Communications and Data Synchronization for Line Current Differential Schemes

Bogdan Kasztenny, Normann Fischer, Ken Fodero, and Adrian Zvarych
Schweitzer Engineering Laboratories, Inc.

Published in
Line Current Differential Protection: A Collection of Technical Papers Representing Modern Solutions, 2014

Previously presented at the
38th Annual Western Protective Relay Conference, October 2011

Originally published in the
proceedings of the 2nd Annual Protection, Automation and Control World Conference, June 2011

Communications and Data Synchronization for Line Current Differential Schemes

Bogdan Kasztenny, Normann Fischer, Ken Fodero, and Adrian Zvarych,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—This paper considers line current differential schemes from the point of view of data communications and current data alignment. The goal is to improve understanding among relay practitioners of some of the unique and key aspects of digital line current differential schemes: communications, data handling, and alignment. This paper also seeks to improve the appreciation of line current differential protection applications and related network requirements among utility communications engineers.**

I. Introduction

The line current differential protection principle becomes increasingly more attractive in today's power systems because of its good immunity to changing system conditions and ever-increasing penetration of nontraditional sources of fault currents, excellent sensitivity, good performance on multiterminal and series-compensated lines, and simplicity of application from the point of view of traditionally understood protection engineering. The expansion and reduced cost of utility communications networks further promote this superior protection principle.

However, line current differential protection requires a long-haul communications channel to exchange current data, as well as a synchronization mechanism to align the current values measured at geographically dispersed line terminals. These are relatively new application dimensions for a protection engineer, but are absolutely critical to both the security and dependability of line current differential protection schemes.

This paper focuses on data exchange and alignment issues for line current differential (87L) schemes to allow better understanding of the protection and communications domains as they intersect in this particular application.

First, the paper briefly reviews the channel requirements for 87L applications and compares direct point-to-point and multiplexed channels used in 87L schemes. This includes availability, latency, bit errors, symmetry, and simplicity of use, as related to 87L applications.

Second, the paper considers various transient conditions and impairments in the communications network and how they may impact the dependability and security of 87L schemes. In this context, a number of relay design details are reviewed that ensure security and maximize dependability under the presence of channel impairments.

Third, the paper elaborates on typical channel monitoring and alarming features built into line current differential relays and multiplexers to maximize the security and availability of the 87L protection and aid 87L scheme commissioning and troubleshooting of issues in the field.

Fourth, the paper considers current data alignment in 87L applications, including channel-based and external time-based methods. For the latter case, the paper reviews key application guidelines for engineering time sources in 87L applications and describes possible fallback strategies to account for situations when the 87L time sources are out of service or tolerance.

The paper includes three appendixes to expand on some key concepts related to 87L applications. Appendix A is a primer on time-division multiplexing (TDM) and synchronous optical network (SONET) technology. Appendix B explains the current alignment methods and reviews the foundation for the measurements of the round-trip channel delay and channel asymmetry. Appendix C reviews some key concerns related to the application of the Global Positioning System (GPS) to protection and presents a new terrestrial method of distributing time over a wide area.

II. 87L Channel Requirements

The following are the key channel performance criteria for 87L applications.

A. Availability

As an indispensable part of the protection scheme, the 87L channel needs to be of adequate availability. Channel availability means not only providing communications between a pair of 87L relays (i.e., keeping momentary and permanent channel outages to a minimum) but also meeting the applicable channel characteristics during an outage-free period. Channel availability is an input parameter in the overall 87L protection scheme availability calculations and, as such, is expected to be in the range of or better than the availability of the 87L relays. Channel redundancy is one method of enhancing availability.

B. Latency

Latency (channel delay or channel propagation time) is an additive component in the 87L trip time calculations. Excessive latency slows down the 87L operation and may violate the critical clearing times. Typical requirements for 87L channel latency are in the range of 5 to 10 milliseconds. Reference [1] suggests specifying channels with latency below 5 milliseconds.

Latency should be understood as a port-to-port propagation time that includes the buffering and processing of any active

communications devices used to make up the 87L channel. Also, the worst-case latency is of interest because in some networks, the latency may change considerably, depending on the data traffic, failure modes, or network configuration changes.

C. Bit Errors

Bit errors (i.e., corruption of data in transit) impact the security and dependability of the 87L protection that relies on the data. The 87L relays incorporate means to detect bit errors as well as secure the relay against undetected bit errors. Still, the channel is expected to have an adequately low bit error rate (BER). Excessive BER not only jeopardizes security but erodes dependability by causing the 87L function that detected the errors and rejected the data to be momentarily unavailable.

Typical utility requirements for BER are in the range of 10^{-3} to 10^{-6} for 87L channels. The exact requirement may depend on the security features built into the applied relays.

D. Channel Symmetry

87L schemes can align the remote and local currents using the channel alone (i.e., without the aid of any external time reference), but only if the channel is symmetrical (see Appendix B). This means that the propagation times in the transmitting and receiving directions are equal. For these schemes, channel symmetry is a key channel characteristic. Asymmetry in the order of a quarter to a half of a power cycle (depending on the relay design) renders the 87L schemes that align current without external time sources useless [2]. As in the case of channel latency, the worst-case asymmetry is of interest.

E. Other Desired Channel Characteristics

Other desired channel characteristics include:

- Simplicity of the channel configuration and stability of the channel performance over the 87L scheme lifetime (channels that are highly variable may degrade over time, causing problems for 87L applications).
- Ease of testing (channels link two points that are separate by definition—testing such entities can be challenging [3]).
- Simplicity of the channel-to-relay interface (the interface may be a source of performance and compatibility issues [3]).

III. Point-to-Point Fiber Channels for 87L Applications

A direct point-to-point fiber connection between 87L relays is often considered the preferred communication for line current differential schemes. The direct fiber method inherently addresses a number of the stated channel requirements, as the following explains.

A. Availability of Point-to-Point Fiber Channels

Direct point-to-point links do not involve any other active components that could fail or introduce failure modes. This increases availability. At the same time, however, direct channels lack inherent redundancy, as explained later in Section II, Subsection F, reducing availability compared with most networked 87L channels.

B. Latency of Point-to-Point Fiber Channels

Direct point-to-point fiber links communicate at the speed of light through the fiber. No extra delays are incurred as a result of converting to electrical signals, encoding, buffering, multiplexing, and demultiplexing.

C. Bit Errors in Point-to-Point Fiber Channels

Fiber is immune to the electrical interference that is commonplace in the electric system. This immunity and avoidance of active communications devices keep the BER for fiber channels in the order of 10^{-5} to 10^{-6}.

D. Symmetry of Point-to-Point Fiber Channels

Point-to-point channels are inherently symmetrical. The propagation times depend on the speed of light in the fiber medium and, as such, are guaranteed to be identical in the transmitting and receiving directions of a given fiber pair.

E. Other Characteristics of Point-to-Point Fiber Channels

Point-to-point channels are normally passive and practically reduced to a physical medium. As a result, they are easy to test [3], require a passive interface in the form of a fiber connection in the relay chassis, and are not subject to configuration changes and network maintenance or other activities. No other data traffic takes place over a dedicated link that otherwise may impact the security and/or dependability of the 87L scheme.

F. Disadvantages of Direct Point-to-Point Fiber Channels

There are three disadvantages of using direct point-to-point fiber links for 87L applications.

1) Limited Distance

Typically, relays can operate directly up to a distance of about 100 kilometers. If a longer fiber path is required for the application, either because the protected line is long or the channel is routed around the protected line for path diversity, optical repeaters at fiber regeneration sites may be required. The cost and impact on overall availability are not the only concerns related to repeaters and regeneration sites. Internal policies or regulations may require redundant power sources, physical security perimeters, access roads, and so on to the place of the regeneration installation, considerably increasing the cost and logistics of having amplifiers for each direct fiber link in those 87L schemes that involve long fiber runs.

2) Underutilization of Bandwidth

Fiber media are capable of reliably transmitting thousands of megabits per second and are able to provide communications services for entire cities over a single fiber pair. A typical 87L scheme uses kilobits per second, greatly underutilizing the medium and creating an impression of stranded investment.

3) Lack of Inherent Channel Redundancy

A point-to-point link does not provide any redundancy upon a failure of the fiber. Many 87L relays support two ports

that in two-terminal applications can be used with two direct point-to-point links to effectively provide redundant communications paths. Diversely routed fiber paths increase the dependability of the scheme. In some cases, the alternate path may require longer-reach optics than available directly at the relay, resulting in optical repeaters or regeneration sites required along the route.

IV. Multiplexed Channels for 87L Applications

The 87L data can also be transported via SONET/synchronous digital hierarchy (SDH) multiplexer systems, addressing the shortcomings of direct fiber channels. The SONET/SDH systems are designed to provide highly reliable and deterministic channels (Appendix A reviews the basics of the SONET/SDH networking method). From the point of view of the 87L relay, a SONET/SDH service appears as a virtual point-to-point link.

Section V discusses issues specific to 87L applications over multiplexed channels in detail. In this section, we only briefly contrast multiplexed channels with direct point-to-point fiber channels.

A. Availability of Multiplexed Channels

Multiplexed channels are carried over a network, and as such, their availability is adversely impacted by the finite availability of the many devices and physical channels that carry the data. This erosion in availability is compensated by the self-healing mechanism in the form of ring topologies and path switching, where the network routes the data traffic around a failed physical channel or a failed network device.

B. Latency of Multiplexed Fiber Channels

Delays in multiplexed networks are longer because they include signal conversion and buffering, in addition to the travel time of the light in fiber. Also, delays can change as the network switches paths to self-heal broken communications links or devices.

C. Bit Errors in Multiplexed Fiber Channels

BERs are also higher in multiplexed connections as compared with direct fiber connections. This is because there are more points where noise can couple to the data or clocks. Also, some of the local connections between the devices can use electrical signals, and some of the long-haul connections can use digital microwave. As a result, BERs would increase.

D. Symmetry of Multiplexed Fiber Channels

Symmetrical channels are no longer a given in a multiplexed system. Many multiplexers use unidirectional ring topologies. This means that the transmitting and receiving data paths are no longer coupled as they are in the direct fiber system. The multiplexer system needs to provide a method to guarantee that the transmitting and receiving paths are switched together. Typically, a short-lived asymmetry, lasting for a duration in the order of a few tens of milliseconds, is tolerable to 87L applications, depending on the relay design.

E. Other Characteristics of Multiplexed Channels

Multiplexed channels are more difficult to test and commission [3], have a tendency to exhibit some variability due to changes in the network, and rely on interoperability of the communications interface. In short, they bring the many shortcomings and issues of a networked channel as a price to pay for the benefits of cost-efficiency, path redundancy, and seamless connectivity to any remote location in the network.

