# Channel Performance Considerations for Ethernet Circuits Applied to Teleprotection

**Power System Relaying and Control Committee**
**Report of Working Group H32**
**of the**
**Relaying Communications and Control Subcommittee**

**Members of the Working Group**


**Ken Fodero, Chair** **Walter McCannon, Vice-Chair**

Jay Anderson
Galina Antonova
Marc Benou
Phil Beaumont
Jorg Blumschein
Jeff Brown
Rolland Cooke
Tom Dahlin
Thomas Flanagan
Christopher Huntley
Mike Keating
Craig Palmer
Bruce Pickett
Dan Reckerd
Takaya Shono
Tuan Tran
Solveig Ward

## KEYWORDS

Channel Asymmetry
Channel Latency
Committed Information Rate
Delay Variation
Ethernet Transport
Jitter
Network Failover
Performance Requirements
Queue Scheduling
Teleprotection

## ACRONYMS

BER - Bit Error Rate
FDM – Frequency Division Multiplexing
GOOSE – Generic Object-Oriented Substation Event
LAN – Local Area Network
MTBF - Mean Time Between Failure
RDI - Remote Defect indication
TDM – Time Division Multiplexing
VF – Voice Frequency
WAN – Wide Area Network
WECC – Western Electricity Coordinating Council

# CONTENTS


1. Introduction ..... 1
2. Scope ..... 1
3. Purpose ..... 1
4. General communications channel performance considerations for teleprotection ..... 2
   - 4.1 Availability ..... 2
   - 4.2 Channel Latency (end-to-end delay) ..... 3
   - 4.3 Delay Asymmetry ..... 4
   - 4.4 Channel Quality ..... 5
   - 4.5 Performance Monitoring ..... 5
   - 4.6 Performance Recommendations ..... 5
5. Ethernet communications channel performance considerations for teleprotection ..... 6
   - 5.1 Ethernet Network Architecture ..... 6
   - 5.2 Ethernet Switch Queues ..... 7
   - 5.3 Queue Priorities ..... 8
   - 5.4 Jitter or Delay Variation ..... 9
   - 5.5 Network Engineering ..... 9
   - 5.6 Path Planning Considerations ..... 10
   - 5.7 Network Failover ..... 10
6. Conclusion ..... 12
7. REFERENCES ..... 12

Appendix A - Sample Protection Communication Requirements Agreement Form ..... 13

THIS PAGE LEFT BLANK INTENTIONALLY

# 1. Introduction

The communication channel is a part of the protection system and enables fulfillment of the protection system requirements. Generally, communication technologies evolve much faster than protective relaying technologies. The current shift towards packet-based data switching, such as Ethernet communications, presents new challenges as characteristics of new packet-based communications are less deterministic than those of traditional Time Division Multiplexing (TDM). By its nature performance of packet-based switching depends on resource availability, while TDM communications utilize dedicated resources.

As protection engineers face the transition to Ethernet-based communications, understanding their operation and expected performance becomes crucial for achieving required reliability of the protection systems.

# 2. Scope

This report discusses the use of Ethernet transport for teleprotection services (directional comparison pilot protection, transfer trip and line current differential protection); plus, the circuit performance considerations for these circuits including latency, channel asymmetry, delay variation (jitter), failover considerations. Legacy TDM interfaces carried over these networks, synchronous 64 kbps (electrical & optical) and asynchronous EIA 232 will be impacted more severely than teleprotection signals that are natively Ethernet.

This report provides general considerations applicable to Ethernet and other packet-based communication technologies. Environmental conditions are out of scope for this report.

# 3. Purpose

The assignment of this working group was to create a document for use by protection engineers with their IT / Telecom counterparts to agree on the expected performance of protective relay circuits applied over Ethernet circuits. This report discusses the various considerations and explains why they are important to the protective relay applications. This document is intended to aid the protection engineer to communicate and document the performance for teleprotection circuits.

