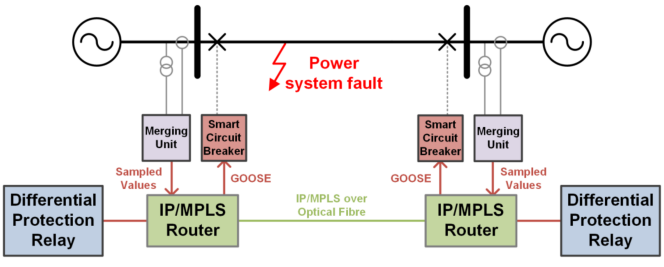

Fig. 4. IEC 61850 test setup. Figure taken from [3].

The test setup is depicted in Fig. 4. A simulated merging unit generates a stream of SV messages by taking measurements on the power line. The SV data is transmitted to relays, which serve as IEDs and analyze the data. In the event of a fault being detected, the relays transmit a GOOSE trip message to the local and remote circuit breakers. A virtual private LAN (VLAN) is created to transmit the Ethernet-embedded SV and GOOSE messages over the MPLS network to the other end of the power line..

To validate the feasibility of MPLS, it is necessary to consider two different types of delays. The first is *network delay*, which is caused by the propagation time of the signal in the network combined with the processing time at routers. The second type of delay is the *failure switchover time*, which is the time required for communication to recover after a link failure has occurred. The network delay of the remote circuit breaker trip using GOOSE and SV was $24.9ms$.

Failure switchover time depends on the network topology. To achieve redundancy using MPLS by utilizing its backup paths, the network must have multiple paths available. To establish this, the authors consider a ring MPLS network. When a link in one half of the ring fails, MPLS is able to switchover to the other half of the ring. In testing the failure switchover time was $< 50ms$. To achieve the bumpless requirement, the authors recommend having an additional separate redundant path, which lies outside of the ring network, on which all data sent on the ring network is duplicated. This solution effectively provides three paths with no switchover time. When a link in the ring fails, we still have the alternative path in the ring and the separate redundant path. However even with full redundancy, in case of a link failure, the devices might experience a small delay caused by the different network delays of different paths. For example increasing the number of hops in the network had a increase of delay of up to 30µs her hop. In principle this is a combination of PRP and HSR. One of the dual LANs of PRP is implemented as a HSR ring with an another separate redundant path acting as the second LAN. In conclusion, to achieve a seamless transition in the event of a link failure, the network path must be sufficiently diverse to provide multiple active paths. By employing a MPLS network, we can circumvent the delay that can be caused by the protocol overhead of IP/TCP. Furthermore, MPLS offers enhanced flexibility [29] and range compared to Ethernet when used over longer distances.

C. MPLS-TP

Research has also been conducted on the potential application of a variant of MPLS, namely *MPLS Tunnel Profile (MPLS-TP)*, in power grid communication Main difference between basic MPLS and MPLS-TP is the removal of some features, for example Penultimate Hop Popping or Equal Cost Multi Path. These features are not necessary nor utilized in our use case, resulting in a more lightweight protocol. While this protocol may not be suitable for a general purpose network, it still has the necessary parts for our purposes.

D. Application of MPLS-TP for Teleprotection

1) Paper 2 [2], by Blair et al.: The objective of this paper is to ascertain the viability of utilizing MPLS-TP over

a SDH/SONET network for communication between protection relays in the presence of other Ethernet traffic within the network. The general configuration is analogous to that described in reference 4, wherein a Merging Unit (MU) is emulated to generate SV data. The MU is connected locally to a circuit breaker via Ethernet. At the opposite end of the line, we have a remote circuit breaker situated within its own Ethernet network. The two Ethernet networks are connected via a MPLS network over an SDH/SONET optical network. In this instance, we have also have additional Ethernet traffic injected into the MPLS network. SV and GOOSE messages are utilized to trip the local and remote circuit breakers. The local relay need to activate a circuit trip on the remote relay, and the delay between the activation is measured. Three potential routes exist for traversing the MPLS network to reach the other end. In contrast to the previous paper, which recommended a separate redundant path with duplication, this paper does not include such a path. Consequently, it is up to MPLS to provide a switchover in case of a link failure.