F. Discussion

In practice, both direct point-to-point and multiplexed links can be used in 87L schemes. The selection involves a tradeoff between the ability to dedicate a fiber pair to a given 87L scheme and the cost and complexity of using existing multiplexed fiber and overlaying an 87L data stream within the SONET/SDH technology. Many 87L relays support dual ports to facilitate redundancy of communications. One port can be connected to a dedicated point-to-point channel, while the other can use a multiplexed connection.

V. 87L Channel Application Considerations

As part of a protection scheme, the 87L channel must be considered from the point of view of its failure modes. This means not only considering it functioning “as designed,” but considering it functioning under realistic, if rare, failure modes, such as fiber breaks, device failures, and configuration errors. This is no different than considering a loss-of-potential condition as a failure mode for a distance protection element, for example.

In this respect, the failure modes of direct point-to-point fiber channels are relatively well-known and straightforward. The main focus in this section is therefore on multiplexed channels.

A. Interface Compliance

When communicating over direct point-to-point fiber links, 87L relays interface with one another directly, typically using a proprietary method. Relays of the same model are used within any given 87L scheme, and because of this approach, their interfaces are naturally compatible. The direct fiber pair is just a physical medium (a passive and analog entity) for digital communication.

This is not the case for multiplexed channels. These channels are truly digital channels. On the transmit end, the 87L relay clocks its data out and the interfacing multiplexer samples the data signal in to buffer and transport it toward the destination. At the destination (receiving end), the multiplexer clocks the data out and the 87L relay samples the data signal in for usage in its 87L element (refer to Appendix A for the basic introduction to SONET). Standard interfaces are used between the relays and multiplexers. These interfaces are historically EIA-422 (North America) or G.703 (Europe) for electrical or copper hardware interfaces. The IEEE C37.94 standard specifies a dedicated and universal fiber-based interface for multiplexed protection channels.

The need to pass the data over an interface between the relay and the communications device calls for strict compliance with parameters such as jitter (short-term variability in the clock frequency), wander (long-term swings in the clock frequency), clock recovery (generating a data clock by the receiving device by phase-locking to the data line transitions), electrical signal levels, and fiber power budgets, as well as allowable options such as the data sampling clock source selection (which of the two communicating devices drives the clock).

Using standard communications interfaces provides the benefits of field experience and maturity, with many successfully implemented schemes in the industry and a broad depth of experience and case history to use as examples. However, the need to use an interface between the 87L relays and third-party communications devices adds complexity, calls for extra type testing and certification testing [3], and potentially creates compatibility issues, slowing down commissioning or impairing operation of in-service 87L schemes.

B. Data Sharing and Security

Organized around the TDM concept, SONET provides for excellent data security and isolation of data streams when sharing high-speed physical media between multiplexed channels.

Each channel has a reserved time slot and therefore a guaranteed bandwidth inherently protected from congestion due to data traffic spikes and other issues that can be inherent with generic packet-based transport networks, precluding them from applications like 87L.

Typically, 87L applications use a single DS-0 channel for communications between any pair of 87L relays in the scheme. The 56 kbps rate is sometimes used, but 64 kbps is the most common rate.

Several aspects related to the very nature of TDM systems and 87L applications are worth mentioning. They include data buffering and the danger of channel asymmetry, frame slips, and clock issues with T1 multiplexers.

1) Buffering and Impact on Latency and Asymmetry

In order to add the low-speed data rates of the DS-0 channel to the high-speed data rate of the T1 frame and subsequently drop the DS-0 stream at the destination, the DS-0 bits must be buffered at both the transmitting and receiving ends. At the transmitting end, enough bits must be collected before the assigned time slot can be filled at the higher clock rate of the T1 frame. At the receiving end, a T1 frame lasts for a short period of time, and the data need to wait to be clocked out at the rate of the DS-0 clock. The required buffers are relatively short—in the range of 150 to 200 microseconds for a T1 frame. Under normal conditions, said buffering adds a small time delay to the channel latency. However, the sheer existence of the buffers creates a potentially dangerous failure mode. A firmware deficiency combined with clock wander can inadvertently lead to an increased buffer size in one of the buffers. A longer buffer adds delay to one direction, creating channel asymmetry—a potentially dangerous condition for 87L applications. SONET networks balance the rigor of synchronicity (i.e., having closely locked clocks) with the danger of losing frames because of jitter and wander (known as frame slips). Small buffers are in place to prevent frame slips, but if the buffers malfunction, they may change channel latency, including the effect of channel asymmetry.

It should be pointed out that protection-class SONET networks typically have integrated channel and transport functions within the same chassis, sharing a backplane that contains timing pulses that are common to the transport side (SONET) and the channel side (T1) of a circuit. This greatly reduces the potential for issues dealing with wander and jitter and lost frames. Buffers are a normal part of telecommunications networks and are a way to capture information prior to filling the data frame with information. This concept is true for TDM and packet-based networks and is a mature practice, with solid performance compared with other methods. It is only the failure modes that may lead to undesired responses in buffering.

2) Frame Slips

Frame slips are theoretically less likely to occur within substation-class networks because transport hardware and channel hardware are contained within one chassis and thus share the frame timing bus on the backplane of the shelf. Should frame slips occur, alignment pointers will reestablish proper alignment. Frame slips are indicators that the synchronization sources in the network may be in a state of drift. These are serious issues and can lead to an unstable network, impacting the availability of 87L channels and 87L protection.

3) Clock Synchronization With T1 Multiplexers

For telecommunications-class SONET/SDH equipment, it is typical that T1 or E1 channel equipment is located in a separate shelf or chassis from the OC transport equipment. Timing pulses for synchronizing the T1 or E1 frames are not integral within one shelf. Synchronization is accomplished by using the synchronization bits within the T1 frame format or through an external timing source input such as a building integrated timing source (BITS) clock input. In this way, frame synchronization is derived from the synchronous output of the transport equipment.

When the transport equipment experiences an event that leads to switching to an alternate path, the synchronization bits can be momentarily lost from the transport equipment to the channel equipment until the transport layer is reestablished. When T1 or E1 framing is once again available from the transport node, the channel equipment will adjust the necessary framing pointers until the circuits and associated error detection and correction algorithms can once again run.

Multiframe alignment processes, such as pointer realignment, will normally occur to bring the T1 channel back into alignment so that the payload, or data within the T1 frame, is able to reestablish synchronism with the remote end of a discrete T1 device. For a typical T1 or E1 multiplexer, up to 60 milliseconds may be required to reestablish proper frame

alignment so that data can once again be passed successfully from end to end. For a substation-class optical network, T1 framing synchronism with the higher-order SONET network is virtually guaranteed, because the timing pulses are integral with the backplane of the SONET node.

C. Path Switching

Path switching is an inherent advantage of SONET networks. The SONET standard, applied in telecommunications-class and business-class networks and more rigidly applied in protection-class networks, calls for an interruption in a circuit to be sensed in 10 milliseconds and restored in 50 milliseconds on the transport side. The channel portion of network equipment may require an additional 60 milliseconds to reframe (synchronize) with the channel equipment on the remote end. This may result in a total circuit outage time of up to 120 milliseconds (note that protection-grade multiplexers perform path switching in 5 milliseconds).

Automatic rerouting of data around failed media or a failed communications device effectively provides for channel redundancy. Channel redundancy is a desired feature for 87L applications, but it may create problems as well.

First, switching a path in one direction only (transmit or receive) could make the channel latency different in one direction compared with the other and therefore create channel asymmetry. This method of switching is common in telecommunications-class transport equipment but atypical in substation-class or protection-class networks.

Second, switching to a much longer path can lead to channel latency beyond the specified limit driven by the maximum 87L trip time. In this respect, the path length is not only the physical length of the fiber but is also related to the device count and latency introduced by each device that carries the data.

Third, the alternate path is typically difficult to test. Testing it would require forcing a network failure, and this is typically difficult or not permitted [3]. As a result, the alternate path may have unknown characteristics to some degree, and switching to it can cause problems for the 87L schemes. Moreover, depending on the network design and path selection, there may be more than one alternate path, exposing the 87L scheme to more variability in the network performance.

Fourth, path-switching mechanisms can exhibit failure modes and lead to accidental cross-connections between different 87L schemes (including loopbacks). If not prevented by the relays or substation-class networks, these cross-connections could cause misoperation, typically of both 87L schemes involved.

Protection-class SONET multiplexers support configuration, testing, and monitoring tools to make path switching secure. Protection personnel engineering 87L schemes should carefully state their requirements when it comes to path switching. Some parameters to consider specifying are worst-case channel latency delays, network switching/failover times, asymmetrical delay tolerance, and joint telecommunications and protection engineering review of telecommunications network expansion or configuration changes on the transport side.

From the path-switching point of view, the most common SONET multiplexer topology is the two-fiber unidirectional path-switched ring (UPSR). SDH refers to this type of topology as the two-fiber subnetwork connection protection (SNCP). This topology requires a single pair of fibers between adjacent multiplexers. The topology transmits the data in opposite directions around the ring, and a local receiver chooses the best path. The UPSR/SNCP is the most simplistic ring topology to implement and is the most commonly used.

The other SONET ring topologies are the two- and four-fiber bidirectional line switched rings (BLSR). SDH refers to these types of topologies as two- and four-fiber multiplex section-shared protection rings (MS-SPR). A two-fiber BLSR/MS-SPR reserves half of its bandwidth for ring protection, and the four-fiber BLSR/MS-SPR utilizes a second pair of fibers for ring protection. The two-fiber BLSR/MS-SPR is complex and requires extensive up-front engineering to ensure protection bandwidth is always available, while the four-fiber BLSR/MS-SPR requires twice the fibers and optical components, making it more expensive to implement.

The features required to make the UPSR/SNCP feasible for 87L protection are the following:

- To prevent channel asymmetry, the multiplexer must be capable of selecting the primary and backup paths at the channel level. This ensures that the shortest path is used for both the transmitted and received 87L data.
- In the rare case when only a single direction (transmit or receive) is affected by a fiber break or equipment malfunction, the multiplexer must also have the ability to perform a “switch on yellow” function. The yellow refers to the yellow alarm of the affected channel. This alarm indicates that the remote channel interface is no longer receiving data. The remote alarm information is used to switch the direction that the local (unaffected) channel is using to receive data. The remote interface switches the received path automatically when the data are unavailable over the primary path. This ensures that the data used by the multiplexer are always sent over the same (symmetrical) path. This method works because in the unidirectional ring, the data are always transmitted in both directions through the ring and are always available for use by the 87L channel interface.
- Automatic reversal to the primary path on channel restoration is another feature required to provide optimal performance without further user intervention. Revertive switching from the backup path to the primary or preferred path should be automatic within the communications network and transparent to the relay system once the communications network is restored.