A Sample Protection Communication Requirements Agreement Form is provided in Appendix A for the protection engineer to share with potential suppliers of communications equipment and services in order to determine that the communications systems can and will provide the required end-to-end performance, particularly for latency and asymmetry.

# 4. General communications channel performance considerations for teleprotection

General communications channel performance parameters outlined in this section apply to all teleprotection systems regardless of the communications network technology (TDM or Ethernet).

## 4.1 Availability

Service availability and system reliability are crucial in the deployment of equipment used in communications networks. Availability is a measurement of time lost, indicating how infrequently the functionality of equipment is impacted by a failure or defect. It is calculated by dividing the mean time between failure (MTBF) by the sum of the MTBF and the mean time to repair (MTTR). The formula used to determine system availability is as follows:

$$Availablity = MTBF \div (MTBF + MTTR)$$

Reliability is an important element when selecting equipment used in telecom networks. Reliability is a measure of the frequency of equipment failures as a function of time, typically expressed in yearly intervals. The ability of the equipment to operate under stated conditions, such as harsh environments, may be considered for increased reliability. Engineers need to understand the impact of individual equipment reliability on the overall end-to-end service availability.

Availability and reliability became a focal point for network design when moving to multiplexed communications since a single failure will impact multiple applications. Availability and reliability were addressed in the SONET Telcordia Technologies Generic Requirements GR-253-CORE, Issue 4, December 2005 [1] which stated that "the underlying foundation for many system reliability criteria is an end-to-end two-way availability objective of 99.98% (0.02% unavailability or 105 minutes/year maximum downtime) for interoffice applications and 99.99% for loop transport between the central office and the customer's premises". IEC 60834-1 Figure 21 also specifies 99.99% [1].

The criteria for protection system availability is typically specified as 99.999% or commonly referred to as "5 nines". This availability can be achieved by eliminating single points of failure in equipment such as having redundant processors and power supplies as well as using redundant circuits (primary and backup). Also, network availability can be improved by deploying ring and mesh topologies and equipment that can automatically switch traffic around a failed path. The faster the failover, the quicker the restoration, the better the network availability. Another consideration for improving availability is addressing environmental performance, which is outside the scope of this report.

Availability is typically expressed as a percentage or unavailability (time lost). Below is a table for availability based on a one-year interval:

| Availability | Time Lost (hours) | Time Lost (minutes) | Time Lost (seconds) |
|---|---|---|---|
| 99.90% | 8.76 | 525.6 | 31596 |
| 99.98% | 1.75 | 105.12 | 6307.2 |
| 99.99% | 0.876 | 52.56 | 3153.6 |
| 99.999% | 0.0876 | 5.26 | 315.26 |
| 99.9999% | 0.00876 | 0.53 | 31.536 |
| 99.99999% | 0.000876 | 0.05 | 3.1536 |
| 1 year = 365 days/yr * 24 hrs/day = 8760 hrs/year | | | |

**Table 1: Availability over 1 year**

## 4.2 Channel Latency (end-to-end delay)

The teleprotection latency of a protection system is the time taken for a local protection message to be transmitted over a teleprotection system to a remote end protection function, shown as the interface (a) to (a) in Figure 1 below. Note: A scheme can utilize common protection and teleprotection functions contained within the same equipment, for example, a protection equipment having a 4-wire VF voice frequency, an optical interface per IEEE Std. C37.94 [4] or an Ethernet communication port.

The channel latency, for the purposes of this report, is defined as the transport time from the physical point where the teleprotection signal interfaces with the communications network to the physical point where the signal exits the communications network shown as the interface points (b) in Figure 1 below.