According to the tests done by the authors, the network delay for SV traffic was less than $20\mu s$ and for GOOSE messages between $20 - 40\mu s$. The effect of link failures can vary for GOOSE messages, in the best case it has no effect when the failure occurs when there are no GOOSE messages to be transmitted. In the worst case, a failure can lead up to $64ms$ delay, when a network failure causes a GOOSE message to be lost and it has to be re-transmitted. For the case of SV, network failures could induce a delay of $26 - 40ms$. In both cases the message were set with high priority and injection of additional traffic into the network had negligible impact. However network failures induced a noticeable delay for SV and GOOSE messages. This reinforces the recommendations from III-B1 and the operating principles of PRP and HSR. In case of a link failure, MPLS alone is not able to provide a bumpless switchover. In order to meet the requirements, an additional redundant path is required to duplication of messages.

2) Paper 3 [30], by Ghanem et al.: Ghanem et al. tests the usage transmitting GOOSE messages using MPLS-TP network over SDH/SONET. The goal again is to test delay between relays, but with a focus on introducing artificial latency and transmission bit errors to simulate a link failure, instead of a complete link failure. Without any introduced errors, GOOSE functioned within acceptable parameters with an average network delay of $5ms$. By causing a bit error rate of 10^{-4} or higher the communication has failed, as the relays can not operate at this high of a bit error rate. If the high priority of messages was implemented correctly and 10% of the bandwidth allocated for our traffic, then introducing other traffic into had no impact. Jitter is an important aspect of connection stability is *jitter*. It represents the deviation and irregularity of the periodicity of packet receival. All communication suffer from some jitter, the lower the jitter the more stable is the connection. It is often solved by introducing a jitter buffer, which collects and stores packets briefly for a set amount of time. By introducing network jitters ranging up to $1ms$ the network was stable albeit with increase propagation delays with up to $9ms$.

E. Multi-path MPLS

Rather than relying on a backup redundant route for duplication, it would be advisable to consider the potential benefits of utilizing a multi-path connection within MPLS itself [31]. To best of our knowledge no research has been conducted on the specific application or testing of multi-path MPLS in the context of the power grid. There are several proposals for the implementation of multi-path MPLS in general.

In their work, "Multi-path MPLS Scheme," Xiao Yu et al [32] propose a solution for failure recovery and bandwidth allocation. The scheme initially identifies a set of disjoint paths between the source and destination. Subsequently, it can select a set of active paths and a set of backup paths. For the selected path, a variety of proposed policies can be implemented to allocate bandwidth and address failure recovery. Similarly Emeshko et al. [33] propose multi-path routing with a focus on load balancing based on QoS parameters, primarily the delay.

Both proposals face the challenge of first determining and choosing the paths, which is not a trivial task. Multi-path routing is a common approach to increasing throughput, whereby traffic is split into multiple paths. However, if the principle of PRP II-D1 is applied, it could be adapted to achieve redundancy in a MPLS network. This would entail actively sending the same data over two different routes within a MPLS network. However, this only applies if the network is relatively static. Otherwise, new paths would need to be recalculated, which would result in unacceptable delays for our use case.

IV. Multi-path Transport Layer

A different approach to achieve redundancy with respect to our constraints would be to use a higher level transport layer protocol to achieve redundancy. Specifically to use utilize multi-path protocols.