These advanced options are not available in telecommunications-class multiplexers, and therefore, some

87L users opt out of path switching and request static routes for 87L channels, particularly when using large networks with many legacy telecommunications-class devices. In this scenario, a medium or multiplexer failure would lead to a loss of communications between 87L relays rather than to a change in the communications path. It is not uncommon for protection-class SONET networks to complete the detection of a circuit path interruption, switch to a healthy path, and restore connectivity at the DS-0 level in 5 milliseconds or less without resulting in asymmetrical paths. Once the primary path is healed and is stable, the system can normally be set to automatically revert back to the preferred path without any further circuit interruptions. The total cycle time for a telecommunications-class SONET network may be as long as 120 milliseconds, may introduce significant asymmetry in large networks, and may not automatically switch back to the preferred path.

D. Accidental DS-0 Channel Cross-Connections

Some substation-class multiplexer systems support circuit and network path addressing to protect against accidental misconnections of the DS-0 channels. This is done in a multiplexer via circuit and/or network path addressing in the provisioning of a telecommunications channel used for protective relaying and works as follows.

The circuit address allows the user to set unique numerical addresses for each DS-0 circuit. The circuit address provides the ability to recognize and prevent circuit misconnections at the multiplexer interface, thus preventing unintentional connections between 87L relays.

The network path address provides additional protection. The path address allows for individual addresses to be set on transmit and receive data paths (inside of the circuit). This prevents inadvertent or intentional data loopbacks.

If the circuit and network path addresses do not match what is expected to be received, the communications channel is blocked from communicating and provides an alarm to the telecommunications network management system software.

This type of condition normally would occur during the initial provisioning or subsequent network provisioning and is detected at the DS-0 hardware interface module as part of its valid path-checking algorithm. Should a data packet arrive at the module with invalid addresses from the remote end, a continuous bit stream with all ones results at the output of the module, which can be interpreted by the receiving device as erroneous information. This feature is supported by some protection-class equipment, but not all.

E. Availability Considerations

Availability in SONET networks is high, assuming path switching is permitted. Three issues are worth mentioning in relation to 87L applications.

First, the local connection between an 87L relay and the first multiplexer is typically not redundant. This may have a small impact on the overall communications redundancy because only the failure of the local medium in the substation and/or the interfacing multiplexer would lead to the loss of service. This limitation can be overcome by using redundant ports in the relay to interface with two different communications multiplexers, each using a diverse path to the higher-level network.

Second, if static paths are configured for the 87L data, the self-healing mechanisms are not in place and the availability is reduced. The availability depends on the number of physical links and devices involved in passing the data on a static path, and these elements are connected in series in a classic reliability model of the system.

Third, there are considerable differences between the telecommunications-class equipment and substation-class or protection-class equipment.

IEEE 1613 establishes electrical and environmental criteria which electronic devices, specifically functioning in the communications realm at substations, need to meet in order to provide reliable services [4]. IEEE 1613 moves in the direction of requirements for relays and other critical equipment. Some of the IEEE 1613 highlights are:

- Operating temperature range of at least –20° to +55°C with no moving parts for air circulation.
- Ability to withstand up to 95 percent average relative humidity for a maximum of 96 hours and operate successfully in an average relative humidity of 55 percent.
- Ability to withstand dielectric tests with a pulse of 5 kV.
- Ability to withstand electrostatic discharge (ESD) testing of 8 kV and up to 30 A.

F. Data Integrity Protection Embedded in T1 Frames

The 192 bits in a T1 frame corresponding to the 24 DS-0 slots, each containing 8 bits of data, can be appended with a 6-bit cyclic redundancy check (CRC) data integrity protection code (using the extended super frame [ESF]). This data integrity check is applied for monitoring purposes of the T1 connection. A failed CRC does not cause frame retransmission (this would be contrary to the spirit of TDM and the concept of guaranteed deterministic data delivery), and the output DS-0 channels are not altered in response to the CRC failure. A persistent CRC failure in a repeating pattern can be used by the communications equipment to mark the connection as unhealthy and alarm and/or apply countermeasures, such as switching paths.

The end devices, such as the 87L relays, must monitor data integrity using their own methods, and they do not benefit from any data integrity detection that may be embedded in the T1 and higher-order multiplexed channels.

G. Realities of Using Multiplexed Channels in a Network

It is important to remember that telecommunications industry standard equipment typically adheres to standard SONET/SDH specifications, which historically have been designed to support mainstream telecommunications needs such as analog telephony, Ethernet (including Voice Over IP), and video.

Further, despite its determinism, SONET/SDH is a networking method. The hierarchy of the SONET/SDH data organization (DS-0 channels combined into T1 frames, T1

frames combined into OC-1 frames, and so on) invites a matching device hierarchy. For example, an 87L relay may interface at the DS-0 level with a protection-class T1 multiplexer located in the same substation, the said T1 multiplexer may interface with an OC-3 SONET multiplexer in the same substation, and the said OC-3 data may be passed to a higher-order OC transport multiplexer at a different site using a telecommunications-class cross-connect device. To a protection engineer, the DS-0 channel appears as a point-to-point service with a guaranteed bandwidth between the two ports in the network, but the underlying networking to make the connection possible can be relatively complex. The involved network devices may have been installed over long periods of time, be of different vintages and manufacturers, and have their own failure modes and possible limits to interoperability.

Recognizing the realities of networked channels is therefore another important consideration. Networks are large, potentially changing systems, comprised of a large number of devices relying heavily on standardized interfaces and services, built with different brands and classes of devices, maintained without taking an outage of the entire network, temporarily reconfigured for a number of reasons, exposed to human errors such as accidental cross-connection or loopback, and so on.

These issues can be mitigated by keeping the 87L applications simple, encouraging cross-education and cooperation between the protection and communications departments, enforcing communications network configuration and procedures critical to 87L applications, and using SONET/SDH equipment specifically designed for the more demanding protection applications by implementing homogeneous protection-class networks where possible.

Multiplexed 87L channels are considerably more cost-efficient than direct point-to-point channels. SONET/SDH offers the best performance so far when it comes to deterministic data delivery for 87L applications over multiplexed networks. However, as with any network, SONET/SDH networks are complex and may create problems for 87L schemes, particularly when assuming equipment malfunction or human errors. The 87L relays are designed to take a number of failure modes into account and follow a defensive design approach, as described in the next section.

VI. Design of 87L Relays for Communications Issues

A. Bit Errors and 87L Data Integrity

Noise in the communications channel can corrupt the data. The term “noise” refers to interference coupled to the channel medium or electronics, failing components in the electronic devices comprising the network, poor quality of fiber terminations and associated losses, marginal power budget for fiber transceivers, and so on.

Modern 87L relays typically use a 32-bit data integrity code to protect the 87L data. For example, when using a Bose-Chaudhuri-Hocquenghem (BCH) code to protect a 255-bit packet, the minimum distance for error detection is 10 bits, meaning all 9-bit errors are detected. Assuming a uniform distribution of the probability of corrupting any single bit in the packet, the probability of an undetected error is below $1.2 \cdot 10^{-10}$. Typically, 87L relays do not use any error correction algorithms because these algorithms would degrade the strength of data protection. Corrupted packets are rejected, and the relay algorithm falls back gracefully.

B. Disturbance Detection Supervision

Any data integrity protection has a finite, non-zero probability of defeat. Realizing that 87L relays send, receive, and use large numbers of packets during their lifetime, a second layer of protection against corrupted data is needed. For example, by sending packets every 4 milliseconds, a relay works with about 7.884 billion packets a year. A 32-bit data integrity check is sufficient if the channel is relatively noise-free. However, protective relaying applications need to assume the worst-case scenario of a standing noise in the communications channel, such as that caused by a failing optical component in the communications equipment or the relay. A very small probability of defeating the data integrity protection ($1.2 \cdot 10^{-10}$, for example) multiplied by the very large number of trials ($7.884 \cdot 10^{9}$ a year, for example) under the standing noise would result in a finite, non-zero probability of eventually accepting corrupted data and potentially an unwarranted 87L operation. This cannot be tolerated by a state-of-the-art protective relay.

In reference to Fig. 1, ultra-sensitive and fast disturbance detection logic supervising both the current-based 87L operation and the execution of the received 87 direct transfer trip bit (87DTT) is the preferred solution.

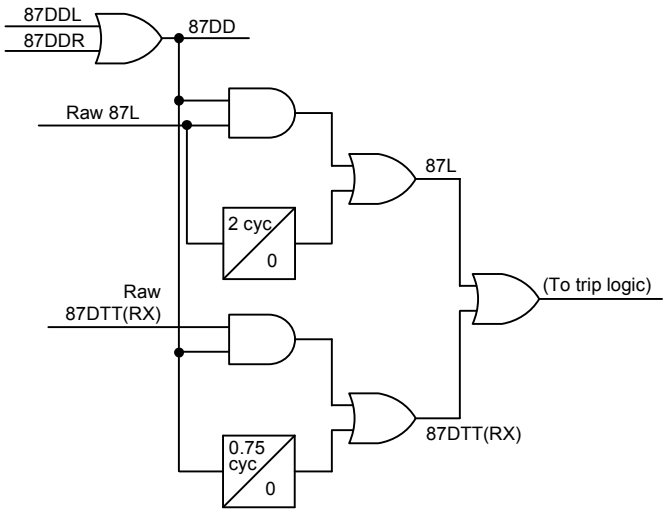

Fig. 1. Application of disturbance detection in an 87L relay

Note that corrupted data that would activate the raw 87L function or spuriously assert the received 87DTT bit would be short-lived, typically a single packet only. Therefore, a time-delay approach is used when supervising the 87L with disturbance detection—the response of protection is instantaneous if the fault is confirmed by the disturbance detection and only slightly delayed if the disturbance detection fails to pick up. This precaution is implemented in order to maximize dependability while still fulfilling the primary

purpose of the disturbance detection supervision, validating the remote data with the existence of a disturbance in the local currents or voltages.

The local disturbance detector (87DDL) may respond to sequence currents (zero- and positive-sequence) and voltages (zero-, negative-, and positive-sequence). The voltages are used to account for weak infeed conditions.

The local signals used in the 87DDL logic are taken before any 87L processing, time alignment in particular. In this way, the disturbance detector operates faster, because it does not need to delay the local data to align the data with the remote signals. Also, independent from the time alignment, the local disturbance detector guards against possible issues with data alignment that might be caused by any unusual behavior of the 87L communications channel.

The remote disturbance detector (87DDR) may respond to zero-, negative-, and positive-sequence components of all remote currents. If a given current is very low, such as upon the remote breaker being opened or under weak infeed conditions, the current is not used and permission is granted to operate. This is to preserve dependability of the 87L operation.