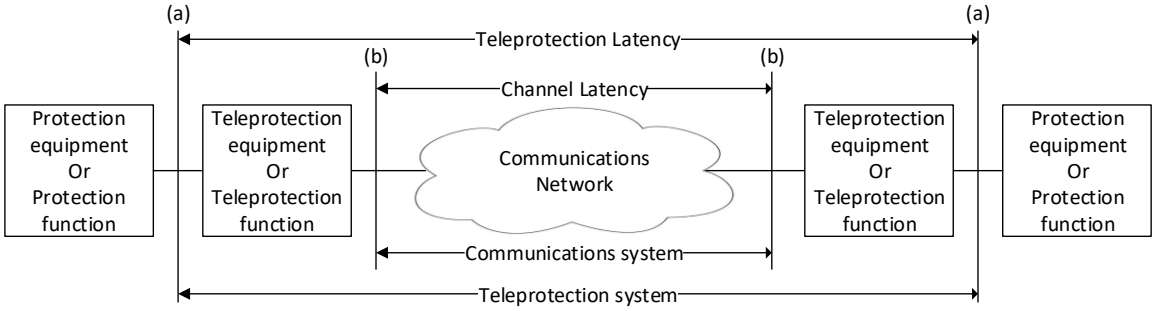


**Figure 1: Teleprotection / communications system latency**

Teleprotection latency is a factor in determining fault-clearing times. A channel's worst-case latency value can have an effect on the power-handling ability of a transmission line (and collaterally the power system's stability). For this reason, the migration of an

existing transmission line's protection scheme and affiliated teleprotection communication channel from a deterministic Time Division Multiplexing (TDM) channel to an Ethernet WAN channel, degradation of channel latency is discouraged.

For green-field transmission line designs the worst-case channel latency value is needed to determine the fault-clearing time. Faster tripping means less damage, better power quality, better stability, and faster service restoration.

There are varying teleprotection latency requirements specified for example by IEC 61850-5 [4]. As technology has evolved the de-facto teleprotection latency has continued to improve, resulting in a continuous expectation of lower channel latencies (as well as faster protection algorithms).

Historically, before the transition from Frequency Division Multiplexing (FDM) to TDM multiplexers, Voice Frequency (VF) channels were used with a latency around 2 milliseconds (ms) and the teleprotection equipment used frequency-shift audio tones. The signal processing required to keep the false-trip probabilities below $10^{-6}$ IEC 60834-1, Figure 21 [1] resulted in a teleprotection latency around 12 ms. In comparison the current TDM multiplexers (e.g. SONET) provide an IEEE C37.94 digital interface [3] with a sub-millisecond channel latency, dropping the (currently typical) teleprotection latency to around 2 ms.

## 4.3 Delay Asymmetry

Asymmetry, sometimes referred to as channel asymmetry or asynchronous channel delay, is the absolute value of the difference in latency for each direction of a communications circuit.

$$Asymmetry = | \text{Latency}_{A>B} - \text{Latency}_{B>A} |$$

For example, assume the latency from point A to point B is 3 ms and the latency from point B to point A is 4 ms. The asymmetry of this circuit is: |3 ms – 4 ms | = 1 ms.

Current differential schemes that synchronize over the communication link can be affected by channel asymmetry since the local and remote measurements must be time-aligned to be correctly evaluated.

As local and remote clocks are adjusted using one-way delay calculated based on delay symmetry assumption, a time error occurs when delay asymmetry is present. For the above example, one-way delay calculated as (3ms + 4ms) / 2 = 3.5ms has a time error of 0.5ms that corresponds to a phase angle error of 10.8 degrees for 60Hz system, and an associated magnitude error.

Legacy differential relays are particularly vulnerable to asymmetrical channel delay, adversely affecting the protection system. Modern microprocessor-based relays can offer improved reliability by using external time synchronization. Consult the manufacturer's

data sheet for allowable asymmetry and fallback mechanisms for loss of time synchronization source.

For large complex communications networks, especially in regard to backup and/or alternate path configurations, calculation of possible channel asymmetry for all paths is performed.

Normal and backup paths are likely to have different latencies. Therefore, asymmetry-sensitive circuits are likely to include the requirement that any unidirectional path failure forces both directions to use the backup path. This is called switch on Remote Defect Indication (RDI).

