Ethernet-Based Line Differential Protection Over Passive Multiplexers

Ron Nathan and Chido Chandakabata
Schweitzer Engineering Laboratories, Inc.

Ray Barnes
Metro Trains

Presented at the
South East Asia Protection, Automation and Control Conference
Melbourne, Australia
March 14–15, 2017

SEAPAC 17 - APB5 – Melbourne March 14th-15th

Ethernet-Based Line Differential Protection Over Passive Multiplexers

Name	Company Name	Email Address
Ron Nathan	Schweitzer Engineering Laboratories, Inc.	ron_nathan@selinc.com
Chido Chandakabata	Schweitzer Engineering Laboratories, Inc.	chido_chandakabata@selinc.com
Ray Barnes	Metro Trains	ray.barnes@metrotrains.com.au

Keywords: Line Differential, CWDM, VLAN, RSTP, Time Synchronisation

Contents

1 Abstract

Line differential protection applications are common and are often based on deterministic serial communications. These communications are typically connected utilising pilot wire, dark fibre, or multiplexers. Applying line differential protection using Ethernet provides benefits, but also challenges such as handling the nondeterministic nature of a packet-switched network.

This paper describes a solution designed for a rail company that required new three-terminal line differential protection as part of a refurbishment project. The rail company had limited available leased fibre cores between the substations, and these cores were already being used in conjunction with existing passive coarse wave division multiplexers (CWDMs) to run multiple services. The chosen design was to implement line differential protection (87L) over Ethernet using managed switches equipped with CWDM small form-factor pluggable (SFP) transceivers.

The paper explains each of the different technologies used for this project, including line differential protection over Ethernet, CWDMs, and managed switch configuration. It also provides details on the performance of the system in terms of speed and stability.

2 Problem Statement

A rail company in Victoria, Australia was refurbishing and building new substations and required line differential protection for three-terminal connections and possibly four-terminal connections in the future. They had existing infrastructure that used Ethernet and passive multiplexers. The rail company did not own the fibres between these substations and instead leased the cores from a third-party provider at a high cost. As such, the rail company wished to maximise the use of the existing leased cores and infrastructure.

Most modern differential protective relays have built-in copper or fibre serial line current differential channels with typical multimode and single-mode frequencies in the range of 850 nm, 1,300 nm, or 1,550 nm. Most protective relays do not support CWDM frequencies and are therefore incompatible with the rail company's CWDM infrastructure. To use the existing CWDM equipment, a media converter was required between the non-CWDM protective relays and the CWDM multiplexers. The proposed solution was to use an Ethernet switch with CWDM SFP fibre-optic transceivers. A protective relay that was chosen could support line differential protection over Ethernet.

3 Line Differential Technologies

The principal of line current differential protection is simple: the vector sum of current entering and leaving a transmission line should be practically zero. One benefits of line differential protection is that it is selective and therefore only responds to faults within the protected zone. As such, time grading with other protection systems is not required, which makes this type of solution suitable for fast main/primary protection of transmission lines.

For relays to calculate the difference between the terminal currents, each relay must be aware of its local current as well as the currents at the remote terminals. The readings of the local and remote current must be aligned to each other in time. A complete power cycle at 50 Hz occurs in 20 ms, which equates to 360 degrees. Therefore, a 1 ms misalignment in readings results in an 18 degree angle error. When designing numerical protection using communications schemes, the timing source and accuracy become critical, as discussed later in the paper. The subsections below describe different line differential technologies and their suitability to the rail company's application.

3.1 Pilot Wire

Pilot wire schemes measure differential current electrically. A common scheme is one in which protective relays use the output of current transformers (CTs) to represent the three-phase currents in the form of a single-phase voltage. The voltage produced by each relay is proportional to the current flowing in the transmission line being protected. Under normal conditions, each end of the line should have the same magnitude and phase and negligible ac current will be flowing around the pilot wire. When a fault occurs, ac current flows because of the unbalance and the line trips.[1]

This technology was not suitable for this project because no pilot wires existed between the substations that required the protection scheme.