Once the disturbance is detected, the 87DD bit is maintained for some extended period of time (ten power cycles, for example) to ensure reliable 87L operation.

In one approach [5], both the local and remote parts of the disturbance detection logic use the same adaptive algorithm depicted in Fig. 2. First, a one-cycle difference is calculated for the input phasor IN. This operation is executed on a sample-by-sample basis and yields a very fast and sensitive response due to the subtraction of the standing value in the input phasor IN. Subsequently, the magnitude of this incremental signal is calculated. This magnitude, DX, is filtered through an infinite impulse response (IIR) filter in order to get a notion of the standing noise in the DX signal. Normally, this standing noise is very small because even under the presence of harmonics, the phasor errors tend to be periodic and, as such, would cancel as a part of the delta calculation over one power cycle. The input to the IIR filter is clamped at appropriate minimum and maximum values for security and dependability. The standing value of the DX signal, multiplied by a factory constant k_{TH}, becomes an adaptive threshold of the comparator. If the DX signal exceeds such threshold, the output OUT asserts.

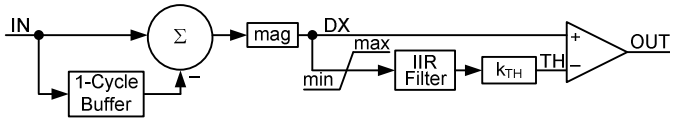

Fig. 2. Adaptive disturbance detector logic

In this way, the disturbance detection algorithm is very sensitive, yet will not trigger under load conditions even if the load current or voltages are heavily distorted, as long as they are periodic. With this implementation of the disturbance detection, there are no concerns with the dependability of the supervised raw 87L and 87DTT outputs. First, the disturbance detection logic is very dependable and fast. Second, even if it were to fail, the net effect is delayed but still results in near instantaneous operation of the raw 87L function with a slight delay of two cycles and not a failure to operate.

C. Other Benefits of Disturbance Detection Supervision

Consider the simplified diagram of the 87L scheme shown in Fig. 3. A line current differential scheme consists of two or more independent relays located in different substations, supplied from different batteries, connected to different secondary circuits, and subjected to different environmental conditions, including conducted and radiated electromagnetic transients and static discharge conditions. Due to the fact that the relays making up the protection zone are not expected to be exposed to the same transient noise or hardware problem, there is an opportunity to implement 87L schemes that apply stronger self-tests by cross-checking data between individual relays of the scheme in order to provide better security for communications events and failures.

In this respect, it is worth realizing that disturbance detection guards not only against undetected communications errors but against multiple problems, such as relay failures, greatly increasing the security of the 87L scheme.

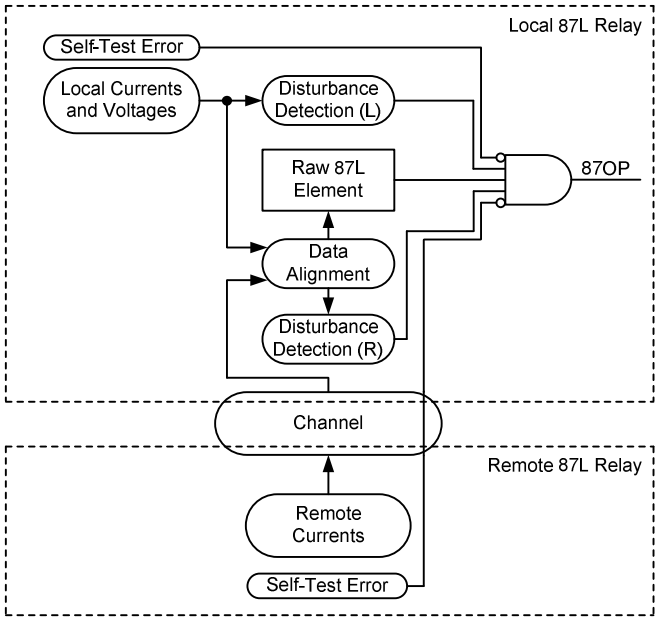

Fig. 3. Disturbance detection guards against multiple problems, greatly increasing security

Consider the following failure modes:

- Undetected communications error (defeated data integrity check). Under this scenario, the raw 87L function as well as raw 87DTT may spuriously pick up because of heavily corrupted remote data. For the same reason, the disturbance detector responding to the remote currents may pick up (87DDR). However, the portion of the disturbance detection that responds to local currents and voltages (87DDL) will not assert, preventing misoperation.
- Failure in the ac acquisition chain of the local relay, such as an analog-to-digital converter (ADC) problem. Under this scenario, the raw 87L function may spuriously pick up because of heavily corrupted local data. For the same reason, the disturbance detector responding to the local currents and voltages may pick up (87DDL). However, the portion of the disturbance detection that responds to remote currents (87DDR) will not assert, preventing misoperation. Subsequently, the self-test error will assert in the local relay in response to the problem, taking it out of service. In this way, the disturbance detection logic gives extra time to the self-test logic and, in combination, dramatically improves the security of the 87L scheme.
- Failure in the ac acquisition chain of the remote relay (such as the ADC problem). Under this scenario, the raw 87L function may spuriously pick up because of heavily corrupted remote data. For the same reason, the disturbance detector responding to the remote currents (87DDR) may pick up. However, the portion of the disturbance detection that responds to local currents and voltages (87DDL) will not assert, preventing misoperation. Subsequently, the self-test error will assert in the remote relay in response to the problem, taking it out of service, including the remote 87L function and all other instances of the 87L function via the provisioned blocking bit in the 87L data packet. In this way, the disturbance detection logic gives extra time to the self-test logic and, in combination, dramatically improves the security of the 87L scheme.
- Problem with data alignment. Assume a hypothetical channel event or a failure of an internal component of the relay that leads transiently to a misalignment of the local and remote data (such as a single upset event in a microprocessor). Under this scenario, the raw 87L function may spuriously pick up because wrong local and remote current data were compared. However, the portion of the disturbance detection that responds to local currents and voltages (87DDL) will not assert because it bypasses the alignment operation entirely, preventing misoperation of the 87L scheme.

D. Relay Address Checking

Cross-connection of 87L relays is another communications event to consider. In this scenario, a given relay is inadvertently connected to a wrong remote relay, or the relay is looped back into itself by mistake as a part of communications circuit testing. As explained in Section V, Subsection D, protection-class multiplexers may prevent and set off an alarm on cross-connections within the SONET/SDH system, but the cross-connection can still happen at the cable or fiber patchcord level between the multiplexers and relays. To guard against this threat, the 87L relays use transmit addresses and check them upon reception against the expected receive address setting. When the received and expected addresses do not match, the data are not used, and the 87L function is taken out of service while an alarm is set for the user.

The ability to override address checking is typically provided in order to facilitate loopback testing of the 87L relays.

VII. Channel Monitoring in 87L Applications

Line current differential schemes are channel-dependent, and therefore, it is beneficial to monitor some key characteristics of the channel in real time. This helps in commissioning and troubleshooting but also improves the overall performance of the scheme by discovering and rectifying channel issues in a timely manner. In addition, certain characteristics of the channel may be used automatically by the 87L function to engage more secure settings, switch to a redundant channel if applicable, and more.

A. Round-Trip Delay and Step Change in Delay

The term “round-trip channel delay” refers to the sum of channel latency in the receiving and transmitting directions. This is an important attribute of the channel because it impacts the total trip time of the 87L scheme.

In applications with direct point-to-point fiber connections, the round-trip channel time is constant and should not change. In applications with multiplexed channels, the round-trip time may change when the SONET/SDH system reroutes data traffic in response to lost fiber connections or the failure of a multiplexer.

In any case, it is beneficial to monitor the round-trip delay and alarm if this delay exceeds the maximum allowable value or if the value is too high and clearly indicates abnormal operation of the communications network.

The round-trip channel delay can be measured without absolute time connected to the 87L relays, as explained in Appendix B.

A step change in the round-trip delay is another important channel attribute. Changes in the round-trip channel delay signify switching events in the communications network.

Alarming on these switching events can help to discover issues with the communications network, regardless of whether the total round-trip delay is within the system design specification or not.

B. Channel Asymmetry

If valid time sources are connected to both relays of a given communications channel, it is possible to measure channel latency in the receiving (t_{CH_RX}) and transmitting (t_{CH_TX}) directions individually, as explained in Appendix B. The difference between the delays in the two directions is channel asymmetry.

Channel asymmetry is an important channel attribute. A typical consideration is related to using symmetrical channels in the 87L channel-based alignment mode. Relays having access to absolute time can constantly monitor if the channel is truly symmetrical during in-service conditions, as a part of scheme commissioning, or during troubleshooting. This is especially beneficial for multiplexed channels or when considering potential failure modes of any active communications component between any two 87L relays.

Note that the asymmetry measurement depends on the time sources at both ends of a given channel. Accuracy of the used time sources also impacts accuracy of the asymmetry measurement. This is an important consideration for avoiding spurious channel asymmetry alarms.

C. Lost Packet Counts

Typically, an 87L relay declares a lost 87L packet if any of the following occurs:

- The data as detected by the integrity code are corrupt.
- The time elapsed since the last packet the relay received exceeds 100 percent plus margin of the normal time between the packets (packet time-out).
- The difference between the sequence number the relay receives in the present packet and the sequence number it receives in the last packet is other than exactly 1.

The relay may run a lost packet counter to count packets that have been lost in the most recent few tens of seconds (instantaneous channel quality measure). In addition, the relay may run a 24-hour lost packet counter (long-term channel quality measure). Alarm thresholds are typically provided to alert and force remediation if the channel becomes too noisy, resulting in elevated counts of lost packets.

Lost packet counts can be used to estimate the BER of the channel and compare it with the BER requested from the communications department that owns the 87L channels.

D. Other Channel Characteristics

Other monitoring functions can be provided in 87L relays as well. This includes measures such as momentary channel break or noise burst.

E. 87L Channel Monitoring in Multiplexers

Some of the channel monitoring and alarming functions are similar between 87L relays and protection-class multiplexers. This is beneficial because comparing the relay and multiplexer measurements can greatly help in troubleshooting some problems.

Also, as a rule, the relay and communications systems are maintained by separate groups, and alarms in both systems ensure that both equipment owners are aware of the issue at the same time through their own familiar and trusted alarm systems.

In addition, multiplexers always have access to a common time reference by the principle of TDM data transport and therefore can measure more channel parameters as compared with relays.

Typical SONET/SDH multiplexer systems provide performance monitoring and alarming at the transport level but are blind to problems at the individual circuit level.