## 4.4 Channel Quality

Digital channel quality is defined in terms of bit error rate (BER) performance. IEC 60834-1 [2] specifies bit error rates per voltage level for normal operation, during a disturbance and when protection is blocked. Additional guidance on expected BER levels is provided in IEEE PSRC Report on Digital Communications for Relay protection [8].

## 4.5 Performance Monitoring

Constant monitoring may be necessary to verify critical performance requirements are being met appropriately as defined for each protection communications circuit. It is not enough to verify that the communications circuit meets requirements at commissioning, and then trust that all will remain well. Some relays can monitor and alarm for several parameters: loss of communication, excess bit error rate, channel asymmetry, or other circuit parameters. There are also techniques and methods for measuring these types of parameters in the communication equipment itself, depending on the type and manufacturer. In all cases, there tends to be an agreement about which equipment will monitor which parameters (protection relay or communications device). Performance monitoring is typically implemented for any parameter which is specified as a performance requirement (except those mutually agreed upon by the protection and communication engineers). In many cases the best approach may be to split the performance monitoring between devices, such as a relay monitoring communication failure, and a communications device monitoring channel asymmetry, as an example.

## 4.6 Performance Recommendations

For a discussion on system level and local area network (LAN) requirements in electrical power substation a reader can refer to clause 7 in IEEE Std 1615 [5].

The channel latency requirements for teleprotection systems tend to vary based on the type of protection scheme and the voltage level of the protected line. Faults on critical transmission lines have far-reaching impacts on the power system, thus it is desirable that such faults be cleared much faster than faults on sub-transmission systems. Therefore, the channel latency and asymmetry times required for each system could be different. Table-

1 provides an example matrix of key channel performance for various protection schemes. The parameters for each scheme are subdivided into three categories, Critical (system stability concerns), High voltage, and Sub-transmission and below. This table is intended as a guide to aid in the selection of channel performance criteria for a communications network.

Channel performance typically includes validation of acceptability for the existing protection scheme.

Availability and channel quality requirements typically vary for these categories. These can be defined per guidance provided in IEC 60834 [2] or local regulatory documents, such as WECC guidelines [11].

| | Current differential protection* | | | Pilot protection | | |
|---|---|---|---|---|---|---|
| | Latency (ms)** | Asymmetry (ms)** | Failover (ms)*** | Latency (ms)** | Asymmetry (ms)** | Failover (ms)*** |
| Critical | 5 | 0.5 | 5 | 5 | 5 | 5 |
| High voltage | 10 | 1 | 10 | 10 | 10 | 10 |
| Sub-transmission | 15 | 1 | 50 | 15 | 10 | 50 |

**Table 2: Example matrix of key channel performance**

* Synchronization over the communications link:
Per explanations provided in clause 4.3, a 0.5 ms of asymmetry results in a 5.4 $^{o}$ phase angle error, and an associated magnitude error for a line current differential scheme. To avoid degrading a scheme's performance by more than 1$^{o}$, the additional asymmetry needs to be kept below 0.2 ms.

** The numbers represent the largest delay allowed:
Line current differential systems using GPS time signals to compensate for message delay variations only require the total circuit latency to be within the specified application requirements.

*** The relays may have the ability of using dual channels, and to seamlessly switch to the alternative channel when the primary channel fails. In these application, longer network failover times may be acceptable.

# 5. Ethernet communications channel performance considerations for teleprotection

## 5.1 Ethernet Network Architecture

For details of Ethernet technology, communication architecture and devices' operation a reader can refer to clause 6.7 of IEEE C37.236-2013 [7], clause 4 of IEEE PSRC/PSCC report [9], and IEC TR 61850-90-4 [10].

A layer 2 Ethernet network regardless of physical topology (bus, ring, mesh, star) [5] is logically a tree. Each leaf being an edge Ethernet port (user access port), each branch

segment being a communication link (copper or fiber Ethernet cable), and each branch-segments' junction being an Ethernet switch or bridge, the correct IEEE 802 terminology. Switch implies hardware forwarding of data.