A. MPTCP

The first the possibility is *Multi-Path TCP (MPTCP)* [34], which is a variant of *TCP*. A MPTCP connection is established via the standard three-way-handshake as is the case with regular TCP. Subsequently, supplementary TCP connections, so called *sub-flows* are established. These sub-flows are capable of being routed independently of one another over disparate network paths. MPTCP divides the data stream into these discrete sub-flows, thereby enhancing the overall throughput efficiency. This has the additional consequence of introducing redundancy through the establishment of multiple active connection

While increasing throughput is a benefit, it is not necessary one of our main goals. The goal of utilizing MPTCP in our context is to achieve redundancy. However when utilizing a protocol like TCP, which involves handshakes, window sizes and congestion control, new problems occur. These features, which facilitate reliability for typical internet traffic,

can potentially introduce delays. This is one of the reasons why the IEC 61850 protocols directly utilize Ethernet for faster communication, thus avoiding the overhead of TCP. Furthermore, TCP/MPTCP functions normally in conjunction with the IP protocol for routing, as TCP/MPTCP does not have routing functionality. This can cause even more network-induced delays from packet header processing. In the context of power grids, WANs often employ a private, dedicated IP network. These networks can be enhanced through the utilization of MPTCP. Not much research has been published about utilizing MPTCP for usage in power grid communication. Nevertheless, research from a related domain, namely railway communication, offers insights that are analogous to those encountered in the power grid context.

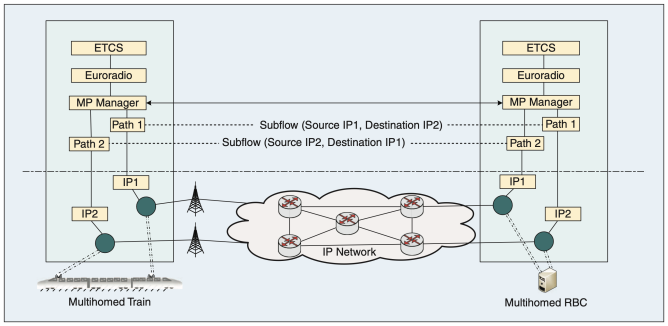

Fig. 5. Communication Model of Trains. Figure taken from [35].

B. MPTCP in Railways

Railway communication, particularly in the domains of signaling and control, is subject to high reliability requirements, as a communication failure could potentially result in a catastrophic crash. Like power grids, it still employs legacy technologies, which is problematic given the dynamic and prone-to-disturbance nature of the environment in which communication occurs. Furthermore, railway signaling has delay constraints, especially the automated parts, which are triggered when an operator error occurs. Finally, the communication has high security requirements, which are similar to those of power grids. Therefore, the research and lessons from railways could be applicable for our use case.

1) Paper 1 [35], by Lopez et al.: In order to address the aforementioned issues and requirements, Lopez et al. put forth the use of a solution based on MPTCP, designated as *RMPTCP*. As in our case, the objective is not to enhance throughput but to achieve redundancy. This is achieved through the implementation of a redundant delivery policy, which stipulates the transmission of messages over all available paths. In the event that one or more of the paths experiences a fault, provided that at least one of them remains available, the recipient is expected to receive the message. Furthermore, the congestion control mechanism for multi-path sub-flows is removed. Normally, congestion control is employed to identify the absence of TCP segments. Given that the message is received multiple times over several sub-flows, it can be inferred that the connection is functional as long as at least one sub-flow is operational. The re-transmission method has also been modified to function more effectively when utilizing multiple redundant sub-flows. Instead of simply using a timeout timer for all connections, the sender now performs an individual check on each sub-flow to ascertain whether an acknowledgment has been received. This allows the sender to make an informed decision regarding the necessity of re-transmission. This approach was developed to address a specific domain issue in the context of rail transportation, namely the handover of communication during the movement of a train. An overview of the communication model can be seen in Fig. 5. A manager for the multiple paths is responsible for the multiple sub-flows, each of which takes a different path in the network. The layers above them MP manager belong to the *European Train Control System (ETCS)*, a unified railway protection system designed to replace the various incompatible country-specific systems. The authors conclude that having sufficient sub-flows can lead to 100% communication availability.

Using this method would require the usage of IP, since TCP, MPTCP nor RMPTCP has routing capabilities, or some other protocol must be used to bridge the gap. In the event of IP utilization, the question arises as to whether power grid communication should be conducted on an isolated IP network or on the publicly available network, particularly in instances of long-distance communication between substations or isolated generation facilities such as windmill farms. The latter option gives rise to a security concern. Furthermore, the question of how to create multiple independent sub-flows arises. One potential solution is to combine both land-based wired communication with wireless communication, such as the wireless telephone network or satellite communication.