SONET/SDH systems designed for the transport of mission-critical data, including 87L protection, exist today. These systems provide a level of performance monitoring and notification required for rapid identification and response to communications issues. These systems have the ability to:

- Redirect 87L communications within 5 milliseconds in the event of fiber-optic path or multiplexer failures.
- Monitor channel latency and asymmetry and provide alarms for delays or asymmetry that affect 87L performance.
- Provide channel performance information without interruption of the 87L data circuit.
- Prevent unintentional misconnections between access ports for 87L devices.

There is an increased user expectation that the monitoring functions are provided to increase system availability and security. The communications system and the multiplexer together can provide the information required to quickly isolate and identify communications issues.

VIII. 87L Data Alignment Considerations

Applications of 87L schemes that require external time must ensure the external time sources are engineered to protection standards and account for the case of the loss-of-time information. This section focuses on these two important considerations. Appendix B reviews the basics of data alignment in 87L applications, including channel-based and external time-based alignment.

A. Application Considerations for 87L Time Sources

Microprocessor-based relays are often connected to GPS-synchronized clocks to ensure meaningful and easily comparable fault and sequence of event recordings or to enable synchrophasor applications. This applies to 87L relays as well.

However, 87L relays may or may not use external time in their 87L functions. Using time in the 87L protection (for asymmetrical channels) or refraining from using time (for symmetrical channels) is a major application decision impacting the dependability of the overall scheme, its failure modes, and the necessity for proper engineering of the time sources and the time-distribution circuits in a substation.

In general, the following three application scenarios are possible:

- The 87L function does not use external time at all. This application is possible for symmetrical or near-symmetrical channels and is the most robust because it does not rely on the extra equipment needed to provide time. Instead, it requires assurance that the channels will remain symmetrical. This works best with direct point-to-point fiber connections.
- The 87L function uses external time for channel monitoring only. This application is possible for symmetrical or near-symmetrical channels. The relays use external time for better channel monitoring. In particular, with the aid of common time, it is possible to measure channel delays independently in the transmitting and receiving directions and calculate channel asymmetry. As a result, this application can monitor the channel for asymmetry and fall back to a safe mode should the channel become asymmetrical. Therefore, this application suits well-multiplexed (SONET/SDH) channels engineered and configured for symmetrical operation. The application requires monitoring the quality of provided time in order to avoid false or missing indications of channel asymmetry, but the application of time is not extremely critical.
- The 87L function uses time for both protection and channel monitoring. This application allows asymmetrical channels but calls for the time sources to be engineered to protection-grade standards and to be monitored. A fallback logic is required to cover situations when the external time is degraded or not available at all.

Historically, the timing signal in use is IRIG-B. By its nature, the timing signal is not dynamic, but rather a repeating pattern (1 pulse per second [pps] mark, time and date code, and time-quality indication). As a result, devices using time, such as the 87L relays, can easily ride through impairments and temporary loss of the IRIG-B timing signal.

Typically, the time-receiving device relies on its own internal clock and phase-locks the internal clock to the IRIG-B input. This may include an online calibration of the internal clock—a continuous adjustment of the clock frequency based on the time elapsed between consecutive 1 pps pulses. As a result, the internal clock becomes very accurate and could provide a ride-through for the loss of the IRIG-B signal in the range of tens of seconds, despite finite accuracy and variability in the relay components or temperature variations.

From this perspective, security of IRIG-B time distribution is more important than dependability.

To provide proper security, the time-receiving device monitors the integrity of the IRIG-B signal. This typically includes jitter in the 1 pps signal, consistency of the time and date code, and, most importantly, the time-quality bits embedded in the IRIG-B signal as per IEEE C37.118 [6].

Critical applications of time, such as 87L protection and synchrophasors, require using clocks capable of asserting the time-quality bits to inform the time-receiving devices about possible timing error, such as during freewheeling when unable to lock to GPS satellites.

When using time for 87L protection, we need to treat the time sources and distribution circuits as a part of the protection scheme. This calls for the following:

- Using due diligence when selecting components of the timing network.
- Applying proper grounding and shielding for copper-based connections, observing the maximum burden for outputs, and following recommendations for maximum distance of copper cables.
- Applying fiber-based IRIG-B distribution for longer runs.
- Documenting the time-distribution networks with diligence.
- Including the clocks and time-distribution networks in the rigorous commissioning procedures and periodic testing programs [3].
- Monitoring the satellite clocks and relays for failures of timing signals and attending to the alarms in a timely manner.

When applying line current differential schemes over asymmetrical channels, the timing signals become as important as the current, voltage, or trip signals and must be engineered, commissioned, and maintained to protection-grade standards.

B. Fallback Strategies for Time-Based Alignment

87L schemes that use external time sources must provide a well-defined response that suits user preferences in situations when the time source is lost or degraded. This is often referred to as time fallback logic. A modern relay can provide for several time fallback modes, varying with respect to balancing security and dependability upon the loss of time. When selecting a fallback mode, we typically consider availability of the second redundant protection scheme, as well as regulatory constraints or internal utility practices related to operating a line without redundant schemes capable of instantaneous fault clearance.

Table I summarizes possible time fallback modes, progressing from the simplest (and most secure) to more elaborate solutions that attempt to enhance dependability.

TABLE I
SUMMARY OF TYPICAL TIME FALLBACK MODES

Mode	Summary of the 87L Scheme Response
1	If any required time source is unavailable or degraded beyond a safe 87L usage, the 87L function is effectively inhibited at all relays of the 87L differential system. This mode is biased toward security of protection. There is no attempt to continue providing 87L protection upon loss of a required timing source.
2	If a local and/or remote time source for a given channel is unavailable or degraded, the affected channel is forced out (i.e., effectively marked as unusable). The relays respond by switching to a hot standby channel, switching to the slave mode, or disabling the 87L function entirely, depending on the application and the status of the other channels. This mode provides no benefits in two-terminal, single-channel applications, but it may maintain dependability in two-terminal applications with redundant channels and three-terminal master applications if only one channel operates in the external time-based alignment mode.
3	If a local and/or remote time source for a given channel is unavailable and the channel was symmetrical prior to loss of the time reference, the logic forces the affected channel into the channel-based alignment mode. The 87L settings may additionally switch into high-security mode, and the relay continues to use the channel. If the switchover to channel-based alignment is impossible, the logic forces out the channel, with consequences similar to those in fallback Mode 2.
4	If a local and/or remote time source for a given channel is unavailable and the channel was symmetrical prior to loss of the time reference, the logic forces the affected channel into the channel-based alignment mode. The 87L settings switch into high-security mode, and the relays continue to use the channel. This state continues until the channel switches. The logic detects channel switching via the step change in the round-trip channel delay or temporary loss of channel. If the logic detects path switching in the multiplexed network while in the channel-based alignment mode or if switchover to channel-based alignment is impossible, the logic forces out the channel, with consequences similar to those in fallback Mode 2.

Table II reviews the applicability of the four time fallback modes to typical line current differential applications [5], including two- and three-terminal lines, single or redundant channels, and master or slave operation.

TABLE II
APPLICABILITY OF TIME FALLBACK MODES

Application	Merits of Time Fallback Modes
Two-terminal line with redundant channels	All modes have merit. In Mode 2, the scheme can continue operation with the second channel. In Modes 3 or 4, the scheme can continue operation if the channel was symmetrical at the moment of time reference loss.
Three-terminal line with all relays as masters	All modes have merit. Mode 2 has merit if not all channels are synchronized based on time. In Modes 3 or 4, the scheme can continue operation if the channel was symmetrical at the moment of time reference loss.
Two-terminal line with single channel or three-terminal line with one master and two slave relays	Modes 3 and 4 can allow continued operation of the 87L scheme if the channel was symmetrical at the moment of time reference loss. The use of Mode 2 has no merit and will result in 87L function loss because no alternative channel is available in these applications.

Fig. 4, Fig. 5, and Fig. 6 illustrate some of the typical scenarios for the introduced time fallback modes.

Consider the two-terminal, dual-channel application depicted in Fig. 4. Typically, one channel (assume Channel 1) is a direct point-to-point fiber connection, while the backup channel (Channel 2) is a multiplexed channel. Assume further that the multiplexed channel cannot be trusted as symmetrical. This application may use channel-based alignment for Channel 1 and time-based alignment for Channel 2, with both relays connected to valid IRIG-B sources. Assume time fallback Mode 2 is used. In this scenario, the scheme is immune to problems with time as long as Channel 1 is available. If either relay loses time, Channel 2 is marked as unusable, meaning the scheme lost channel redundancy but continues working as long as the primary channel is available. It will take both the loss of either of the time sources and the loss of Channel 1 for the scheme of Fig. 4 to lose dependability.

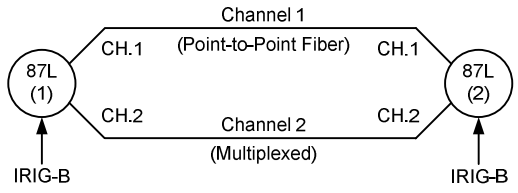

Fig. 4. Two-terminal application with redundant channels

Consider the three-terminal master application depicted in Fig. 5. Assume Channel 1 cannot be trusted as symmetrical, while Channels 2 and 3 are guaranteed to be symmetrical. As a result, CH.1 in Relay 2 and CH.2 in Relay 1 are configured to use time-based alignment and Relays 1 and 2 must have valid time sources connected. Assume time fallback Mode 2 is used. If either Relay 1 or 2 loses time, Channel 1 is marked as unusable, meaning Relay 1 cannot use data from Relay 2 and Relay 2 cannot use data from Relay 1. As a result, Relays 1 and 2 switch to slave modes, while Relay 3 receives all the data via symmetrical Channels 2 and 3 and continues protecting the line in the master mode, sending direct trips to the slave Relays 1 and 2. In this way, dependability is preserved despite the loss of time signals.

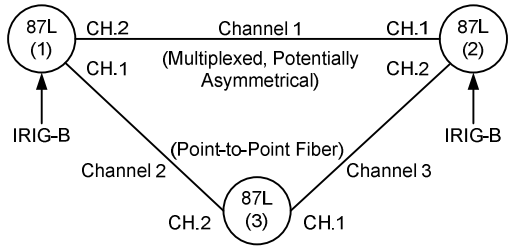

Fig. 5. Three-terminal application with three channels (all relays are masters)

Consider the two-terminal, single-channel application depicted in Fig. 6. The channel may or may not be symmetrical, and therefore, time-based alignment is used, and both relays must be connected to valid IRIG-B sources. Having the absolute time available, both relays measure channel asymmetry. Assume time fallback Mode 4 is used.

If the channel asymmetry was small at the moment of losing time at either of the relays, the relays will switch to the channel-based mode and continue to provide protection. If the channel is subsequently switched in the multiplexed network, as detected by step change in the round-trip time, the 87L function is blocked.