Just as there is one, and only one path between two leaves, there is one, and only one path between two Ethernet edge ports. One function of a switch is to keep traffic flowing only on these (needed) paths whenever possible.

Another function of a switch is to manage the merging of incoming or ingress paths into outgoing or egress paths. Since these paths have generally the same bit rate and the timing of their traffics' Ethernet frames are not coordinated, this merging function necessitates the ability to buffer (or queue due to congestion) these frames to avoid them being discarded.

For teleprotection circuits traversing networks with other non-critical data, traffic engineering plans to prevent priority queuing issues are to be documented and implemented

## 5.2 Ethernet Switch Queues

Operation of Ethernet switches is described in detail in clause 7 of IEEE PSRC/PSCC Report [9].

To reduce the latency of critical traffic, switches generally provide two to eight queues for each egress port so high-priority Ethernet frames can egress ahead of lower-priority frames.

The algorithm used by the frame classifier determines which priority egress queue gets used for each frame from the ingress port shown in Figure 2.

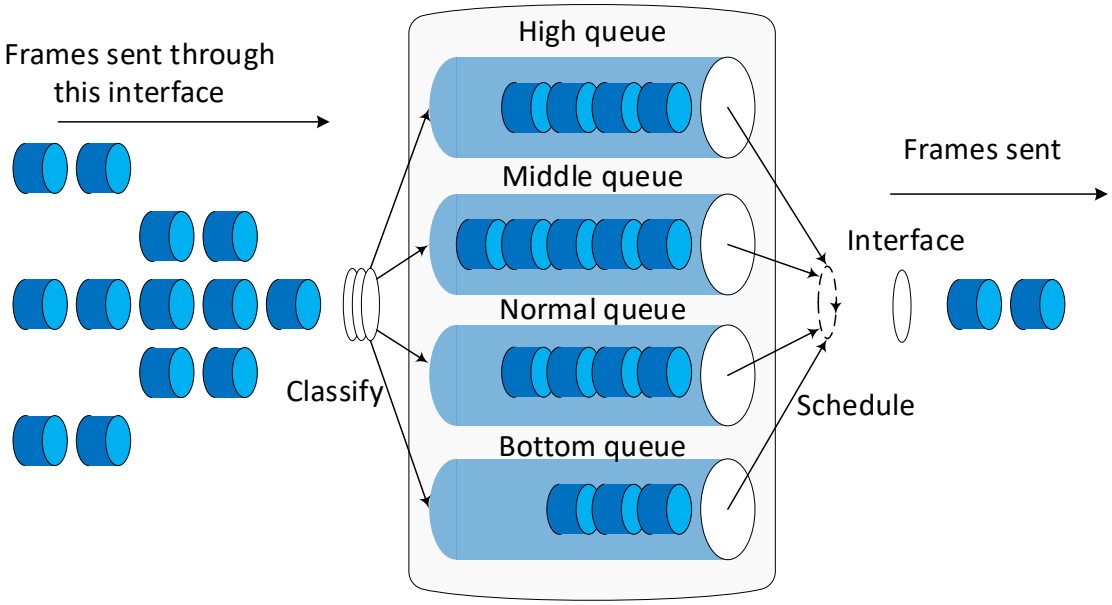

**Figure 2: Ethernet switch queue**

It is very important that the WAN engineer understands what other type of traffic is traversing the Ethernet connections, their potential effect on teleprotection traffic and mitigation techniques required to achieve the desired performance. Traffic queue priorities are used to control and limit non-deterministic traffic which is assigned to lower-priority queues.

## 5.3 Queue Priorities

Two methods of priority queuing are considered here, though not complete. These are strict priority and weighted round robin. Not all devices support both; therefore, it is important to understand which of these are available.

**Strict Priority** will always service the highest priority frames first and will not move down into the lower priority frames until there are no higher priority frames in the queue. IEEE 802.1Q, clause 8.6.8 mandates support for strict priority by all bridges. This is preferred for protection applications.