3.2 Serial Protocols (G.703 and IEEE C37.94)

Line differential applications require little data to be shared between the line protection devices. At a minimum, current magnitude and angle are required along with some guarantee that the measurements are time-aligned. Typically, 64 kbps of data bandwidth is sufficient for serial line differential applications.

Serial applications are point-to-point. Because the channel is dedicated for the line differential application, the data transmission times are relatively constant with low jitter. For this reason, serial applications are often able to operate with either external or internal time sources. External time requires both protective relays to be synchronised to a common source, such as high-accuracy IRIG-B (often defined according to the IEEE C37.118 synchrophasor measurement standard) or Precision Time Protocol (PTP) as defined by IEEE 1588. An internal timing source uses a ping-pong method to determine the round-trip channel delay, which works well when the channel delays are symmetrical (i.e., transmit path = receive path).

When the receive path differs from the transmit path, the channel can become asymmetrical, meaning that the time it takes for packets to travel to the remote relay are different from the time it takes for them to arrive from the remote relay. When this occurs, each relay is required to archive its local values and then wait for the remote values and for the process of data alignment to occur. Protective relays generally have a maximum allowable channel asymmetry (e.g., 4 ms). If substantial channel asymmetry exists, using IRIG-B or PTP within each protective relay is recommended rather than relying on channel-based synchronisation.

G.703 is an International Telecommunication Union (ITU) standard for voice and data communication that is commonly used with multiplexers and is set up to often use 64 kbps of data bandwidth (E0 carrier link designation).[2] G.703 uses metallic cabling, which is susceptible to electromagnetic interference. For this reason, many utilities are adopting the IEEE C37.94 standard for teleprotection and multiplexer equipment. IEEE C37.94 specifies optical fibre interfaces that are immune to electromagnetic interference and ground potential rise.

Because the chosen protective relays for this project did not support the CWDM frequencies, to implement G.703 or IEEE C37.94 the relays needed to be connected to active multiplexers using, for example, synchronous optical network (SONET) or Synchronous Digital Hierarchy (SDH) protocols. The multiplexers needed to be fitted with CWDM SFP transceivers to operate on the rail company's existing leased fibre line. This type of solution was tested, but it was rejected because it was both complicated and costly to use both active and passive multiplexers.

3.3 Ethernet-Based Line Differential Protection

Ethernet-based line differential protection uses the same numerical protection principles within the relay as serial protocols do. However, the Ethernet network protocol is used to transmit the data packets between the relays. This solution presents several advantages as well as challenges. The nondeterministic nature of Ethernet communication can affect the dependability (on-time delivery of traffic), causing current differential protection to be unavailable.

To ensure that the Ethernet-based line differential is dependable and secure, sound Ethernet design principles must be applied. The following guidelines are recommended:

- Dedicated Ethernet packets should be transported over multiplexer channels.
- A dedicated Ethernet network should be engineered to provide appropriate bandwidth, traffic congestion control, and acceptable latency.

An understanding of the nature of the Ethernet packets is needed to correctly provision for and design the network. In the protective relay chosen for this project, the line differential protection packets are sent as Layer 2 multicast packets, similar to IEC 61850 GOOSE packets. Some network design considerations are bandwidth, latency, and jitter. The protective relay uses a packet with a fixed size of 696 bits that is sent every 4 ms. The relay can tolerate a 0.1 ms deviation from the expected time interval between packets. The bandwidth can be calculated as shown in the following formula.

$$\text{Bandwidth} = \frac{696 \text{ bits}}{0.0001 \text{ s}} = 6.96 \text{ Mbps}$$

Based on this formula, four terminals each with an Ethernet-based line differential relay require 6.96 • 4 = 27.84 Mbps. Therefore, for this project a minimum bandwidth of 100 Mbps was specified in order to ensure a safety margin.

Latency, or channel delay, is defined as the one-way measurement from the time a packet is sent by the remote relay until the time it is received by the local relay. The protective relay can tolerate a constant delay of up to 50 ms. However, every millisecond of latency in receiving the packet results in a millisecond delay in tripping. Therefore, it is desirable to ensure low latency for fast tripping. The reason the line differential scheme can operate with constant delays is that the packets containing current magnitude and angle are time-stamped and the relays align the local and remote readings before making the calculation.