2) Paper 2 [36]: Using MPTCP in conjunction with MPLS addresses the issue of routing, as MPLS provides the requisite routing capability. This was done by some of the same authors as in the RMPTCP approach for railway signaling communication. Similarly, MPTCP is employed as a redundancy method, whereby the same data is transmitted over all MPTCP sub-flows. This method of operation was previously presented in their paper [37], in which it was used for *Modbus* [38], a railway SCADA system to reduce effects of network link failures and Distributed Denial of Service (DDoS) attacks.

The combination of these two approaches provides temporal and path diversity, thereby achieving redundancy. By dividing the MPTCP sub-flows across a MPLS network, it is possible to direct each sub-flow along a different path. Furthermore, the MPLS network is equipped with the necessary features to cope with link failures. Moreover, their approach introduces a principle of temporal redundancy, whereby the same data is sent over multiple sub-flows, with a built-in delay for sub-flows. This allows the data to arrive at the receiver multiple times with some delay. The objective is to eliminate the necessity for TCP re-transmission, which is considerably more time-consuming. The receiver does not immediately initiate a re-transmission request, as demonstrated by the authors in their

test scenario, which can take up to $500ms$.

C. MPTCP As Security Against Attacks

In the context of power grids, MPTCP has been explored as a method to achieve resilience against attacks by Farooq et al. in [39]. *Phasor Measurement Units (PMUs)* are used to measure the properties of electricity on various parts of the larger grid, often at a distance from substations in the distribution part of the grid. The majority of these devices utilize the *IEEE C37.118* [40] framework for communication. It is also possible to use IEC 61850 GOOSE and SV messages, although this newer standard is not yet supported by all devices. The location of PMUs often necessitates their use of publicly available networks, as previously mentioned. This poses a significant challenge, as these devices can be compromised and used for a DDoS attack. The authors of the paper propose utilizing an MPTCP-based technique of port hopping, which employs MPTCP's capabilities to create new sub-flows with a new port number, thus mitigating the effect of attacks. By changing the ports with new sub-flows, the attacker's DDoS messages are avoided.

D. MPQUIC

QUIC [41] is an emerging transport protocol, which utilizes UDP datagrams. An extension of QUIC, *Multi-path QUIC (MPQUIC)* [42] could be of use for application in power grid protection redundancy.

While to best of our knowledge there is published research or application of QUIC nor MPQUIC, we can still explore its potential. QUIC was developed as a general-purpose transport protocol. While it is designed to serve as a transport protocol, it actually utilizes the existing transport protocol UDP. Compared to TCP, UDP provides connectionless and unreliable communication. Many of the mechanisms and features of TCP are missing, but this simplicity makes UDP much faster. QUIC employs UDP and implements the desired functionalities of TCP in its own right. Initially developed by Google and subsequently standardized by the Internet Engineering Task Force (IETF), its most prevalent deployment is in web browsers in conjunction with the HTTP3 protocol. The objective of QUIC is to reduce the latency associated with TCP.

MPQUIC is an extension of QUIC, which functions in a similar fashion as MPTCP to TCP, by creating additional sub-connections to increase the throughput. Several papers compare MPTCP and MPQUIC: [43], [44], [43]. The protocols were tested in various scenarios including mobile wireless communication, transmission of big files and non HTTP usage. In general, MPQUIC demonstrated superior performance compared to MPTCP. However, the outcome is influenced by various factors, including the implementation of both protocols, configuration, and the specific use cases. MPQUIC is a novel protocol that is still undergoing active development. Therefore, it is anticipated that future performance enhancements will be achieved.

If it is possible to successfully apply MPTCP in railways signaling communication, it would be reasonable to suggest that MPQUIC could be applied as well. If MPQUIC is capable of exceeding the capabilities of MPTCP, it could also be applied in power grids.