**Weighted Round Robin** services all priority queues but applies rate limits. For example, a common rate limit is 8:4:2:1 which divides eight priority settings down to four. For an 8:4:2:1 rate, frames with the two highest priority queue settings are allowed to send 8 frames each and then the next two highest priority frames are each then allowed to send 4 frames and so on. This prevents the higher priority traffic from starving access to lower priority traffic.

Queuing latency examples:

1. At each egress switch port, a high-priority frame may have to wait for a maximum-length lower-priority frame to complete its egress:
    a. 1518-byte (standard maximum) frame takes 122 (microseconds) μs at 100 Mbps, 12 μs at 1 Gbps and 1.2 μs at 10 Gbps.
    b. 9000-byte (“jumbo”) frame takes 720 μs at 100 Mbps, 72 μs at 1 Gbps and 7.2 μs at 10 Gbps.

    A potential 2 ms (12 ms for jumbo-frame networks) extra delay could therefore be incurred for a network path comprising 16 hops at 100 Mbps or 160 hops at 1 Gbps in the worst-case scenario.

2. At each egress switch port, a high-priority frame may also have to wait for many other high-priority frames to egress:

    600-byte frame (typical for GOOSE) requires 48 μs at 100 Mbps, 4.8 μs at 1 Gbps and 0.48 μs at 10 Gbps.

    A potential 2 ms extra delay could therefore be incurred for an event-triggered burst of 40 GOOSE frames at 100 Mbps or 400 frames at 1 Gbps.

For a given network the number of switches (hops) in each path and the support of jumbo frames are both known allowing the first example's latencies to be determinable. An objective in this example is to avoid having to compete with jumbo frames but for some networks this may be unavoidable.

For the second example, determining the worst-case wait times requires a detailed knowledge of the parameters (frame lengths and time-distributions) of both the teleprotection traffic and any other traffic with the same or higher priority assignments.

Traffic queue priority planning is likely to be extremely challenging. The highest-priority queues are preferred for teleprotection traffic. When sharing high-priority queues with other (non-protection) traffic, network engineering helps meet the specified performance under all traffic conditions.

## 5.4 Jitter or Delay Variation

In the context of Ethernet networks, jitter is the variation in latency as measured in the variability over time of the frame latency in one direction across a network. A network with constant latency has no delay variation (or Jitter).

The term jitter can cause confusion as it is defined in particular ways by different entities. For example, frame jitter is expressed as an average of the deviation from the network mean latency.

The standards-based term for this variation, per RFC 3393 [6], is packet delay variation (PDV). PDV is an important quality of service factor in assessment of TDM circuit emulation services e.g. TDM based teleprotection and line current differential circuit performance.

Jitter, delay variation or PDV, is measured in one direction. Line current differential protection requires a bi-directional circuit. Jitter, delay variation or PDV, in each direction are asynchronous to each other and can contribute to channel asymmetry. Most communications systems use a PDV setting to eliminate these asymmetries by adding a configurable time delay to the data at the ingress port. This delay causes the system to buffer received frames, eliminating the received jitter. Choosing this option requires the need for the delay to be set greater than the expected PDV, thus mitigating jitter by using additional latency. Jitter buffer increases effective packet delay. PDV settings are specific to TDM circuits carried over pseudo wire or other TDM to Ethernet frame conversion.

## 5.5 Network Engineering

Network engineering is responsible for checking that an Ethernet network is suitable for teleprotection applications for all paths (both primary and backup). For example paths' switch priority-queue assignments can be set to provide:

1. The worst-case latency of each teleprotection path is specified.

2. Worst-case latencies are within the acceptable ranges of the teleprotection applications for all primary and alternate paths.

The network planning process for all future changes to the network's hardware and to traffic with the same or higher priorities needs to evaluate the effect on the two requirements documented above. Ideally there will be no change to existing performance, if performance is impacted new performance parameters need to be agreed to.