Because of the nondeterministic nature of Ethernet networks, packets can arrive earlier or later than expected due to slight variations in the channel delay time. The protective relay must be able to accommodate this jitter. The protective relay chosen for this project can operate with a maximum jitter of 3.5 ms. Jitter can be caused by changed network traffic resulting from an increase in the quantity or size of Ethernet packets or buffering.

To reduce the likelihood of excessive jitter, sufficient bandwidth must be provisioned.
While virtual local-area networks (VLANs) assist in data segregation, they do not play a factor in bandwidth utilisation. As an example, assume a 100 Mbps Ethernet link was used for both SCADA and line differential protection, each had its own dedicated VLAN, and both would be sharing the bandwidth. If the traffic in the SCADA system was excessive, it would leave little bandwidth for the line differential protection VLAN, which could then cause jitter while the switch processed the SCADA packets. Port rate limiting in the switch can be implemented on all SCADA interfaces; however, the authors recommend a different network design with private bandwidth provisioned via a separate Ethernet network or a separate private bandwidth multiplexer channel.

Because of the nondeterministic nature of Ethernet, the channel latency cannot be worked out reliably using the ping-pong method. For this reason, an external high-accuracy time source or PTP is mandatory. If an external time source is not available, the two protective relays will begin to drift apart in time and the differential channel will become disabled because the protective relays cannot default back to channel-based timing. For this reason, a clock source with a long holdover is recommended to minimise drift if the timing source, such as GPS, is lost. Typically, temperature-compensated crystal oscillators can provide an accuracy of 0.1 parts per billion (PPB) or better. The accuracy for a 24-hour period can be calculated as shown in the following formula.

$$t_{\mu s} = \text{PPB} \bullet 24\ \text{Hours} = \frac{0.1}{1 \bullet 10^{9}} \bullet 24\ \text{Hours} \bullet 3600\,\text{s} \bullet 1 \bullet 10^{6} = 8.64_{\mu s}$$

4 Multiplexer Technologies

Multiplexing is a method by which multiple analogue or digital signals are combined into a shared medium to maximise the use of the medium and reduce costs. There are several different multiplexer technologies, but this paper will limit discussion to briefly describing two such technologies.

4.1 TDM Multiplexer

Time-division multiplexing (TDM) is a technology in which time is used to segregate different data streams. A common analogy is a train which has several carts and each cart is dedicated to carrying specific cargo. The train arrives at each station on time and the cargo is loaded into the corresponding cart, as illustrated in Figure 1. Each cart represents a multiplexer time slot. Multiplexers use drop-modules to interface Ethernet, serial, voice, and other applications. Once the data packets have been read by the drop-module and loaded onto the "train cart," the packets are sent to the next stations and "get off" at predetermined stops. Thus, multiple packets for different services are sent by a common carrier and these services are logically separated in time. Common backplane protocols for TDM multiplexers are SONET and SDH.