V. Comparison and integration

A. Local Communication

For local communication within a facility, all the protocols presented are compatible with Local Area Networks (LANs), so IP/TCP is not strictly necessary. The PRP and HSR protocols included and stipulated by the IEC 61850 standard are designed for LANs and function reasonably well [22] [23] [18]. The studied and presented proposals of adopting MPLS, its sub-variant MPLS-TP, MPTCP or MPQUIC would be beneficial. Theoretically MPLS does not require a routing protocol such as IP, though in practice it would not be advisable to disable or drop the support of IP. However the benefits seem to be marginal in a LAN that is specifically designed and we have full control of. If the LAN infrastructure is already fully functional in accordance with the specifications of IEC 61850, then we deem it unnecessary to introduce additional enhancements. Moreover the investment of new devices such as MPLS enabled routers and reconfiguration of the network leads to a downtime and monetary investment. Conversely, when upgrading an existing infrastructure from legacy systems to a modern system, which is a significant investment in itself, it may be prudent to implement a MPLS network for its flexibility and scalability, as a means of future-proofing.

B. Remote Communication

For longer distance communication between facilities a WAN is necessary. Techniques such as tunneling or proxy gateway approach are used [16] over a SONET/SDH network, which emulate circuit switching. It is possible use MPLS over SONET/SDH to provide Ethernet services, in other words to create a larger LAN, as demonstrated in reference III-D2. It is also possible for IP to work over SONET/SDH [45], which would permit the implementation of MPTCP or MPQUIC. Faults may occur at remote locations or even remote, inaccessible locations. For this kind of application, it is reasonable and justified to install mechanisms such as MPLS or MPTCP/MPQUIC. Although not much research exists about utilizing MPTCP nor MPQUIC to achieve the redundancy in the context of power grids.

Table I provides an overview of the three options at disposal. Of the options MPLS seems to be the most suitable for our needs, as evidenced by the extensive research conducted on its applications.MPLS and its variant, MPLS-TP, are feature-rich and provide routing, priority configuration, and backup paths. MPLS can be easily integrated with IEC 61850. It can directly use Ethernet or any proprietary frames as payload. As the protocols IEC 61850 use Ethernet and Ethernet switches can be directly connected to MPLS routers. This enables the implementation of bumpless link failure switchover, which is achieved by having an alternative path in the MPLS network and an additional redundant path. When the concept

is correctly implemented, it can provide fast and reliable communication, as demonstrated in the presented papers and various other papers that exist. The delay induced by the network is acceptable, and it is possible to achieve full redundancy. One disadvantage of MPLS is that MPLS-enabled routers are required. Additionally, the network must be diverse enough and have multiple possible paths for the redundancy mechanisms to work. This introduces the cost of setting up a MPLS network. However, for the use case of grid protection for long-distance communication, these costs can be justified.

Compared to MPLS, MPTCP's and MPQUIC's features can be utilized redundancy. They require a routing protocol like IP and have limited control over what happens on the lower protocols. Packets can be dropped at routers due to congestion, and TCP's congestion control then intervenes and lowers the throughput. Such occurrences can occur when using a publicly available IP network, though this introduces a significant security concern and should be avoided. Consequently, utility companies frequently utilize their own private IP networks. In the event that a secure infrastructure is already in place, the deployment of MPTCP or MPQUIC would be advantageous. However, this is contingent upon the network being sufficiently diverse to offer multiple potential paths between endpoints, which is the same requirement as with MPLS. This leads to the question of why not simply utilize MPLS. Of the two transport protocols, QUIC was designed to overcome the limitations of TCP. Therefore, QUIC or MPQUIC appears to be a superior option to TCP.

An alternative approach would be to utilize the PRP or HSR protocols, as stipulated by the standard, even for longer distance communication. However, these protocols are not suitable for the intended application. Ethernet technology alone is not suitable for such distances. HSR requires a ring topology of specialized devices with a significantly higher cost and is incompatible with standard Ethernet switches.