More discussion on real-time protection over Ethernet can be found in subclause 5.2 and throughout IEEE 1615 [5] and clause 11 of IEEE PSRC/PSCC Report [9].

## 5.6 Path Planning Considerations

With solutions using two (or more) possible paths each path may respond differently to disparate failures. As an example, if the Primary path has an unacceptable performance and the redundant path provides a slightly better but still unacceptable performance, then the next contingency may yield more acceptable results.

A viable plan incorporates consideration of the monitoring and response capabilities of the protective relay utilizing the communications circuit in question. These capabilities may include but are not limited to:

- Relays recognizing a complete loss of communication with each other.
- Relays recognizing end-to-end latency has exceeded acceptable limits.
- Relays recognizing unacceptable quality of data.

## 5.7 Network Failover

Networks designed for teleprotection applications are designed to mitigate fiber failures by switching the circuits' paths within a specified time frame to restore failed circuits, see Table 1. Ethernet WAN networks used for teleprotection applications require similar performance.

A typical simple Ethernet network with a single connection is shown in Figure 3:

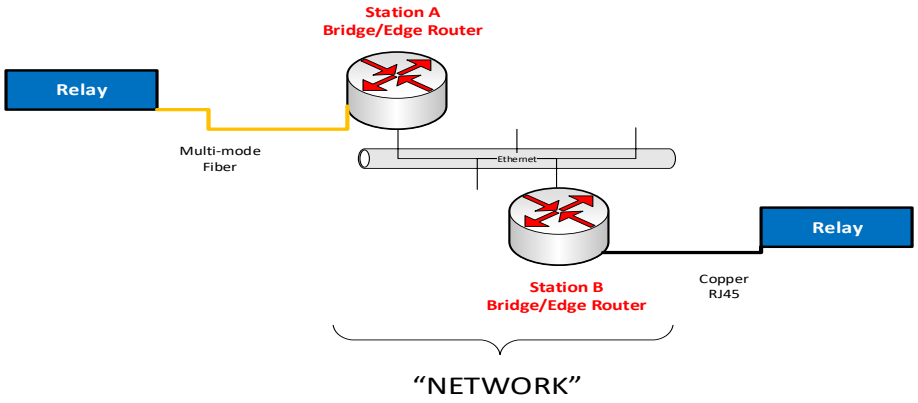


**Figure 3 Simple Network**

In a more complex connection design, as shown in Figure 4: (still only using a simple Ethernet network) there are multiple considerations. The relays can have redundant connections to the bridge/edge router. The bridge/edge router for redundancy can have multiple paths through the Ethernet network. The Ethernet network may have multiple paths pre-programmed. The complex connection design has several recoverable cable-failure scenarios:

- Within the substation directly associated with the relays.
- Within the substation indirectly associated with the relays.
- Outside of the substation.

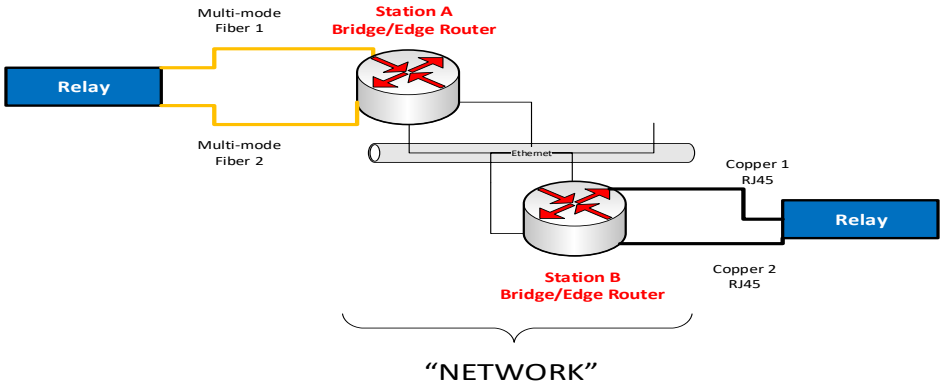


**Figure 4 Complex Network with Multiple Redundancies**

The intended result of the complex network is that the real time data communication from the relay at Station A to the relay at Station B restores within the specified fail-over / restoration time. In order to achieve this, the Ethernet network, the bridge/edge routers, and the relays each need to be able to respond to a port/cable/component failure. Possible network failures could be conditions for a network failover implementation.