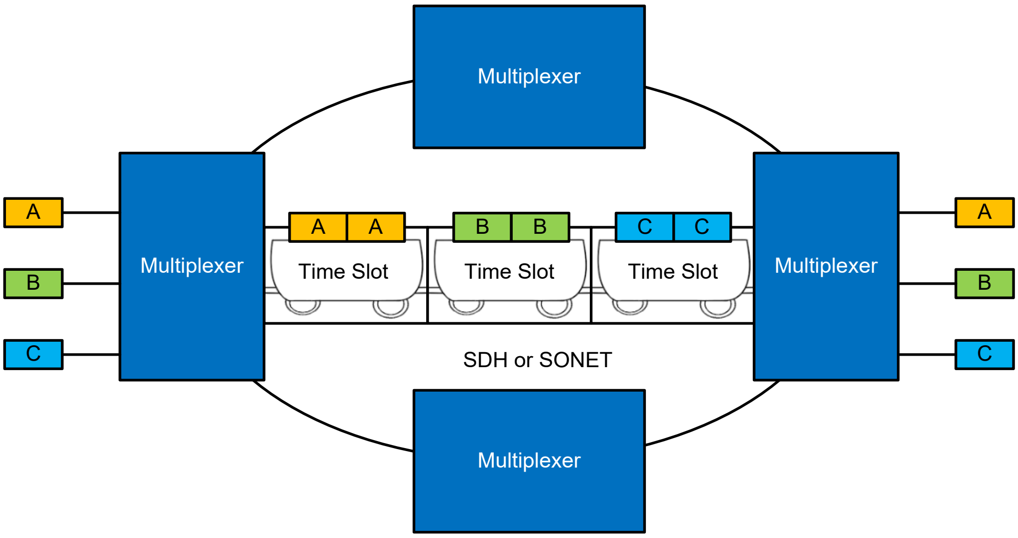

Figure 1 Time-Division Multiplexing

4.2 Coarse Wavelength Division Multiplexing

Wavelength division multiplexing (WDM) uses light-wavelength principles to combine multiple signals onto a fibre-optic cable. WDM is a popular technology because it allows for expanding the capacity of a network without laying new fibres. There are a few common wavelength patterns, namely coarse WDM and dense WDM, with dense WDM having denser channel spacing. Coarse WDM frequencies are defined from 1,270 nm to 1,610 nm with a channel spacing of 20 nm, thus providing 18 channels. Many coarse WDM multiplexers are designed from 1,470 nm to 1,610 nm, avoiding frequencies below 1,470 nm because of their higher attenuation.

Passive CWDMs do not require any external power; wavelengths are separated using passive optical components such as bandpass filters or prisms. For devices to work with CWDMs, they must be able to transmit the CWDM wavelength. Many devices use SFP ports. A CWDM SFP pair must be chosen to multiplex and demultiplex the wavelength, as shown in Figure 2 below. Note that the colours in the figure are for illustrative purposes only; CWDM frequencies are beyond the visible spectrum.

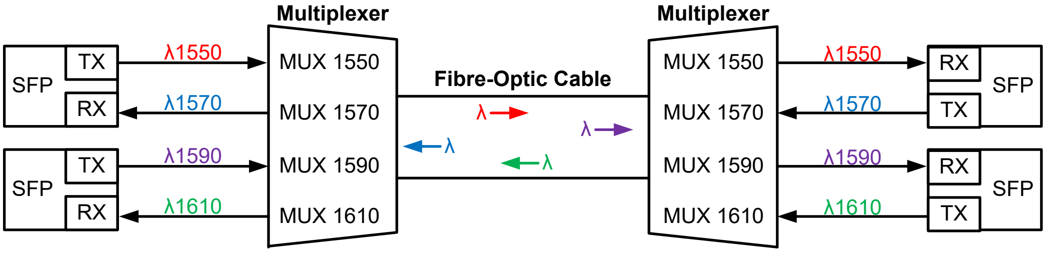

Figure 2 Representation of a CWDM

5 Solution: Ethernet-Based Line Differential Protection Over CWDMs

5.1 Solution

The solution chosen for this project was to implement Ethernet-based line differential protection over the CWDMs. A dedicated Ethernet switch was used for the line differential protection traffic and an additional switch was used for SCADA, engineering, and IEC 61850 traffic.

The Ethernet switch was equipped with single-mode CWDM SFP ports and was connected to the multiplexer. To test the jitter and latency, and to check for dropped packets, a proof of concept was created, as shown in Figure 3.