If at the moment of losing time, the channel was not symmetrical, the 87L function is blocked right away in the time fallback Mode 4.

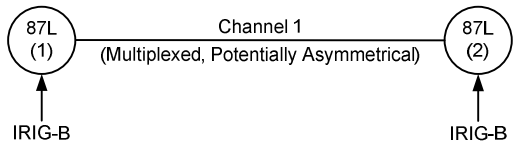

Fig. 6. Two-terminal application with a single, potentially asymmetrical channel

C. Terrestrial Distribution of Time

Using wide-area time for protection applications has been historically approached with some reluctance. Not only is the overall protection scheme more complex, thus less reliable, but also wide-area time depends on the accessibility of the GPS system originally provisioned for military applications and controlled by the U.S. Department of Defense (DoD).

Recently, a terrestrial time-distribution method was proposed that overcomes the many concerns of using GPS in protection applications [7]. Appendix C reviews the key concerns related to GPS-based time sources and many details of the new terrestrial time-distribution scheme.

IX. Conclusion

Line current differential protection provides excellent performance and simplicity of application from the traditional protection engineering point of view.

From the point of view of communications, engineering current differential schemes is a relatively new area and requires close attention. Nonissues when handling the bulk of typical data may become very critical when handling 87L data traffic. These issues include channel latency, channel asymmetry, BERs, path switching, and cross-connecting of multiplexed DS-0 channels.

Many of these issues can be taken care of by proper design of the 87L relays. Considerable progress has been made since the first deployment of microprocessor-based line current differential schemes approximately two decades ago. New schemes apply more security and can deal with a whole array of communications impairments.

Similarly, new protection-class multiplexers are designed with adequate attention to the 87L requirements. As a result, 87L applications over multiplexed channels are becoming safer. Still, we need to keep in mind that the utility communications infrastructure has been typically built over long periods of time and is made up of all sorts of equipment, including telecommunications-class multiplexers not specifically designed for protection applications. In such cases, using modern relays designed for fail-safe response is a prudent approach.

Modern relays and multiplexers perform a number of channel monitoring functions. These real-time measurements should be enabled and used for alarming. They enhance the overall performance of the 87L schemes by calling attention to problems and forcing proper maintenance of the equipment for conditions that could eventually impact the 87L protection schemes if not attended to in a timely fashion. Also, they are helpful in commissioning, testing, and troubleshooting.

Safe usage of time in 87L applications becomes possible because of the availability of safer terrestrial wide-area time distribution. Terrestrial time systems make the timing signals less reliant on the GPS system, thus eliminating many of the traditional concerns associated with time-based 87L current alignment and applications over asymmetrical channels.

87L applications are inherently multidisciplinary and involve both the protection and communications departments in the user organization. Fostering cross-education, encouraging peer reviews of changes, and using the same, more precise language between the protection and communications engineering groups result in better understanding of the key requirements and in improved overall performance of the 87L schemes.

X. Appendix A: Basics of Time-Division Multiplexing and SONET/SDH

TDM is a data communications method that interleaves multiple data streams over the same physical medium, giving each data stream a predefined, fixed-length time slot for utilizing the physical connection. This way, all data streams (subchannels) take turns when using the physical channel and appear to be communicating simultaneously. The time slots are arranged in a consecutive order, preceded by a synchronization bit sequence. This entire bit sequence, including both the payload and the synchronization and time slot information, is known as a TDM frame, which is commonly referred to as a T1 or DS-1 frame in the SONET hierarchy or an E1 frame in SDH. TDM frames are continuously assembled and transmitted—when one frame finishes, the next frame begins, and the process repeats.

Guaranteed bandwidth and data delivery times are key advantages of TDM over alternative methods of sending data without considering if the medium is idle or busy at the moment of intended transmission (such as Ethernet). On the other hand, the bandwidth in TDM networks is reserved for a configured subchannel whether the channel is actually sending new information or not, which leads to a less efficient utilization of the physical medium compared with the alternative (packet-based) methods.

Synchronous TDM is the most prevalent implementation. In synchronous TDM systems, the data bits are clocked in and out of the TDM network using clocks that are synchronized across the network. These systems include T-carrier and SONET in a typical electric utility environment.

Synchronous methods use extra bit sequences in the TDM frames to phase-lock the clocks across the network. The quality of this synchronism is finite because the phase-lock loops swing around their equilibriums, locking the clocks together. Departure from the equilibrium (i.e., from the perfect frequency and phase of a clock signal) is defined as jitter (short-term variability in the clock phase) and wander (long-term swings in the clock frequency and phase). The interconnected TDM devices, as well as the end devices, must tolerate a certain amount of jitter and wander in order to communicate error-free (without losing TDM frames).

The most common and lowest-order subchannel in TDM networks is referred to as a Digital Signal 0 (DS-0) and represents a bit stream of 64 kbps. Historically, the DS-0 channel stems from carrying digitized voice over a multiplexed medium. In traditional telephony, the audio signal is digitized at an 8 kHz sampling rate using 8-bit pulse-code modulation. The product of 8 bits per sample and 8,000 samples per second resulted in a data rate of 64 kbps. The 64 kbps is the maximum bandwidth of a DS-0 channel, but it can be divided into low-rate subchannels in some implementations, resulting in several lower-speed applications being sent over one 64 kbps time slot. For example, up to four 9.6 kbps EIA-232 circuits can be inserted into a single 64 kbps time slot by using a subrate multiplexing technique.

DS-0 channels are typically assembled in groups, constituting a higher-order multiplexing known as T-carrier. The most popular T1 format carries 24 DS-0 channels with an extra 8 kbps of framing information for synchronization and demultiplexing at the receiver, resulting in a 1,544 Mbps transmission rate. A device interfacing a number of DS-0 subchannels into a T1 multiplexed channel is known as a T1 multiplexer.

At the origin, the role of a multiplexer is to interleave or merge (multiplex) the lower-rate channels or circuits, such as DS-0 channels, into a higher-order or transport level, such as T1. At the destination, the multiplexer disassembles or splits (demultiplexes) the higher-rate channel into subchannels or circuits.

In addition, a multiplexer facilitates interoperability with end devices by supporting a number of interfaces at the circuit side, such as EIA-422 and EIA-232. This aspect of multiplexing promotes standardization because it leads to fewer types of interfaces for the transport level while supporting practical interfaces used by the variety of end devices. In a way, a multiplexer is a natural conversion point between different media, data rates, modulating and encoding techniques, and so on.

SONET networks follow the general concept of multiplexing into higher data rates [8]. SONET networks carry synchronous transport signal (STS) frames. The basic STS frame is known as STS-1 and is equivalent to 28 T1 channels. When using fiber media, STS-1 is referred to as OC-1 (optical carrier). OC-3 represents three times the OC-1 carrier, OC-12 represents twelve times OC-1, and so on. The most popular OC rates progress in multiples of four: OC-3, OC-12, OC-48, and so on.

In general, there are three types of SONET devices: add-drop multiplexers (high speed or line side for transport and low speed or circuit side for interfaces), digital cross-connect systems (cross-connecting or mapping of multiple high-speed carriers), and regenerators (regenerating the transport signals to allow longer runs between the add-drop multiplexers and/or digital cross-connects). In addition, large SONET networks may include precise clocks (such as cesium or GPS-based clocks) to help with the system-wide synchronization of the network to facilitate a slip-free communications and network restoration.

The add-drop multiplexer (also referred to as a node) is the most common type of SONET device. Different implementations of an add-drop multiplexer allow different data rates and types of interfaces on the circuit side. Some multiplexers may only support T1 levels and higher, while some, such as protection-class devices, may interface circuits as low as DS-0 directly.

SONET networks are typically built in rings, allowing multiple paths for the data between any two add-drop multiplexers in a given ring. This approach facilitates self-healing via path switching, meaning rerouting the data around a failed physical medium or device.

SONET rings may intersect at more than one location, facilitating more reliable data delivery between any two points

through redundant paths (i.e., true networking). The intersection points are provided by the digital cross-connect systems and are built into protection-class SONET equipment.

The physical media in SONET networks predominantly include single-mode fiber (long-haul channels) but may include wireless media such as digital microwave (medium range) if the bandwidth does not exceed OC-12 capacity. SONET networks may also include copper connections, which pass bandwidth up to DS-3 levels between nodes. Copper connectivity at bandwidths higher than a T1 (1.544 Mbps) is typically not recommended, as exposure to electrical interference in substations may corrupt data flow.

T1 and SONET are the North American standards. The European equivalents, with slight expansions and differences, are known as E1 and SDH, respectively. It should be noted that while the basic building blocks of both T1 and E1 equipment reside at a 64 kbps DS-0 channel, the E1 has a bandwidth sufficient to accommodate 30 DS-0 channels of data as opposed to 24 channels in the T1. The two systems at the multiplexed level are therefore not directly compatible with each other. As a result, higher-order transport layer SONET and SDH systems also operate at different data rates.

Over the years, SONET/SDH technology matured and incorporated a number of expansions and improvements. Today, SONET/SDH systems are probably the most popular networking methods in applications that require a high level of determinism in data delivery. In this context, we distinguish between telecommunications-class equipment designed and manufactured for general applications, substation-class equipment designed and manufactured for more demanding electric utility applications, such as supervisory control and data acquisition (SCADA), and protection-class equipment designed and manufactured to support the most demanding protective relay applications, such as 87L schemes.

XI. Appendix B: Alignment of Current Data in Microprocessor-Based 87L Relays

The differential protection principle requires the values of current measured digitally at geographically dispersed line terminals to be time-aligned. Violation of this basic requirement can lead to a total loss of security and dependability of the 87L scheme. Note that a timing error of half a power cycle is equivalent to a total inversion in directionality of the current—a forward fault would appear reverse and vice versa.

The challenge for line current differential schemes (as compared with any other differential relay) is that the input currents are taken at locations tens or hundreds of miles apart by independent relays communicating over a long-haul channel.

In general, the following requirements apply to the data handling and synchronization for 87L schemes:

- Minimum requirement for extra payload to communicate sequence numbers, time stamps, and other timing and data-tagging information.
- Security and fast recovery from lost packets and channel brownout conditions.
- Immunity to step changes and variations in channel delay.
- Accuracy of data alignment better than a few electrical degrees (1 electrical degree yields a spurious differential current of less than 1 percent of the through current).
- Quick startup, in the order of a few tens to a few hundreds of milliseconds.
- Ability to work in multiterminal applications.

A number of different solutions are used in the industry to provide data alignment for 87L schemes. These solutions differ based on the way the communications bandwidth is utilized by a given relay design, whether the scheme communicates samples or phasors, how often the packets are sent, and what kind of operating characteristic is used for tripping (different 87L characteristics have different immunity to current misalignment).

Two major solutions are typically applied.