VI. Conclusion

The modern smart grid IEDs require reliable and low-latency communication to properly manage and protect the grid, therefore of critical importance. This communication must be reliable and low-latency to ensure the grid is managed and protected properly. We have presented several protocols included in the IEC 61850. The standard also includes two redundancy and recovery protocols PRP and HSR, of which the former works by having two independent LAN networks and the latter by having a ring topology network. Both of the protocols function well in a local communication within a substation, but are not suitable for longer distance communication between facilities.

We explored the idea of enhancing the resiliency of the IEC 61850 communication protocols by introducing and demonstrating how MPLS can be utilized to achieve redundancy while maintaining the strict time constraints necessary for IEDs. MPLS is a protocol that functions between layers 2 and 3 of the Open Systems Interconnection (OSI) model and provides routing based on labels attached to packets. Using the labels, an optimal path can be determined, and priorities can be assigned to distinguish between high-priority and low-priority messages. Additionally, it can be configured to achieve the bumpless switchover in case a network failure occurs, as required in the IEC standard.

TABLE I
Potential Protocols for Power Grid Communication

Overview of Protocols	**Protocols**		
	MPLS	***MPTCP***	***MPQUIC***
Protocol Type	Layer 2-3 Routing	Transport	Transport Utilizing UDP
Equipment Requirements	MPLS Routers	End-User Support	End-User Support
Use Case	Redundancy Lower Latency	Mainly Redundancy	Mainly Redundancy

An alternative to MPLS would be the use of multi-path protocols MPTCP or MPQUIC. There has been little research conducted on the use of these protocols in power grids. However, there is research on their use in railway signaling. The constraints in this context are similar to those in power grids, as the signaling data must be reliable and fast in order to avoid accidents on the rails. Both of the protocols leverage the use of multiple active sub-flows through different paths to achieve redundancy. QUIC and MPQUIC are relatively new protocols designed to address the shortcomings of TCP and MPTCP. Therefore, they appear to be a more suitable choice. However, QUIC is still in active development and further enhancements are possible. Additionally, meeting the strict delay constraints when using these transport protocols is more challenging due to their function at a higher layer of the OSI stack. This is precisely why the IEC 61850 standard functions directly on Ethernet to avoid the overhead of other higher protocols. The findings of this survey indicate that the implementation of MPLS on long-distance communication between facilities to achieve redundancy is a recommended approach, as it fulfills all of the specified requirements. However, this approach is associated with the potential drawbacks of cost and the necessity for network diversity. The implementation of MPLS in the LAN network of a substation appears to be an unnecessary expense, as the PRP and HSR protocols function adequately in this environment using only Ethernet or HSR networks, respectively. Nevertheless, it is generally beneficial to transition to a newer packet-based network.

References

[1] N. Sharma, A. Acharya, I. Jacob, S. Yamujala, V. Gupta, and R. Bhakar, "Major blackouts of the decade: Underlying causes, recommendations and arising challenges," in *2021 9th IEEE International Conference on Power Systems (ICPS)*, 2021, pp. 1–6.

[2] S. M. Blair, C. D. Booth, J. Michielsen, and N. Joshi, "Application of MPLS-TP for transporting power system protection data," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, pp. 619–624.

[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," in *2014 CIGRE Session*, FRA, August 2014. [Online]. Available: https://strathprints.strath.ac.uk/48971/

[4] IEE, "Ieee vision for smart grid communications: 2030 and beyond reference model," *IEEE Vision for Smart Grid Communications: 2030 and Beyond Reference Model*, pp. 1–11, 2013.

[5] M. Yalla, M. Adamiak, A. Apostolov, J. Beatty, S. Borlase, J. Bright, J. Burger, S. Dickson, G. Gresco, W. Hartman, J. Hohn, D. Holstein, A. Kazemi, G. Michael, C. Sufana, J. Tengdin, M. Thompson, and E. Udren, "Application of peer-to-peer communication for protective relaying," *IEEE Transactions on Power Delivery*, vol. 17, no. 2, pp. 446–451, 2002.