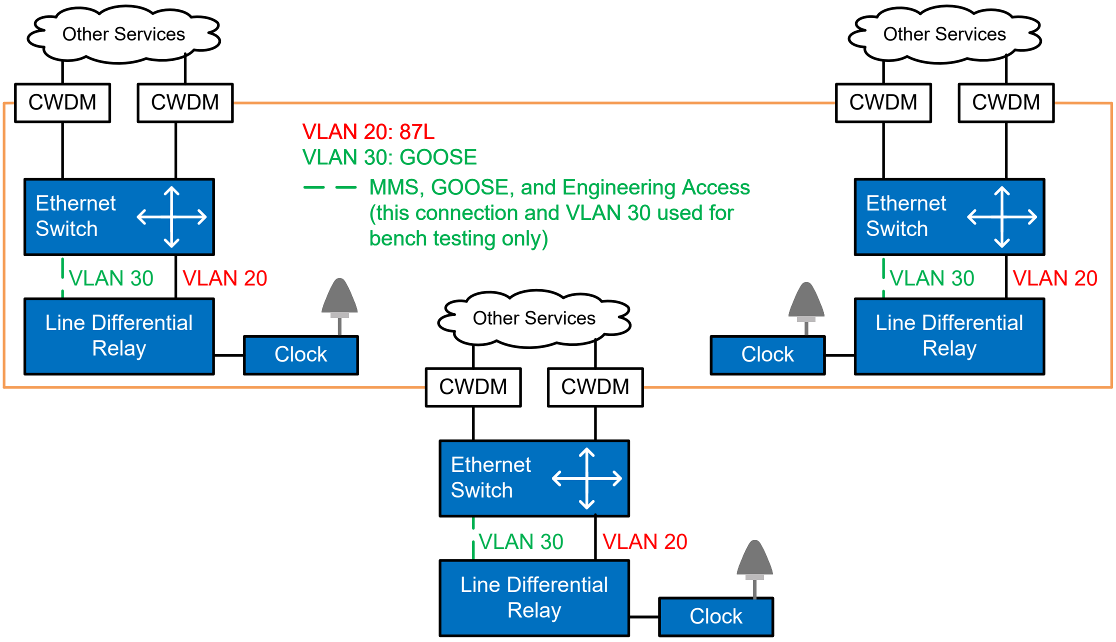

Figure 3 Ethernet-Based Line Differential Protection Over CWDMs

Though the final design has a dedicated switch for SCADA and engineering access, the bench testing was performed with all traffic being sent through a single switch for each substation. In addition, frequently changing GOOSE packets were sent continuously between the switches. The additional GOOSE messages were sent every 4 ms to determine whether this additional traffic affected the system.

VLANs and priority tagging were implemented in the relays and the switches to ensure that the line differential protection and GOOSE Ethernet traffic had a higher priority than other traffic. This also ensured that traffic such as line differential protection and GOOSE messages were logically separated and only sent to the intended Ethernet ports. Doing this ensures that the protective relays will not need to process and reject unrelated Ethernet packets, which can adversely affect their performance. The switches were also configured for Rapid Spanning-Tree Protocol (RSTP) failover to provide network fault detection, isolation, and path reconfiguration for packet delivery via a new path. While not implemented, additional redundancy could have been achieved by introducing another network switch for each site and using two failover ports between the relay and both switches.

5.2 Testing Results

The performance of the line differential protection over CWDMs was confirmed by running the system for 48 hours and monitoring the diagnostics within the protective relay. A feature of the protective relay is that it allows user-programmable bits to be sent over the line differential protection channel. For one test, a bit was sent continuously backward and forward (ping-pong) between two relays and the average round-trip time for the bit was measured using the diagnostic tools within the protective relay.

The results of the 48-hour test, as read from the relay diagnostic tool and event recorder are listed below:

- The maximum latency for the line differential protection packets was less than 0.2 ms (well within tolerance).
- The number of dropped packets was zero.
- The average round-trip time for the bit was less than 7.5 ms.

In addition, Ethernet links and fibre-optic links were connected and disconnected several times to simulate network failures. The average RSTP recovery and convergence times were less than 20 ms.

The recovery time was tested using two methods. One method using an external Internet Control Message Protocol (ICMP) ping tool running on a laptop, and the second method read the number of dropped line differential protection packets during a network failure using a diagnostic tool built into the relay. Because it is known that packets are sent every 4 ms, a loss of five packets equates to a 20 ms network recovery.