In one group of methods, the relays are allowed to sample asynchronously from each other, independently tracking system frequency and potentially, but not necessarily, aligning their samples with the absolute time (for accurate fault recording). The 87L alignment mechanism measures the clock offset between each pair of free-running relays that communicate over a channel and uses the calculated offset to shift the current values in time in order to align them properly.

The other group of methods uses the measured clock offset to force the relays to sample synchronously with each other. A control loop is implemented to zero out the current sampling clock offset by speeding up or slowing down the relay sampling clocks. This method works adequately for two-terminal applications but faces considerable challenges in multiterminal applications. Not only does a cluster of relays need to converge, but all relays may need to track system frequency in addition to staying in synchronism with each other. This poses questions regarding the overall stability of the alignment method and limits the speed of recovery from communications events.

When communicating current phasors rather than samples, a given 87L scheme is practically required to use the second approach. This is because the phasors are typically exchanged more rarely and cannot be resampled for alignment. Instead, they must be measured simultaneously using synchronized sampling clocks.

The 87L schemes communicating current samples may use either of the two methods. In the first approach, the alignment and frequency tracking may be done in one step by resampling the received current samples in the relay firmware.

Both of these approaches stem from the measurement of the clock offset. One method measures the offset and uses it to shift the data. The other method controls the offset at zero by speeding up or slowing down the clocks so it does not need to shift the data.

Regarding the measurement of the clock offset, two application scenarios are possible.

In applications with symmetrical channels (the channel delays in the transmitting and receiving directions are equal),

the 87L relays measure the clock offset using an industry-wide method known as ping-pong (see Appendix B, Subsection A).

In applications with asymmetrical channels (the transmitting and receiving delays differ by more than 2 to 4 milliseconds), the 87L must use an external common time reference to measure the clock offset because the ping-pong principle fails (see Appendix B, Subsection B).

In general, the channel-based method is preferred over the external time-based method for its simplicity and independence from time sources historically provided by the GPS satellite system and clocks in substations.

When operating in the external time-based synchronization mode, 87L schemes require the time sources to be engineered for protection-grade performance (see Section VIII, Subsection A). This includes monitoring of time quality and fallback logic when the sources are not available or are out of tolerance.

In this section, the term "clock" refers to the current sampling clock and time, not to the data clock associated with serial communications between 87L relays.

A. Channel-Based Synchronization

Refer to Fig. 7. In the channel-based alignment mode, Relay 1 sends its 87L packet and time-stamps the moment of transmission as t_0. The packet is marked with a sequence number to identify it at the later time of usage. The time t_0 is captured by Relay 1 using its own local time.

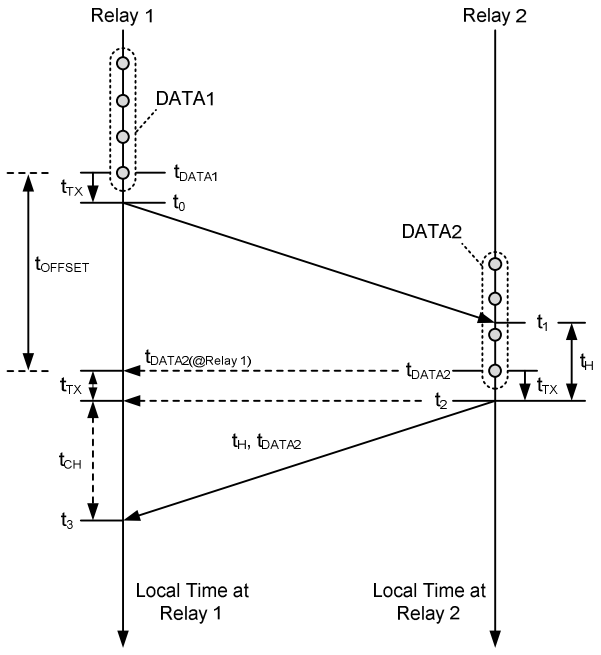

Fig. 7. Illustration of the channel-based alignment method

The packet arrives at Relay 2 after the channel delay time (a few milliseconds to tens of milliseconds). Relay 2 captures the packet arrival time t_1 using its own local clock. This clock is asynchronous from the clock of Relay 1. Time t_1 is required to measure the message hold time (turnaround time) at Relay 2 in order to facilitate the ping-pong algorithm for estimation of the channel delay.

Some time afterward, Relay 2 is ready to send its 87L packet to Relay 1. Again, the message goes out and is time-stamped as time t_2 in the Relay 2 local time. The hold time, $t_H = t_2 - t_1$, is included in the payload of the message. If a constant sampling rate is used by the relays, the hold time can be precalculated at some point after capturing t_1 and be conveniently put in the packet ahead of the transmission time. Relay 2 returns the message sequence number, letting Relay 1 know that the hold time returned to Relay 1 was for the message that originated at t_0.

In its packet, Relay 2 includes a time stamp for the current data t_{DATA2}. In many implementations, the packet sequence number and this time stamp are the same value.

Relay 1 receives the packet channel delay. It captures the time of reception as t_3, using its own clock. From the sequence number received, Relay 1 knows this is a reply to the message sent out at time t_0.

At this point, Relay 1 can finish the key calculations related to channel delay, clock offset, and data alignment.

Assuming symmetrical channel delay, the one-way channel delay is:

$$t_{CH} = \frac{(t_3 - t_0) - t_H}{2} \tag{1}$$

Note that the difference between t_3 and t_0 is the time elapsed at the local relay and the hold time is the time measured by the remote relay and is communicated back explicitly. Therefore, (1) makes sense even though its components were derived from two asynchronously running clocks.

Backdating t_3 by the channel delay time, we get the transmission time at Relay 2 expressed in the local time of Relay 1 (see Fig. 7):

$$t_{2(@\,Relay\,1)} = t_3 - t_{CH} \tag{2}$$

Backdating further by the known delay in transmitting a packet after capturing the data (see t_{TX} in Fig. 7), we obtain the data time stamp expressed in Relay 1 time:

$$t_{DATA2(@\,Relay\,1)} = t_3 - t_{CH} - t_{TX} \tag{3}$$

The data time stamp expressed in Relay 2 time is included in the packet. This allows calculation of the time offset (i.e., the difference in time between the two relays):

$$t_{OFFSET} = t_{DATA2(@\,Relay\,1)} - t_{DATA2} = t_3 - t_{CH} - t_{TX} - t_{DATA2} \tag{4}$$

Positive values of the offset time mean the local clock (Relay 1) is leading the remote clock (Relay 2); negative offset means the remote clock is ahead.

Inserting (1) into (4) gives the following key equation:

$$t_{OFFSET} = \frac{1}{2}(t_0 + t_3 + t_H) - t_{TX} - t_{DATA2} \tag{5}$$

In (5), t_0 and t_3 are local time stamps, t_H and t_{DATA2} are included in the received packet, and t_{TX} is a design constant.

Note that the clock offset value is a very stable number because it reflects a difference between the clocks of the two relays, regardless of channel latency at any given moment.

This means that the raw calculations per (5) are already very stable. They may be further averaged to improve accuracy and provide for a lost packet ride-through capability.

The clock offset t_{OFFSET} is used to shift the received t_{DATA2} time stamp to align it with the local time stamp of the relay:

$$t_{DATA2(@Relay1)} = t_{DATA2} + t_{OFFSET} \quad (6)$$

Differences in the channel latency in the transmitting and receiving directions (channel asymmetry) result in alignment errors while using the channel-based alignment method. When averaging the clock offset, however, a relay is immune to temporary (transient) channel asymmetry. Only a prolonged (standing) channel asymmetry would propagate through the averaging filters and result in alignment errors. This is advantageous because many cases of channel asymmetry are short-lived, resulting from the SONET/SDH systems switching paths.

Note that the 87L relays may be connected to external time sources and synchronize the 87L transmission with the external clocks, while still using the channel-based method in their 87L function. In such a case, the calculated clock offset would be zero as long as the channel is symmetrical and the time sources are accurate. This observation can be used to provide extra channel monitoring and improve the security of the 87L scheme.

B. External Time-Based Synchronization

Data alignment using the channel-based method is often considered superior because it does not require the usage of explicit time sources (historically based on GPS satellite clocks) to be a part of the line protection scheme. Any given 87L operating characteristic handles synchronization errors to a certain degree. However, if the channel asymmetry is beyond the permissible limits given the targeted sensitivity and settings of the 87L function (typically 1 to 2 milliseconds), an option is required to align the data based on the explicit time sources (the external time-based mode). Otherwise, the current differential principle cannot be applied.

In the external time-based mode, relays communicating over an 87L channel require connections to high-precision clocks that provide an absolute time (typically via the IRIG-B inputs). Historically, these clocks are GPS-synchronized but in the near future may use terrestrial, network-based time-distribution schemes (see Appendix C, Subsection B).

The connected clocks need to report time quality via the time-quality bits embedded in the IRIG-B signal, as specified by the IEEE C37.118 standard [6], so that the 87L scheme can respond to situations when the accuracy of time is not adequate for the 87L application.

In the external time-based mode, the free-running internal clocks of the relays are each phase-locked to the external time. Because of that, the clocks are mutually aligned and the time offset does not need to be calculated, but is known to be zero:

$$t_{OFFSET} \equiv 0 \quad (7)$$

The remainder of the data alignment algorithm, starting with (6), works identically as in the channel-based mode, once the time offset is determined per (7).

The 87L relays monitor the presence and quality of connected time sources. A bit is typically provisioned in the 87L data packet to inform the remote relays if the local relay lost absolute time. In this way, the 87L scheme is guaranteed to fail safely if configured to use external time and any of the required sources of time are not available or are degraded beyond the point of safe usage.

Some implementations allow the 87L scheme to configure the data alignment method on a per-channel basis [5]. According to this approach, some channels (known to be symmetrical) may be configured to use the channel-based method. If so, the alignment of data over these channels is not dependent on the presence and quality of connected time sources. Other channels (asymmetrical) may be configured to use the external time-based method. Data alignment over those channels is dependent on the presence and quality of the connected time. In this way, we may limit the exposure of the entire scheme to the availability of time sources.

C. Channel Monitoring Fundamentals

The round-trip channel delay (the sum of the latencies in both directions) can be calculated without the use of absolute time by using the following basic equation (refer to Fig. 7):

$$t_{ROUND\_TRIP} = t_3 - t_0 - t_H \quad (8)$$

When the absolute time is available at both relays communicating over a given channel, it is possible to calculate the channel latencies in the receiving and transmitting directions individually (see Fig. 7, from the point of view of Relay 1):

$$\begin{aligned} t_{CH\_RX} &= t_3 - t_{DATA2} - t_{TX} \\ t_{CH\_TX} &= t_{DATA2} + t_{TX} - t_H - t_0 \end{aligned} \quad (9)$$

The difference between the receiving and transmitting latencies is the channel asymmetry:

$$t_{CH-ASYM} = \left| t_{CH\_RX} - t_{CH\_TX} \right| \quad (10)$$

XII. Appendix C: Concerns With GPS and Terrestrial Distribution of Time

Using wide-area time for protection applications has been historically approached with some reluctance. This appendix reviews some key concerns and summarizes a new terrestrial wide-area time-distribution scheme.