[6] I. E. C. (IEC), "IEC 61850:2024 SER," International Electrotechnical Commission, Geneva, CH, Standard, 2024.

[7] J. Blackburn and T. Domin, *Protective Relaying: Principles and Applications, Second Edition*, ser. Chemical Industries. Taylor & Francis, 1997. [Online]. Available: https://books.google.de/books?id=cdvOkSSvqEAC

[8] S. Xu, J. Ma, L. Cao, W. Hu, L. Chen, H. Lu, B. Liu, and Z. Dai, "Reliability evaluation of centralized protection system in smart substation considering impact of communication message," in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2018, pp. 1–6.

[9] Y.-h. Yi, L.-t. Wang, and Y.-j. Tao, "Research of network transmission of process bus based upon iec 61850," in *2011 International Conference on Advanced Power System Automation and Protection*, vol. 2, 2011, pp. 1578–1582.

[10] K. Ghanem, R. Asif, S. Ugwuanyi, and J. Irvine, "Bandwidth and security requirements for smart grid," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 36–40.

[11] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Communications Surveys I& Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[12] IEEE, "IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks," *IEEE Std 802.1Q-2022 (Revision of IEEE Std 802.1Q-2018)*, pp. 1–2163, 2022.

[13] ——, "IEEE Recommended Practice for Implementing an IEC 61850-Based Substation Communications, Protection, Monitoring, and Control System," *IEEE Std 2030.100-2017*, pp. 1–67, 2017.

[14] I. E. C. (IEC), "IEC TR 61850-90-1:2010," International Electrotechnical Commission, Geneva, CH, Standard, 2024.

[15] S. M. Niejahr J, Schuster N, "Substation to substation (ss2ss) GOOSE exchange for critical relay operations," Jul 2010.

[16] I. Ali, S. M. S. Hussain, A. Tak, and T. S. Ustun, "Communication modeling for differential protection in IEC-61850-based substations," *IEEE Transactions on Industry Applications*, vol. 54, no. 1, pp. 135–142, 2018.

[17] J. Park, E. In, S. Ahn, C. Jang, and J. Chong, "IEC 61850 standard based MMS communication stack design using OOP," in *2012 26th International Conference on Advanced Information Networking and Applications Workshops*, 2012, pp. 329–332.

[18] R. Hunt and B. C. Popescu, "Comparison of PRP and HSR networks for protection and control applications," 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:185967238

[19] IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges: Amendment 2 - Rapid Reconfiguration," *IEEE Std 802.1w-2001*, pp. 1–116, 2001.

[20] J. Farkas, C. Antal, L. Westberg, A. Paradisi, T. R. Tronco, and V. G. De Oliveira, "Fast failure handling in Ethernet networks," in *2006 IEEE International Conference on Communications*, vol. 2, 2006, pp. 841–846.

[21] I. E. C. (IEC), "IEC 62439-3:2021," International Electrotechnical Commission, Geneva, CH, Standard, 2021.

[22] C. Hoga, "Seamless communication redundancy of IEC 62439," in *2011 International Conference on Advanced Power System Automation and Protection*, vol. 1, 2011, pp. 489–494.

[23] S. Kumar, N. Das, and S. Islam, "Implementing PRP and HSR schemes in a HV substation based on IEC62439-3," in *2018 Condition Monitoring and Diagnosis (CMD)*, 2018, pp. 1–5.

[24] IEEE, "Ieee standard for ethernet," *IEEE Std 802.3-2022 (Revision of IEEE Std 802.3-2018)*, pp. 1–7025, 2022.

[25] A. Viswanathan, E. C. Rosen, and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, Jan. 2001. [Online]. Available: https://www.rfc-editor.org/info/rfc3031

[26] D. Tappan, Y. Rekhter, A. Conta, G. Fedorkow, E. C. Rosen, D. Farinacci, and T. Li, "MPLS Label Stack Encoding," RFC 3032, Jan. 2001. [Online]. Available: https://www.rfc-editor.org/info/rfc3032

[27] E. C. Rosen and L. Andersson, "Framework for Layer 2 Virtual Private Networks (L2VPNs)," RFC 4664, Sep. 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4664

[28] M. Bocci, I. Cowburn, and J. Guillet, "Network high availability for ethernet services using ip/mpls networks," *IEEE Communications Magazine*, vol. 46, no. 3, pp. 90–96, 2008.