At the time of this writing, a pilot trial of two relays was installed at the rail company’s substations to confirm the communications and network robustness. Because all of the equipment used in the solution was bench tested, the only variant for the actual application was the distance between the substations.

Assuming the speed that data signals propagate through the single-mode fibre-optic cable is equal to two-thirds the speed of light, the following formula shows that a 10 km cable introduces 50 μs of latency, which is negligible for this project.

$$\text{Time} = \frac{\text{Distance (m)}}{\text{Speed (m/s)}} = \frac{10 \bullet 10^3}{\frac{2}{3}\left(3 \bullet 10^8\right)} = 50\ \mu\text{s}$$

6 Conclusion

This paper discusses some relevant technologies for implementing line differential schemes and presents a viable solution for companies wishing to use existing CWDM infrastructure. The testing results showed that the Ethernet-based line differential scheme over CWDMs is robust and flexible. Serial differential schemes are dependent on the location and physical arrangements of fibre-optic cables and require dedicated equipment that supports the serial differential protocols. These schemes are also affected by channel asymmetry and generally only provide a small bandwidth (64 kbps) for carrying any additional data.

Ethernet-based schemes are extremely flexible. They can operate in any well-designed network topology (such as star, ring, or mesh) and can work on any equipment that supports Ethernet. The testing showed that the Ethernet-based line differential solution can operate reliably over either TDM or coarse WDM multiplexers. Higher bandwidth is available on Ethernet-based line differential channels and therefore more available bits can be used for various signals, such as tripping or interlocking. In addition, the solution that was chosen can easily be implemented for up to four terminals, in line with the project requirements. While Ethernet-based schemes are very flexible, they do require careful design to ensure that a reliable time source is provided and to consider design mitigation against the nondeterministic nature of Ethernet.

References

1. N. Hook, “Commissioning of Translay Pilot Wire Protection Scheme, Version 2.1,” RailCorp, April 2013. Available: www.asa.transport.nsw.gov.au.
2. International Telegraph and Telephone Consultative Committee, G*eneral Aspects of Digital Transmission Systems, Terminal Equipments*. International Telecommunication Union, Geneva, Switzerland, 1989.

List of Figures

Biography: Ron Nathan

Ron Nathan is a SCADA and automation engineer based in Melbourne, Australia. He received his B.Sc. with honours in electrical engineering from the University of the Witwatersrand in South Africa in 2003. He started his career as a SCADA and programmable logic controller engineer at RAM-TEC Systems, designing automation solutions for companies such as Nestlé and South African Breweries. He then worked for CONCO in South Africa as a design engineer working on substation automation systems (SASs) for various utility and industrial companies. Ron continued his career at Consolidated Power Projects (CPP) Australia, where he designed SASs for renewable projects. He currently holds the position of Engineering Supervisor at Schweitzer Engineering Laboratories, Inc. where he manages a team that provides a range of services, including SASs, secondary system design and commissioning, specialised protection systems, and power management systems.

Biography: Chido Chandakabata

Chido Chandakabata is a power systems protection engineer based in Melbourne, Australia. He received his B.Sc. with honours in electrical engineering from the University of Zimbabwe in 2004. He started his career as a graduate engineer at Zimbabwe Electricity Supply Authority, later moving to the role of protection design engineer. He worked for CONCO in South Africa as a commissioning engineer before joining AREVA T&D (later Schneider Electric) as a systems engineer. He currently holds the position of Application Engineer – Protection Systems at Schweitzer Engineering Laboratories, Inc.. His current research interests are in advanced synchrophasor applications, arc-flash protection systems, and new technologies in transformer and line protection.

Biography: Ray Barnes

Ray Barnes has been employed in the rail industry for over 35 years, the last 9 with Metro Trains, working on SCADA systems and managing various SCADA systems. Ray began his career in the electrical / electronic field, and as technology changed moved into communications and operational control systems. He is currently employed as the Electrical Networks Controls and Indication Manager at Metro Trains in Melbourne, Australia where he manages the electrical network SCADA system and high-voltage testing.

20170228 • TP6802-01