A. Concerns Related to the GPS System

The DoD and the U.S. Department of Transportation (DoT) have committed to make GPS available to civilian users at all times, except in a national emergency. The departments also commit the United States to provide the signal worldwide without a fee for a minimum of 10 years.

It should be noted that the GPS system and satellite clocks used in substations to date have provided highly accurate and reliable time. To further improve the reliability of any system, it is important to understand all possible interference sources. Many of the following, although interesting, are fortunately very rare.

1) Solar Flares

It has been known for some time that the GPS system can be disrupted by electromagnetic storms created by solar flares. These storms occur in 11-year cycles and are caused by electrically charged particles and electromagnetic fields, which are spewed by the sun during the flare. These particles and fields travel relatively slowly toward earth. To the GPS receiver, these fields appear as high levels of background noise or as high energy in band signals, depending on the event. Space weather forecasters can usually give GPS users several hours to several days of warning that a disruption may be coming.

2) GPS Jamming

The GPS signal strength measured at the surface of the earth is about –160 dBw ($1 \cdot 10^{-16}$ watts), which is roughly equivalent to viewing a 25-watt light bulb from a distance of 10,000 miles. This weak signal can easily be blocked by destroying or shielding the GPS receiver's antenna [9]. Because the received GPS signal is so weak, it can easily be jammed by transmitting a signal in the proper frequency range. GPS jammers are more readily available than we might expect. Most of these devices have very short effective ranges, in the order of 5 to 10 meters. GPS jamming (if an issue at all) would most likely affect individual GPS receivers and not a wide area. GPS jamming is a common practice during military exercises [10].

3) GPS Spoofing

GPS spoofing is performed similar to GPS jamming, except that instead of using a strong interference signal, a counterfeit GPS signal is sent. The victim GPS receiver locks on to the stronger signal and accepts the incorrect data. There are many GPS test systems available that produce multiple simulated satellite signals at a very low level. Combined with the proper amplifier, these test systems can be converted into counterfeit sources.

B. Wide-Area Time Distribution Using SONET

Communications systems that utilize TDM techniques are frequency-synchronized (syntonized) by design (see Appendix A). SONET/SDH is based on a tight control over the synchronization and use of a centralized system clock. GPS clocks are typically used to provide the frequency synchronization source for SONET/SDH networks. By their very nature, SONET systems ensure precise frequency control but do not have any idea what time it is. A typical SONET/SDH network will always have one Stratum 1 (±10 parts per trillion [ppt] or an error of $\pm 1 \cdot 10^{-11}$ second over a period of 1 second) clock and most likely a second Stratum 1 clock for redundancy or backup. Custom enhancements of the SONET system make it possible to distribute precision time information, which can originate from external time sources or GPS, in addition to using the clock for frequency control, necessary because of the very nature of SONET.

Today, many substations are equipped with GPS clocks. Wide-area synchronization currently exists through the use of local GPS receivers linked through satellite communications.

The goal is to make the system more robust by relying more on terrestrial components under direct control of the user. One solution is to interconnect all of the clocks via the SONET/SDH network (Fig. 8) [7].

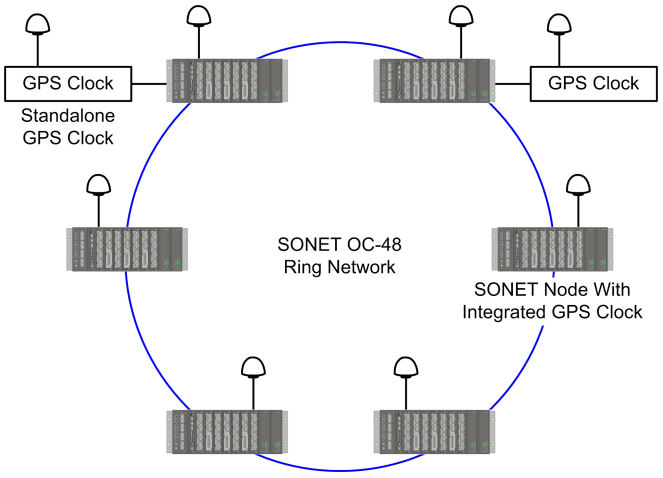

Fig. 8. SONET system with integrated GPS receivers for high-accuracy time distribution

SONET/SDH systems use ring topologies to provide traffic survivability during communications link or multiplexer failures. The proposed system provides a ring topology for the GPS clocks. With all of the clocks in the system networked in a ring topology, the loss of single or multiple satellite downlinks will not disrupt the distribution of high-accuracy timing information. In addition, this clock topology solves issues caused by jamming signals, a broken element in the antenna system, or any other localized disturbances.

An exponentially more robust time system results when the GPS clocks are interconnected through the communications network.

When we integrate the clock into the communications system, use the information from all (legitimate) time sources in the network, and average all of the individual times at each terminal, a timing flywheel is created. Due to the number of potential time sources in the system, clocks that are off from the system average greater than a set tolerance can be identified. These rogue clock signals are ignored by the system until their output comes into compliance. This methodology prevents spoofed GPS clocks from causing errors in the system. Even the local node is able to identify that the local time signal is in error and cannot be trusted, based on a comparison to the system time.

For added stability, the system can also accept high-accuracy timing signals from external clocks. However, if the external clocks are of similar design, they will be susceptible to the same local interferences. The recommended alternative would be a GPS-disciplined cesium atomic clock. Although the GPS portion of the clock is susceptible to common GPS clock issues, the holdover accuracy of a cesium-based clock is capable of providing high-accuracy time for a much greater time period (several months) than a standard crystal oscillator-based clock. The addition of a cesium clock to the system offsets the effect a large solar flare could have on the system, where all of the receivers in any one network would most

likely be affected. With the addition of an atomic clock, the system provides ride-through for any temporary major GPS outage. Because only one or two atomic clocks are required for the network-based time-distribution system and not for each substation, the addition of atomic clocks is attractive economically as well. Atomic clock location on the SONET network can be selected at will, with the system operator control center being the most convenient location.

The described terrestrial time-distribution system is especially attractive for line current differential applications. By combining the communications and time-distribution functions, this system is not only more attractive economically (less equipment, less engineering) but also improves reliability by depending on fewer components to deliver the same total functionality.

Also, the issue of the network breaking into islands followed by the local times drifting apart and the confusion of time when the islands are reconnected is less of an issue for the 87L schemes. If the two relays of a given 87L scheme are connected to two different time islands, the scheme is not operational due to the loss of communications between the relays. Therefore, the local times drifting apart do not impact the scheme. The 87L schemes that use time are secure if the time is adjusted upon reconnection of the islands, the multiplexers assert the degraded time-quality bits accordingly while they adjust time across the reconnected networks, and the relays are designed to ride through such events by responding to the time-quality bits provided by the multiplexers.

XIII. References

[1] CIGRE JWG 34/35.11, *Protection Using Telecommunications*, August 2001.

[2] B. Kasztenny, G. Benmouyal, H. J. Altuve, and N. Fischer, "Tutorial on Operating Characteristics of Microprocessor-Based Multiterminal Line Current Differential Relays," proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[3] D. Finney, N. Fischer, B. Kasztenny, and K. Lee, "Testing Considerations for Line Current Differential Schemes," proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[4] IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations, IEEE 1613-2003, 2003.

[5] H. Miller, J. Burger, N. Fischer, and B. Kasztenny, "Modern Line Current Differential Protection Solutions," proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, March 2010.

[6] IEEE Standard for Synchrophasors for Power Systems, IEEE C37.118-2005, 2005.

[7] K. Fodero, C. Huntley, and D. Whitehead, "Secure, Wide-Area Time Synchronization," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[8] Telcordia Technologies GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, Issue 4, December 2005.

[9] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures," Los Alamos National Laboratory, December 2003. Available: http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html.

[10] U.S. Coast Guard Navigation Center (U.S. Department of Homeland Security), "Overview of the U.S. Federal Government's Policy on Activities Which May Cause Interference to GPS." Available: http://www.navcen.uscg.gov/?pageName=gpsServiceInterruptions.

XIV. Biographies

Bogdan Kasztenny is a principal systems engineer in the research and development division of Schweitzer Engineering Laboratories, Inc. He has over 20 years of expertise in power system protection and control, including ten years of academic career and ten years of industrial experience, developing, promoting, and supporting many protection and control products.

Bogdan is an IEEE Fellow, Senior Fulbright Fellow, Canadian member of CIGRE Study Committee B5, registered professional engineer in the province of Ontario, and an adjunct professor at the University of Western Ontario. Since 2011, Bogdan has served on the Western Protective Relay Conference Program Committee. Bogdan has authored about 200 technical papers and holds 20 patents.

Normann Fischer received a Higher Diploma in Technology, with honors, from Witwatersrand Technikon, Johannesburg, in 1988, a BSEE, with honors, from the University of Cape Town in 1993, and an MSEE from the University of Idaho in 2005. He joined Eskom as a protection technician in 1984 and was a senior design engineer in the Eskom protection design department for three years. He then joined IST Energy as a senior design engineer in 1996. In 1999, he joined Schweitzer Engineering Laboratories, Inc. as a power engineer in the research and development division. Normann was a registered professional engineer in South Africa and a member of the South Africa Institute of Electrical Engineers. He is currently a member of IEEE and ASEE.

Ken Fodero is currently a research and development manager for the multiplexer systems product line at Schweitzer Engineering Laboratories, Inc. (SEL) in Pullman, Washington. Before coming to SEL, he was a product manager at Pulsar Technology for four years in Coral Springs, Florida. Prior to Pulsar Technology, Ken worked at RFL Electronics for 15 years. His last position there was director of product planning.

Adrian Zvarych is currently a senior communication application engineer with Schweitzer Engineering Laboratories, Inc. (SEL). Adrian has over 28 years of combined field, engineering, and planning experience in the electric utility industry in protection, control, and telecommunications systems. Prior to joining SEL, Adrian worked at TRC Engineers as a consultant for three years. Prior to that, he dedicated 15 years to Progress Energy in the protection and telecommunications areas. He started his engineering career at NextEra (formerly Florida Power & Light) in South Florida in 1982. Adrian maintains his membership in the IEEE in the PES and Communications Societies and is a licensed Professional Engineer in the State of Florida.