[29] P. Beaumont, F. Kawano, A. Kawarada, T. Kase, H. Sugiura, F. Lam, J. Hurd, P. Worthington, D. Richards, and P. Merriman, "Performance evaluation of current differential relays over a wide area network," in *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*, 2012, pp. 1–6.

[30] K. Ghanem, S. Ugwuanyi, and J. Irvine, "IP/MPLS and MPLS/TP teleprotection latencies over high voltage power lines," in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2023, pp. 381–386.

[31] C. Villamizar, "Use of Multipath with MPLS and MPLS Transport Profile (MPLS-TP)," RFC 7190, Mar. 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7190

[32] X. Yu, G. Feng, K. L. Gay, and chee Khang Siew, "An integrated design of multipath routing with failure survivability in MPLS networks," in *The Ninth International Conference onCommunications Systems, 2004. ICCS 2004.*, 2004, pp. 508–513.

[33] O. Lemeshko, T. Vavenko, and K. Ovchinnikov, "Design of multipath routing scheme with load balancing in MPLS-network," in *2013 12th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, 2013, pp. 211–213.

[34] A. Ford, C. Raiciu, M. J. Handley, O. Bonaventure, and C. Paasch, "TCP Extensions for Multipath Operation with Multiple Addresses," RFC 8684, Mar. 2020. [Online]. Available: https://www.rfc-editor.org/info/rfc8684

[35] I. Lopez, M. Aguado, and E. Jacob, "End-to-End Multipath Technology: Enhancing availability and reliability in next-generation packet-switched train signaling systems," *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, pp. 28–35, 2014.

[36] I. Lopez, M. Aguado, D. Ugarte, A. Mendiola, and M. Higuero, "Exploiting redundancy and path diversity for railway signalling resiliency," in *2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT)*, 2016, pp. 432–439.

[37] I. Lopez, M. Aguado, C. Pinedo, and E. Jacob, "SCADA systems in the railway domain: Enhancing reliability through Redundant MultipathTCP," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, 2015, pp. 2305–2310.

[38] Modbus Organization, *Modbus Messaging on TCP/IP Implementation Guide V1.0b*, 2006. [Online]. Available: http://www.modbus.org/specs.php

[39] S. M. Farooq, S. Nabirasool, S. Kiran, S. Suhail Hussain, and T. S. Ustun, "MPTCP based mitigation of Denial of Service (DoS) attack in PMU communication networks," in *2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, 2018, pp. 1–5.

[40] IEEE, "IEEE Standard for Synchrophasors for Power Systems," *IEEE Std C37.118-2005 (Revision of IEEE Std 1344-1995)*, pp. 1–65, 2006.

[41] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," RFC 9000, May 2021. [Online]. Available: https://www.rfc-editor.org/info/rfc9000

[42] T. Viernickel, A. Froemmgen, A. Rizk, B. Koldehofe, and R. Steinmetz, "Multipath QUIC: A deployable multipath transport protocol," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[43] T. Schmidt, J. Deutschmann, K.-S. Hielscher, and R. German, "POSTER: Revisiting Multipath QUIC experiments and comparing them with more recent Multipath TCP implementations," in *2021 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, 2021, pp. 1–2.

[44] Q. De Coninck and O. Bonaventure, "MultipathTester: Comparing MPTCP and MPQUIC in mobile environments," in *2019 Network Traffic Measurement and Analysis Conference (TMA)*, 2019, pp. 221–226.

[45] X. Deng, Z. Huang, S. Su, C. Liu, G. Tang, and Y. Zhang, "Research of information processing on SDH backbone networks," in *2008 Second International Conference on Future Generation Communication and Networking*, vol. 1, 2008, pp. 395–398.