## 6. Conclusion

This report assists protection engineers and communications engineers who are working on implementing protection channels over Ethernet networks by outlining specific performance requirements the protection engineer needs to communicate to the network engineer. The report emphasizes the need for network engineering to achieve the required and agreed to performance requirements. The report provides a sample protection communications requirements agreement form that is intended as a method to document the agreed performance.

## 7. REFERENCES


[1] Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria *(A Module of TSGR, FR-440; FR-SONET-17; and FD-29).* Telcordia Technologies Generic Requirements GR-253-CORE, Issue 4, December 2005.

[2] IEC 60834-1 Ed.2.0:1999, Teleprotection Equipment Of Power Systems – Performance And Testing – Part 1: Command Systems.

[3] IEEE C37.94-2017 – IEEE Standard for N times 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment

[4] IEC 61850-5 Ed. 2.0 b:2013 Communications networks and systems for power utility automation – Part 5 Communication requirements for function and device models.

[5] IEEE Std 1615-2019 IEEE Recommended Practice for Network Communication in Electric Power Substrations

[6] RFC 3393 – Proposed Standard – IP Packet Delay Variation Metric for IP Performance Metrics (November 2002) The Internet Society

[7] IEEE Std. C37.236-2013 IEEE Guide for Power System Protective Relay Applications over Digital Communication Channels.

[8] IEEE PSRC Report by WG H9 Digital Communications for Relay protection

[9] IEEE PSRC/PSCC Report by WG H12/P6 “Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations”, 2017

[10] IEC TR 61850-90-4:2013 Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines

[11] WECC Guideline “Communication Systems Performance Guide for Electric Protection Systems”, July 25, 2013

# Appendix A - Sample Protection Communication Requirements Agreement Form

This appendix is provided for the protection and communications engineer to document the expected performance requirements for TDM based current-differential and pilot protection applications (Teleprotection) applied over an Ethernet network.

The table below allows the specifications to be applied to each of the circuits used to carry teleprotection communications between protective relays. The channel availability per IEC 60834-1 Figure 21 is 99.99%, [2] and can be less for lower voltages. Channel quality varies per voltage level as well and can be defined by IEC 60834-1 [2], or guidance provided by local regulatory agencies, such as WECC Guidelines [10].

| *Circuit ID* | Interface (type and bandwidth) | Committed Information rate (mbps) | Worst-Case Channel Latency (milliseconds) | | Worst-Case Jitter (aka PDV) (milliseconds) | | Worst-Case Channel Asymmetry (milliseconds) | | Worst-Case Failover (e.g. upon fiber failure) (milliseconds) | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | *Required* | *Offered* | *Required* | *Offered* | *Required* | *Offered* | *Required* | *Offered* |
| *<circuit 1>* | | | | | | | | | | |
| *<circuit 2>* | | | | | | | | | | |
| *<circuit 3>* | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Table 3 Teleprotection Circuits Performance Specifications

The “Required” columns are completed by the protection engineer. “Offered” columns are completed by the network engineer (what can be achieved). Additional considerations such as any IEEE 802.1Q priority and/or VLAN ID, etc. need to be agreed upon and documented.

The following notes apply to Table 3:

1. Channel latency is defined as the WAN system transport time from the point that the teleprotection signal interfaces with the WAN to the point where the signal exits the interface at the drop location. The worst-case figure includes whatever PDV is encountered through the network.
2. Worst-Case is for 99.99% of the time over any hour.
3. Committed Information Rate (CIR): the guaranteed data rate for the Ethernet data path through the network.
4. The requirements apply to both the normal (primary) channel, and the backup (redundant) channel (or channels).